



CYBERTECH100

Profiles of the **CYBERTECH100**, the world's most innovative CyberTech companies that every leader in the financial services industry needs to know about in 2021





3rd Annual
**FINANCIAL SERVICES
CYBERTECH FORUM**

SAVE THE DATE

28 SEPTEMBER 2021 | LONDON



**Join the Leading Event for
Information Security in
Financial Services**

FIND OUT MORE ABOUT OUR HYBRID FORMAT AT

www.CyberTechForum.com



The **CYBERTECH100** is an annual list of 100 of the world's most innovative CyberTech companies selected by a panel of industry experts and analysts. These are the companies every financial institution needs to know about as they consider and develop their information security and financial crime fighting strategies.

There's plenty of interest and hype about CyberTech in financial services given the increased risk of data breaches and cyber attacks, but much of it is superficial, incoherent or self-serving and fails the needs of decision-makers in incumbent financial institutions who require independent facts, figures and analysis.

The **CYBERTECH100** list will help senior management filter through all the vendors in the market by highlighting which business models have market potential and are most likely to succeed and have a lasting impact on the industry.

CRITERIA

The criteria assessed by the Advisory Board and FinTech Global team include the following:

- Industry significance of the problem being solved
- Growth, in terms of capital raised, revenue, customer traction
- Innovation of technology solution
- Potential cost savings, efficiency improvement, impact on the value chain and/or revenue enhancements generated for clients
- How important is it for a financial institutions to know about the company?

PROCESS



RESEARCH CYBERTECH UNIVERSE

Analyse universe of CyberTech solution providers on RegTech Analyst's database and external sources



NOMINATE COMPANIES

Shortlist candidates that meet criteria along with companies nominated via the website



CONDUCT INTERVIEWS & SURVEY

Undertake in-depth interviews or surveys with founders and CEOs of shortlisted companies



IDENTIFY CYBERTECH 100

Determine which companies excel in terms of the criteria and can be classified as CyberTech innovation leaders



PUBLISH

Announce results to media and finalists



4th Annual

**GLOBAL
REGTECH
SUMMIT**

SAVE THE DATE

14 OCTOBER 2021 | LONDON






**Join the World's Largest
Gathering of RegTech Leaders
and Innovators**

FIND OUT MORE ABOUT OUR HYBRID FORMAT AT

www.GlobalRegTechSummit.com



-  Founded 2016
  Employees: 11-50
-  Subsectors: Threat Management/Security Operations, Endpoint Security, Cloud Security, Threat Hunting
-  Regions of operations: United States

Active Countermeasures is a group of like-minded geeks that believe in giving back to the security community. The company's AC-Hunter solution is a network-based threat hunting tool. There are no agents to install and AC-Hunter is capable of protecting desktops, servers, network hardware, IoT, IIoT, or any other type of device connected to the network. AC-Hunter hunts the complete network on an hourly basis and reports its findings using a threat score system. Junior analysts can then respond to score changes to identify systems that have been compromised. This both focuses the workflow as well as dramatically reduces the false positive rate.



-  Founded 2009
  Employees: 251-500
-  Subsectors: Data Security/Data Governance, Risk Assessment/Risk Management
-  Regions of operations: United States, Bulgaria, United Kingdom, Ireland

A-LIGN is a technology-enabled security and compliance partner that helps global organisations take a strategic approach to confidently mitigate cybersecurity risks. A-SCEND, A-LIGN's proprietary compliance management platform, helps businesses consolidate their security and compliance processes. Driving automation, workflow and efficiency through technology has been absent in the compliance industry until now, and A-SCEND complements the professionals in the audit workflow to make their role as streamlined and automated as possible. A-SCEND delivers a polished user experience with real-time audit tracking, improved communication between assessors and clients and the ability to enable additional security controls like two-factor authentication and database encryption.



-  Founded 2014
  Employees: 51-100
-  Subsectors: Data Security/Data Governance, Cloud Security, Threat Management/Security Operations, Application Security
-  Regions of operations: United States, Canada

ALTR delivers data governance, security, and intelligence as a service to the data-driven enterprise. The industry's first no-code, cloud-native platform, ALTR simplifies control over your data so you can focus on getting value from it. Understand where your sensitive data is, how it's being used, and mitigate your data risk. By eliminating time consuming installation, configuration, and maintenance, ALTR's customers can get started quickly and operationalize their data strategy using a single platform.



Founded 2018



Employees: 51-100



Subsectors: Cloud Security



Regions of operations: United States, Canada, United Kingdom, EMEA

AppOmni is a leading provider of SaaS Security Management software. The company was founded by a team of security veterans from top SaaS providers, high tech companies, and cybersecurity vendors. Its patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. The AppOmni solution makes it easy for security and IT teams to secure their entire SaaS environment from each vendor to every end user. As SaaS applications evolve, AppOmni stays current with all updates and releases to keep customer environments secure over time.



Founded 2013



Employees: 11-50



Subsectors: Fraud Prevention, Risk Assessment/Risk Management, Financial Crime Risk Governance



Regions of operations: Africas (South Africa), APAC, EMEA (United Kingdom), Americas (Canada & United States)

Arctic Intelligence is a global RegTech firm that has developed enterprise risk assessment software enabling regulated businesses to better assess, document and manage their financial crime risks. Trusted by over 200 clients globally, Arctic Intelligence solutions are cost-effective and multi-jurisdictional allowing businesses regardless of their size or complexity to carry out their financial crime risk assessment and manage vulnerabilities consistently across their entire organisation. The company's Risk Assessment Platform can be used to assess other risk domains such as cyber risk, information security risks by people bringing their own risk models and loading them in the platform. It also allows customers to connect globally via a single instance and enables access to company data that resides within regional databases. This functionality addresses and solves the global issue around maintaining privacy regulations and data ownership. It also means that clients can still enjoy all the benefits of 'software as a service' and have client specific data and information, such as financial crime risk assessments, stored in country to align with privacy regulations.



Founded 2015



Employees: 251-500



Subsectors: Threat Management/Security Operations, Endpoint Security, Risk Assessment/Risk Management



Regions of operations: Global

Most businesses can't see 40% of the devices in their environment. From managed to unmanaged, businesses struggle with identifying all the devices around them, and being able to secure themselves. Armis discovers all devices and associated risks in your environment, detects threats, and acts automatically to protect your critical systems and data - especially unmanaged devices. Armis is agentless and integrates easily with your existing security products. Armis passively monitors wired and wireless traffic on your network and in your airspace to identify every device and to understand each device's behaviour without disruption. Then the company analyses this data in its Risk Engine, which uses device profiles and characteristics from the Armis Device Knowledgebase to identify each device, assess its risks, detect threats, and recommend remediation actions.

THREATQUOTIENT 

FOCUS ON THE THREAT

Prioritize, automate & collaborate
with a platform purpose-built for

**THREAT-CENTRIC
SECURITY OPERATIONS**

WWW.THREATQ.COM



Founded 2010



Employees: 11-50



Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Fraud Prevention



Regions of operations: United Kingdom, Europe

Astr Cyber Security is a cloud-first cybersecurity consulting firm offering implementation of security components to secure client's cloud environments and threat hunting/monitoring services for AWS & GCP. One of the company's main offering is Managed Detection & Response (MDR). Astr implements tools and evaluates GDPR, PCI-DSS compliance while reporting on vulnerability within end points or network.



Founded 2014



Employees: 11-50



Subsectors: Application Security Cloud Security



Regions of operations: India, United States, Europe

A NASSCOM Emerge 50 company, Astra is a security suite consisting of security audits, a Web Application Firewall, a Malware scanner and other security tools. The company's flagship product, ASTRA, brings together an extensive feature set of manual/automated penetration testing tools, while performing a comprehensive vulnerability assessment and proactively responds to threats. Astra stops one million+ threats on its customer's web applications every day. The VAPT product has uncovered 100,000+ vulnerabilities in client applications. Many prestigious brands like Gillette, Carrier, African Union, Ford, Oman Airways, Cosmopolitan, Hotstar, Kotak Securities, Dolls Kill, Invicta, Akeneo (founded by former CTO of Magento) and thousands of other brands use Astra's security solution.



Founded 2011



Employees: 101-250



Subsectors: Threat Management/Security Operations, Identity & Access Management, Endpoint Security, Cloud Security



Regions of operations: United States, India, United Kingdom, Europe, Dubai, Middle East, Australia/New Zealand, Singapore, Mexico

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE Shield, and its capabilities tightly align to the MITRE ATT&CK Framework. Attivo has won over 150 awards for its technology innovation and leadership.

AURAYA



Founded 2010



Employees: 11-50



Subsectors: Threat Management/Security Operations, Identity & Access Management, Fraud Prevention



Regions of operations: Australia, New Zealand, United Kingdom, United States

Auraya is a world leader in voice biometric technology with the mission of empowering people and organisations to interact and engage with convenience and security in all channels and languages.

awareGO



Founded 2007



Employees: 11-50



Subsectors: Employee Risk, Risk Assessment/Risk Management



Regions of operations: Iceland, Czech Republic, United States, Croatia

AwareGO is a global provider of security awareness training content and solutions that help enterprises improve cybersecurity awareness in the workplace and protect their business from modern-day cybersecurity risks. The company's training ethos is based on peer education instead of lecturing, a no blame-no shame approach as well as explaining complex situations in a simple manner through fun and engaging bite-sized video lessons. AwareGO's continuously growing library of training videos applies best-in-class tools and techniques from the advertising industry to create effective one-minute, real-life videos proven to increase security awareness. To date, the company has successfully trained more than 8 million employees worldwide.



BigID



Founded 2016



Employees: 251-500



Subsectors: Identity & Access Management, Data Security/Data Governance, Risk Assessment/Risk Management

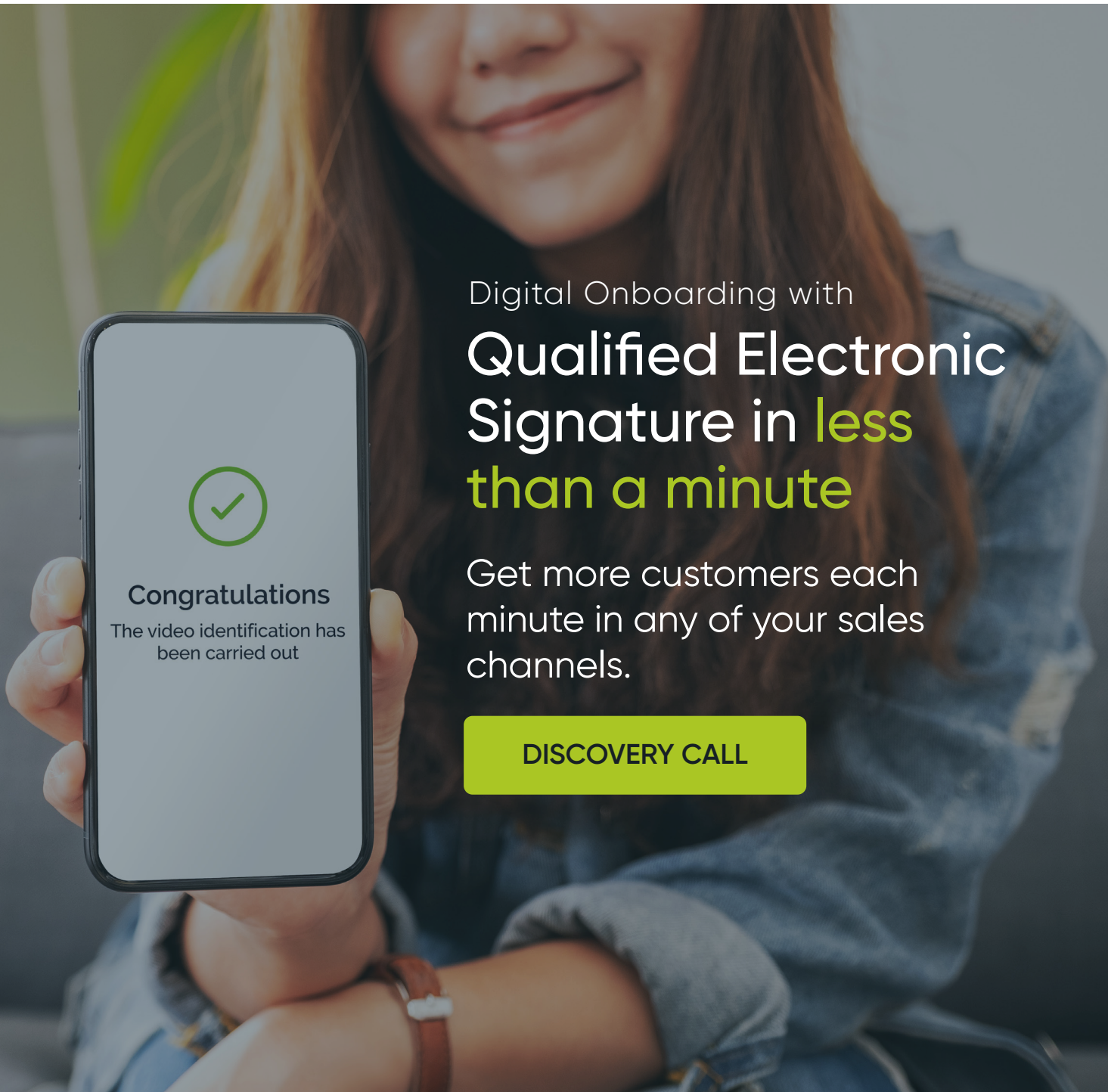


Regions of operations: Global

BigID's data intelligence platform enables organizations to know their enterprise data and take action for privacy, protection, and perspective. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape. By applying advanced machine learning and deep data insight, BigID transforms data discovery and data intelligence to address data privacy, data security, data governance, compliance, and risk challenges across all types of data, at petabyte-scale, on-prem and in the cloud. Get actionable data intelligence with BigID: one platform, infinite possibility.



**Electronic
IDentification**[®]
www.electronicid.eu



Digital Onboarding with
**Qualified Electronic
Signature in less
than a minute**





Get more customers each
minute in any of your sales
channels.

[DISCOVERY CALL](#)

Do you need an end-to-end solution to onboard new customers?





We help you acquire customers easily and increase your business with the most secure Digital IDentification system on the market. Our solution integrates an end-to-end process to ensure no additional suppliers: from the verification and authentication in all your systems to the Qualified Electronic Signature.



-  Founded 2011
  Employees: 251-500
-  Subsectors: Threat Management/Security Operations, Identity & Access Management, Fraud Prevention
-  Regions of operations: United States, United Kingdom, Europe, Middle East, Asia

Callsign is an identity fraud, authorisation and authentication company, with solutions for businesses across all digital sectors. The company solves challenges that organisations face in getting their users onto and interacting with their digital platforms easily and securely. Callsign provides solutions to some of the world's largest banks and offers "bank grade" identification to public and private sector clients of all sizes to ensure that their legitimate customers can access their services easily, whilst at the same time blocking fraudsters. Callsign's modular solution includes intelligent analytics e.g. behavioural biometrics, device fingerprinting, location analytics and telco data; feeding into a decisioning module which orchestrates dynamic, and contextual user journeys; and active authenticators e.g. swipe. Companies are faced with the challenge of having to prioritise fighting fraud, regulatory compliance, user experience and managing costs. Callsign has removed the need to compromise with an agile solution that is adjustable to customers evolving business needs.



-  Founded 2009
  Employees: 11-50
-  Subsectors: Risk Assessment/Risk Management
-  Regions of operations: Ireland, United Kingdom, United States, Gulf Cooperation Council


The CalQRisk cybersecurity solution assists organisations in conducting risk assessments, maintaining control libraries, generating reports, and much more. Its out-of-the-box knowledgebase of risks and controls can be used to benchmark your efforts against regulation, legislation, and international standards such as ISO 27001, NIST, etc. Users can maintain multiple risk registers, generate interactive dashboards to evidence their efforts, and avail of a suite of standard and custom reports. The CalQRisk solution can also be employed to facilitate effective third party / vendor due diligence by streamlining what for many organisations can be a predominantly paper-based exercise. CalQRisk clients range across the financial services industry, as well as many other sectors including aviation, public bodies, and educational institutions.




-  Founded 2018
  Employees: 11-50
-  Subsectors: Data Security/Data Governance, Risk Assessment/Risk Management
-  Regions of operations: Australia, United Kingdom, The Netherlands, New Zealand, Singapore


Castlepoint is an information and records management solution for the enterprise. Castlepoint uses artificial intelligence to automatically register, classify, sentence, track, monitor and audit all records of a business, no matter what system they are stored in. Castlepoint is an innovative AI regulatory technology solution that reads every word of every document, email, database, or webpage, for example. It understands what each information asset is about, what risk and value it has, who is doing what to it, what regulatory rules apply to it, and whether they are being met.



 Founded 2015


 Employees: 51-100

 Subsectors: Threat Management/Security Operations, Fraud Prevention, Risk Assessment/Risk Management, Threat Intelligence


 Regions of operations: Global


Cobwebs Technologies is an industry-leading AI-Driven, multilingual automated threat intelligence platform for digital risk protection. Cobwebs platform provides real-time valuable and actionable insights that enable organisations to detect and expose unknown threats and threat actors to prevent criminal activity while maintaining business continuity and viability. Cobwebs' Threat Intelligence solution combined with human expertise produces superior security intelligence that disrupts adversaries. Instantly alerts among others, online phishing campaigns, data leaks, and fraud. Enhance your vulnerability assessment and incident response to deliver stronger brand protection with complete access to the most comprehensive, fully automated data collection available from the open, deep, dark web, and other growing publicly available data sources.



 Founded 2018


 Employees: 1-10

 Subsectors: API Security, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security

 Regions of operations: United States, Europe, Asia


Corsha's API Security Platform simplifies API security and empowers financial institutions to embrace modernisation, complex deployments, and hybrid environments with confidence. The platform protects data and applications by pinning API access to trusted, authorised machines, thereby preventing attackers from exploiting API keys, tokens and certs. The platform is easy to integrate and deploy in virtually any network environment and enables visibility and control over all API traffic. Corsha's platform is based on patented technology that creates a dynamic machine identity for every authorised machine in a network and then uses that identity to provide dynamic, multi-factor authentication (MFA) for every API call.



 Founded 2018

 Employees: 1-10

 Subsectors: Threat Management/Security Operations, Identity & Access Management, Cloud Security, Fraud Prevention, Threat Intelligence

 Regions of operations: United States, India, Australia, Singapore, UAE

Crysp's Trust Intelligence Platform leverages advanced analytics and behavioural biometrics to reduce fraud by using innovative device identification, device reputation and smart authentication solutions. Crysp enables FinTechs, EdTechs, eCommerce, online gaming & betting organizations improve online trust by proactively identifying bad actors (users and machines). Crysp technologies have currently been deployed on 200M+ devices and are helping clients: Reduce misuse of promotions and cashbacks; Detect account takeovers and identity theft; Detect new account registration fraud; Reduce chargeback and friendly fraud; Reduce false declines and reviews; Reduce reseller fraud; Detect bots and machine behaviour; Reduce customer friction and improve genuine customer adoption; Block previously blacklisted fraudsters from returning; Enhance effectiveness of existing anti-fraud solutions.



COMPANY RESEARCH PROFILE



Founded 2016
 New York, United States
www.cssregtech.com
cybersecurity@cssregtech.com

Employees: 101-250
 Regions of operation: United States, United Kingdom, Ireland, Netherlands, Sweden, Luxembourg, France

KEY EMPLOYEES:



Doug Morgan
Chief Executive Officer



John Lee
President



Ronan Brennan
Chief Product Officer



E.J. Yerzak
Director of Cyber IT Services

Subsectors: **Threat Management/Security Operations, Data Security/Data Governance, Network Vulnerability, Employee Risk, Risk Assessment/Risk Management, Compliance Management**

OFFERING

CSS helps organisations understand cybersecurity risks from regulatory, business and operational perspectives. From implementing and maintaining cyber and business continuity policies and procedures to performing testing, conducting security awareness training or assessing or building a full cyber program, CSS's cybersecurity experts will design or adapt a cyber program based on a company's needs and stage of growth leveraging a combination of custom services and technology solutions.

PROBLEM BEING SOLVED

Cyberattacks have increased in both volume and sophistication over the years. As more firms operate in the cloud through email, file sharing, and trading through their custodian, and as detection capabilities improve, hackers work to evolve their techniques and methods. Investment managers need to do more than ever to help protect their firms from potential cyber threats and mitigate risk to proprietary and client data.

EXPERTISE

The CSS team maintains industry-leading cybersecurity certifications and frequently interacts with industry regulators to stay on top of the latest trends, bringing actionable risk management capabilities to clients.

CSS specializes in the investment management and financial services space and understands the cyber risks that are most critical to organisations in these industries and to their clients and investors.

PRODUCT DESCRIPTION

CSS's technology solutions and services include:

- **Policies & Procedures Development and Review** – The CSS team will help establish a robust, well-documented cyber program which forms the backbone of a control framework, providing strong governance, accountability, and repeatable processes.
- **Security Testing** – Security testing backed by our proactive and responsive team provides you with clear, understandable risk reporting and interaction with our subject matter experts through a secure, encrypted SaaS technology solution.
- **Cyber Training** - Whether your employees prefer to complete security awareness training on their own time through on-demand modules or whether they respond best to live training customized to your policies and procedures, CSS can help.
- **Cyber Preparedness Assessment** - CSS has a deep bench of regulatory expertise supporting its cybersecurity risk management solutions. It can customize an assessment to a framework or risk approach that best meets client objectives.
- **Dark Web Monitoring** - Monitor 24/7, 365 days per year through artificial intelligence and human interaction to identify stolen credentials and other personally identifiable information (PII) in private websites, chat rooms and dark web forums, with technical breach reporting backed by clear, understandable explanations of risk tailored to financial services firms.

TRACTION/GROWTH

- CSS currently serves over 650 clients in the financial services vertical comprising of traditional asset managers, hedge funds, and fund administrators, from both buy-side and sell-side institutions.
- The company is partnering with private equity firms to conduct cybersecurity risk assessment of portfolio companies.
- CSS is the best of both worlds – offering flexible and automated technology powered by artificial intelligence and complemented by trusted cybersecurity experts that provide a human, personalized touch.

How CSS is leveraging AI to keep bad actors in the digital world at bay

The ubiquity of high-profile cyberattacks in the last few years have highlighted the importance of online security, and AI and machine learning (ML) might be the antidote against cybercriminals.



Almost every organisation in the world, regardless of what industry or sector, is at risk of suffering a crippling cyberattack at any given moment. With the rapid digital shift during the pandemic, threats from online scams are only getting worse and the scale and severity of incidents have escalated. The Colonial Pipeline attack has shown no one is immune as online threat actors continue to employ a suite of sophisticated methods for hacking. Compliance Solutions Strategies (CSS) Director, Cyber IT Services E.J. Yerkak said, "Every company is now a data company, increasing the target on the backs of all of them."

Figures clearly indicate that cyberattacks are on the rise and are becoming more damaging for companies. Dealing with the fallout of breaches isn't cheap. The average cost for a firm to recover from a ransomware attack jumped to \$1.85m in 2021, per research by Sophos. Attacks are increasingly causing consequences to be felt beyond the perimeter of an organisation, as demonstrated by Colonial Pipeline being forced to shut down operations causing fuel prices along the East Coast to soar.

According to Yerkak, cyberattacks by nation states have grown in complexity and sophistication impacting critical national infrastructure. The SolarWinds attack, for instance, infiltrated organisations across the world via seemingly

legitimate software updates. What these kinds of stealthy supply chain attacks have made startlingly clear is the capacity for a cyberattack to cripple enormous sections of national infrastructure and have the potential to cause substantial damage.

Tellingly, it is no longer an option for government cybersecurity policy and technical strategy to be reactionary when attackers are already employing ransomware to sabotage critical systems. Yerkak said, "The key to moving from an ad hoc, reactive cybersecurity program to a mature, proactive program is well-documented processes. Formal cybersecurity policies and procedures establish a strong risk governance framework, providing for ownership of risks by relevant business units."

Along with causing hurdles for governments, incumbent enterprises like Ashley Madison, Microsoft, Facebook and Netflix have too fallen prey to the malicious intent of digitally savvy offenders. SMEs aren't left unscathed either; the Federation of Small Businesses estimates that small British firms annually spend £5.26bn dealing with cyberattacks.

Additionally, the ongoing Covid-19 has exacerbated the threat of attacks. "Remote and traveling workforces expand the risk footprint of a business to every single device and app used by the business. Containing these threats requires a strategic approach to processes, people, and technology," Yerkak opined.

The key reason for companies becoming increasingly vulnerable to cybercriminals is that these attacks have become commoditised. Yerkak said, "Malware and ransomware as a service have made it possible for anyone with a few dollars to add a cyberattack and a target to one's shopping cart and launch it against a company." Online fraud could be in the form of bot attacks, false invoices, money laundering, phishing attempts and ransomware.

Pointing out the main concern for companies, Yerkak said there is a lack of experienced staff. He said, "Many companies are hard-pressed to find qualified, competent cybersecurity expertise and talent needed to take a holistic, proactive approach to cybersecurity." Frost & Sullivan predicts that the growing gap between available qualified cybersecurity professionals and unfulfilled positions will reach 1.8 million by 2022. In addition, the 2020 Cybersecurity Workforce Study conducted by (ISC)2 found that employment in the field needs to grow by circa 41%

in the US and 89% worldwide to fill the present talent gap. "Until nations do a better job of educating workforces for the skills of tomorrow's security jobs, firms will be in a defensive posture when it comes to cybersecurity," he continued.

The challenges don't end with lack of qualified cybersecurity professionals. Those working as security professionals are under constant pressure as they need continuous training and professional development to keep up with evolving technologies and the threat landscape. Yerzak continued, "What tends to happen is that those firms who are able to hire cyber staff in house end up spending most of the time putting out fires instead of fireproofing the house. Cyber teams are stretched thin, creating opportunities for more vulnerabilities to remain unmitigated for too long."

Is AI the "Mjolnir" to combat cybercriminals?

Having robust cybersecurity encompasses multitudes of subdomains – from malware analysis, penetration testing and code review to forensics, threat intelligence and risk assessment. It also entails regulatory compliance, cryptography, network monitoring, and timely incident response. Traditional security tools lack the ability to detect a potential cyberattack that may threaten to destabilise a company's or even a city's entire infrastructure.

Moreover, the most qualified human security teams can be easily outsmarted by complex lines of code with attacks capable of disabling several components of a system at once, Yerzak detailed. Consequently, the solution is to deploy technologies that can respond autonomously when humans cannot. This is where AI and machine learning comes in.

By analysing data from millions of cyber incidents and using it to identify potential threats – from an employee clicking on phishing links or a new variant of malware – AI can be used to improve human analysis.

Yerzak believes that AI is the shield which can be essential to protect one against online danger. He said, "Knowledge is power, and as data volumes continue to increase exponentially, AI and machine learning will play ever-increasing roles in helping firms filter out the relevant threat intelligence from all the cyber noise."

AI – bane or boon?

It takes no expert to see that instead of waiting for the inevitable, companies must start reassessing their basic cyber hygiene practices, updating the patches and accounting for human error and shortcomings.

For Yerzak, while the golden nugget has been the use of AI and machine learning, he added that it might be a double-edged sword. By using advanced technology, cybercriminals have tried to tweak their malware code so that security software no longer recognises it as malicious. A report by Europol warned that AI is one of the emerging technologies that could make cyberattacks more dangerous and more difficult to spot than ever before.

Yerzak said, "AI and ML capabilities will further the cat and mouse game, making it easier and easier for cybercriminals to create convincing deep-fakes and to launch sophisticated attacks with minimal interaction, while simultaneously increasing the ability of threat hunters to find and detect relevant risks."

How CSS can help in fighting back

Clearly, as technologically connected cyber-physical environments become more prevalent, so does advanced attacks targeted against them, therefore making risk prevention and mitigation increasingly essential. Companies must deploy measures to proactively stop threats before they are able to release malicious software throughout a digital ecosystem. And according to Yerzak, CSS can help firms "to elevate the strength and maturity of their cybersecurity programs from reactive to proactive."

CSS's AI-based risk management database has proven capable of increasing visibility across all environments, Yerzak continued. Essentially, CSS's solution specialises in threat identification with end-to-end encryption for communication and collaboration of vulnerabilities and remediation with relevant stakeholders. Building on the operation of CSS's cybersecurity technology, he detailed, "The CSS solution provides a risk management dashboard and data warehouse for tagging and tracking issues through to resolution and offers the ability to interact with our cybersecurity experts with the click of a button for detailed explanations of technical concepts."

The surveillance software is even able to detect the silent and stealthy attacks that slip under the radar, as well as monitor the dark web for compromised credentials "to supplement the research and threat analysis of our cybersecurity experts," Yerzak added.

Alongside detecting anomalous activity that appears, CSS's AI solution autonomously distinguishes between malicious and benign. "Our cyber solutions enable firms to sift through the noise to quickly see which risks are worth worrying about and should be prioritised, and which issues present a lower level of risk in the context of their particular business," he said. "Partnering with a firm like CSS can help reduce your cyber risk, enabling you to focus on your core business."

It's no secret that the impending gravity of cyberattacks results in serious collateral damage. While it is impossible to guarantee complete protection against an attack, organisations must prioritise security to deter would-be attackers and enable recovery. In IBFS global chief information security officer Stephane Nappo's words, "It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

Yerzak concluded, "Regardless of how far the technology itself advances, cybersecurity programs will continue to need the right combination of technology and strategic partners to be able to find risk and communicate risk in a meaningful, actionable way to the business itself." ●



Regulatory Technology Driven by Data. Backed by Service.

Cybersecurity - Client Success

Market Landscape

The Securities and Exchange Commission (SEC) published a report on Cybersecurity and Resiliency Observations and several risk alerts in which it sets forth expectations for strong information security controls to combat the growing risks of phishing, ransomware, and credential stuffing, as well as increasingly sophisticated attack methods employed by cybercriminals. Our client is an adviser to private funds. The RIA was challenged to manage its own cybersecurity risk while simultaneously seeking to understand the cybersecurity risk profile of its portfolio holdings.

The Client:

Our client is an SEC-registered investment adviser with 85 employees across three U.S. offices. The RIA advises private equity funds in sectors which include manufacturing, healthcare, professional services, and real estate.

Business Challenge:

The Chief Compliance Officer (CCO), Chief Operations Officer (COO) and Chief Technology Officer (CTO) recognized the need to increase their cybersecurity defenses while trying to get a handle on the inherent cybersecurity risks in their portfolio company investments. The senior management at the RIA understood that breaches at the underlying portfolio company level could have a material impact on fund valuations in addition to operations and cash flow (in the event of network or system outages and ransomware). The firm had experienced several successful phishing attempts, including one in which funds were stolen. The firm's existing cyber policies were minimal, although some ad hoc control structures existed. The firm's appreciation of the risks to the business was enhanced by the current increased regulatory scrutiny around cybersecurity controls and an ever-expanding set of expectations from investors around privacy and security arising in the course of investor due diligence.

Business Results:

Using a combination of technology backed by in-house regulatory and cybersecurity expertise, CSS provided the RIA with a comprehensive cybersecurity risk management suite. The firm engaged CSS to conduct 24x7 dark web monitoring of its email accounts across several domains, using artificial intelligence and human interaction to present actionable risk intelligence in clear, understandable terms for senior management to reduce the risk that compromised credentials could be used against the firm. CSS rolled out a cybersecurity testing plan which included regular vulnerability scanning, penetration testing, phishing testing, and a combination of on-demand security awareness training modules and live, customized security training tailored to the firm's specific policies and procedures.

Value Realized:

The RIA was able to identify that 25% of its staff and 10% of its portfolio company employees were susceptible to phishing attacks and promptly remediate, saving the firm up to \$5.86M in data breach costs. CSS testing identified opportunities to add Multifactor Authentication to applications, identified passwords which had not been changed in over a year, and its team developed a tailored set of information security policies and procedures that have helped the firm respond favorably to investor RFPs and DDQs to expand its investor base.

Don't wait until a cyber incident occurs.

Contact CSS's Cybersecurity Team today to see how you can achieve a cybersecurity program that showcases your strength and resiliency: cybersecurity@cssregtech.com.





Founded 2017



Employees: 11-50



Subsectors: Threat Management/Security Operations, Endpoint Security



Regions of operations: Canada, United States, UAE, South America, Africa, Mexico

CYDEF is a Canadian cybersecurity company that delivers managed Endpoint Detection and Response (EDR/MDR) to organizations of any size. Set up is simple. A rapidly deployable agent is installed on the endpoint (Mac and PC) to enable CYDEF to monitor the device's application and process behaviours. No capital equipment, no ramp up period or fine tuning, NO cyber security expertise required. CYDEF's supervised Machine Learning sends only valid alerts (no false positives or 100s of alerts to review). The value outcome for our customers is saving them up to 80% in IT overhead. Their IT teams can focus on their business instead of cyber threats.



Founded 2016



Employees: 11-50



Subsectors: Risk Assessment/Risk Management, Integrated Risk Management, Cyber & IT Risk Management



Regions of operations: United States, EU, EMEA, Asia, Australia, New Zealand

CyberSaint Security was founded in 2016 with the mission to empower organizations to build a cybersecurity program that is as clear, actionable, and measurable as any other business function, lifting up cyber and IT as business enablers in the digital age. The CyberStrong platform empowers teams, CISOs, and Boards to measure, mitigate, and communicate risk with agility and alignment, and seamlessly integrates all cybersecurity and IT risk and compliance functions with a powerfully automated approach. From high-growth startups to Global 100 titans, CyberSaint's customers embrace a cutting-edge approach to risk and compliance that allows them to mitigate the risks that stand in their way and take the risks that matter.



Founded 2017



Employees: 51-100




Subsectors: External Attack Surface Management & Protection





Regions of operations: North America, Europe, Israel


CyCognito empowers companies to take full control over their attack surface by uncovering and eliminating the critical security risks they didn't even know existed. Every organization contains countless points of entry across an ever-changing attack landscape, many of which they aren't even aware of. But one single weak spot is all it takes for attackers to get in the door. So how can security teams possibly eliminate every single point of entry, when their security tools can't even see all of them? CyCognito's team uses its intelligence-agency expertise and keen understanding of hacker techniques to help organizations uncover their shadow risk and protect their entire attack surface before attackers have a chance to exploit any gap.



 Founded 2011

 Employees: 51-100

 Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Risk Assessment/Risk Management


 Regions of operations: North America, Europe, Asia Pacific, Middle East


CYE was founded in 2012 by the founder of the IDF's red team unit and grew to become a market specialist in red team (black-box) cyber security assessments and cyber maturity programmes. The company's technology leverages advanced AI and analytics to continuously assess behaviours and events, automatically block threats before they occur, and enable the organisation to focus resources and efforts where they matter the most. CYE operates globally with offices in five locations and support clients (Fortune500, with a strong foothold in the banking and insurance sector) throughout their cyber security journey with a range of tailored solutions.



 Founded 2015

 Employees: 1-10

 Subsectors: Data Security/Data Governance, Cloud Security, Risk Assessment/Risk Management

 Regions of operations: United Kingdom, The Netherlands

CyNation is an Integrated Risk Management company focused on managing the risks inherent in third-party ecosystems. Its solutions are trusted by banks, insurers, asset management firms and innovation centres across Europe. CyNation helps companies in industries that typically have large, third-party networks, are data-rich and highly regulated. These sectors face a high volume of data flows, interconnected processes, lack of transparency, compliance and third-party risk. The company's CyDesk solution is an integrated risk management platform that automates digital risk management, providing advanced, prescriptive analytics that identify, analyse and manage risk factors across third-party ecosystems. As these ecosystems can be large and complex, it also mitigates risks stemming from fourth parties and shadow vendors.



 Founded 2019

 Employees: 1-10

 Subsectors: Application Security, Cloud Security, Employee Risk, Risk Assessment/Risk Management

 Regions of operations: United States, United Kingdom, APAC

Cynergy is an Israel based company which was established to solve the biggest problems in cybersecurity nowadays, helping enterprises with lean cybersecurity team to focus and correctly use their internal and external resources by advance prioritization of vulnerabilities. Cynergy is comprised out of Israel's leading cybersecurity experts, security architects, red teamers, and former cyber consultancy leaders. The company enables clients to discover their full external attack surface, cloud, web, infrastructure, employees, and data. Cynergy uses advanced prioritization AI to help companies focus on what's important to resolve using actual exploitation of identified vulnerabilities.



dathena



Founded 2016



Employees: 51-100



Subsectors: Data Security/Data Governance, Risk Assessment/Risk Management



Regions of operations: APAC, EMEA, AMS

Dathena is a deep-tech company that provides an AI-Driven Data Discovery and Classification platform, bringing a new paradigm to data privacy and security solutions. In a world of ever-growing information, regulation, and consumer privacy expectations, enterprises around the globe rely on Dathena to identify, classify and control their sensitive data, reduce risks, and enhance the data protection framework. Leveraging the power of modern AI technologies, Dathena delivers breakthrough, petabyte-scale solutions with unprecedented accuracy, efficiency and speed that build consumer trust in a digital world and ensures the “privacy and data security protection journey.



Deceptive Bytes
Prevention by Deception



Founded 2016



Employees: 1-10



Subsectors: Deception, Endpoint Security, Threat Management/Security Operations



Regions of operations: Global

Deceptive Bytes provides organisations and MSSPs with its Active Endpoint Deception platform that provides them with real-time prevention against unknown & sophisticated cyber attacks in an ever growing advanced threat landscape. The solution helps security & IT teams reduce alert fatigue, operational burden and overall costs, allowing organizations to increase security and to focus on their business rather than recovering from cyber attacks. Deceptive Bytes' technology uses malware's own defenses & techniques against it. The solution dynamically responds to malware as it evolves, based on the current stage of compromise, making malware believe it's in an unattractive/hostile environment to attack & reducing its motivation and by changing the outcome of the attack. Recognized as a Gartner Cool Vendor in 2019.

deepwatch



Founded 2019



Employees: 251-500



Subsectors: Threat Management/Security Operations, Managed Detection and Response, XDR, MSSP



Regions of operations: United States


deepwatch delivers managed detection and response services to protect organizations from cyber threats. The company helps secure the digital economy by protecting enterprise networks, everywhere, every day. deepwatch leverages its highly automated cloud-based SOC platform backed by a world class team of experts that protect customers' digital assets 24/7/365. deepwatch extends security teams and proactively improves cybersecurity posture via its squad delivery and proprietary maturity model. Many of the world's leading brands rely on deepwatch's managed security services.



-  Founded 2017
  Employees: 11-50
-  Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Email/Communication Security, Fraud Prevention, Employee Risk, Risk Assessment/Risk Management
-  Regions of operations: United States, Europe, India, Australia, Switzerland

Since its inception at Disney, Dragonchain's primary concern was to provide solutions to the problems that businesses face. The company has built a fundamentally interoperable system with built-in privacy, transparency, and security features. Dragonchain smart contracts can be written in any language to accommodate the existing skill set in an IT department. Its flexible platform can connect to any traditional system through a RESTful API, making the end product user-friendly at any technical skill level. Dragonchain is uniquely positioned to help secure and dramatically improve network security and functionality for companies. Its technology provides self-reporting real-time audits with audit trail proof and chain of custody and connects disparate systems and siloed networks from healthcare to FinTech.



-  Founded 2013
  Employees: 51-100
-  Subsectors: Security Operations(as-a-service)/ Threat Management/XDR/MDR/EDR/Application Security/Endpoint Security/Cloud Security
-  Regions of operations: Global. Office presences and focus in the United Kingdom and Australia.

e2e was founded on the premise that technology should be there to support Analysts, but not dictate their behaviour to them. This led to the development of e2e's SOC platform built for Analysts (Cumulo) and kept inhouse to ensure no reliance on a 3rd party roadmap and frees up e2e's and their customers Analysts to better detect and respond to incidents across e2e's ever-growing customer base. e2e focus on augmenting and integrating with existing customer technology as opposed to 'rip out and replace' and focus on building efficient security operations with existing customer people and teams; cybersecurity is a people and process challenge, technology is just an enabler. e2e delivers this through its SOC-as-a-Service XDR and MDR proposition.



-  Founded 2011
  Employees: 51-100
-  Subsectors: Application Security, Cloud Security, Fraud Prevention, Vulnerability Management
-  Regions of operations: EU, United Kingdom & Ireland, United States, Canada, APAC

Edgescan was founded in 2011 as a cyber security consultancy. The Edgescan SaaS was launched in 2015 with the aim to deliver high volume industrial penetration testing and vulnerability management. The Edgescan SaaS Accurately identifies vulnerabilities and exposures across the full stack. All threats are verified by cybersecurity experts, providing exploitable risk and remediation guidance. The company delivers on-demand assessments coupled with validation and support. The company engages with some of the worlds largest media, financial, Information technology and pharma companies globally.



COMPANY RESEARCH PROFILE



PRODUCTS NAMES:
VideoID, SmileID,
SignatureID and HelloID

Founded 2013
 Madrid, Spain
 www.electronicid.eu
 info@electronicid.eu
 Employees: 51-100
 Regions of operation: Global

KEY EMPLOYEES:



Iván Nabalón
Founder and CEO



José Villalba
COO

Subsectors: **Unique solution compliant in the whole EU for Remote Onboarding in 1 minute via Qualified Electronic Signature (QES)**

OFFERING

Electronic IDentification is a software provider created to lead the next generation of e-trust solutions and the only one proposing an end-to-end solution with a Qualified Electronic Signature based on a remote and asynchronous video identification, that allows a Digital Onboarding all over Europe in less than a minute.

Of its numerous awards, Electronic IDentification was recognised by Gartner as a “Cool Vendor” and creator of this new market segment for video identification.

PROBLEM BEING SOLVED

Digital Onboarding processes cause huge costs for companies in financial services, decreasing client conversion and increasing time to acquire new clients. Electronic IDentification offers a solution that can verify people in seconds and in real time with the same level of legal compliance as face-to-face identification, from any device and through any channel with an end-to-end solution valid across Europe in compliance with eIDAS and AML.

TECHNOLOGY

Electronic IDentification offers the only end-to-end solution valid in the EU market to perform a Customer Onboarding process in one minute, with a video identification and Qualified Electronic Signature.

PRODUCT DESCRIPTION

Electronic IDentification has created the first and **only end-to-end technology** that combines a **Qualified Electronic Signature (QES) with video streaming**, based on the most advanced machine learning and artificial intelligence algorithm, to identify people in seconds from any device and through any channel, offering a **complete solution in Europe**.

Their solution is creating a new services category on the Internet to identify customers remotely by providing the same technical security and legal compliance as face-to-face identification and works asynchronously.

Main differentiators:

- Electronic IDentification is a Qualified e-Trust Services Provider according to eIDAS and complies with the guarantees required at European level. Currently they are **the only provider offering a fully digital QES solution to onboard new users in European markets in less than 1 minute**. Everything under a standard API and patented.
- They have a technology called **HelloID** that allows banks and fintechs to develop any digital onboarding in hours.
- Their proposal offers an **omnichannel** solution that allows an optimal User Experience but also with a **universal** approach: in all channels, through all platforms and in any country.

TRACTION/GROWTH

- Electronic IDentification has more than 30 global partners including Salesforce, Accenture, PEGA Systems, Allfunds, Tessi, NTT Data.
- With headquarters in Madrid, Paris, Berlin, Lisbon, Mexico City and Hong Kong, Electronic IDentification is present in more than 35 countries. With over 700 active references in all market sectors, Electronic IDentification specialises in the financial, governments and travelling industry.
- The company works with leading financial institutions around the world including:



- Electronic IDentification has been recognised with numerous awards including Gartner Cool Vendor 2017, named as a RegTech 100 company in 2018, 2019, 2020 and 2021, 1st influencer in Europe for Digital Identity OWI 2018, Winner of Finance Titans 2016, Cybercamp Award 2015, Winner NTT Data Open Innovation Contest.

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.

Electronic IDentification: Why Digital Identity may eclipse Euro currency launch

Founded in 2013, Electronic IDentification have the most secure digital identification system on the market and the only patented technology with an end-to-end solution of Qualified Electronic Signature based on a remote and asynchronous video identification that enables digital onboarding all over Europe, in less than a minute.



While Electronic IDentification was established almost a decade ago, the company became commercially operative in 2016 – at a time when regulators had started to approve remote user identification. The firm claims it was created to lead the next generation of e-trust solutions and the currently are the only provider being able to propose an end-to-end solution with a Qualified Electronic Signature based on a remote and asynchronous video identification, that enables digital onboarding all over Europe in less than a minute.

Electronic IDentification founder and CEO Iván Nabalón said, “What truly inspired me to create Electronic IDentification was the challenge of meeting the new needs of regulated sectors such as finance,

telecommunications, or public administration and to apply and take advantage of existing technological advances in these sectors.”

“We saw that physical boundaries were going to change in the short term and that the offline and online worlds would eventually coexist and that at the same time many processes, although face-to-face, could be digitalised to offer a better user experience while at the same time, in the financial sector for example, acquisition costs could be reduced, and conversion rates increased.”

Electronic IDentification have created the first and only end-to-end technology to combine a QES with video streaming and is based on the ‘most advanced’ machine learning and AI algorithm to identify people in seconds from any device and through any channel. The company currently markets different solutions to help its customers with digital onboarding. To date, the company has over 30 global partners including Salesforce, PEGASystems and Accenture and has headquarters in Madrid, Paris, Berlin, Mexico City, Hong Kong and Lisbon.

The company is currently using QES to support the digitisation of social security in France with their technology. The firm added it has the only end-to-end solution that is compliant in the EU for remote onboarding within one minute through QES and the only one with a patented technology.

When asked what sets the company apart from other competitors in the space, Nabalón cited the firm’s vision of creating a strong digital identity through the usage of QES.

He added, “This strong digital identity (QES) can be used across Europe to identify 500 million citizens in the most demanding industries, such as the financial sector or governments. The strong digital identity is a game changer in the relationship with citizens and the digitalisation of the economy. It has taken us eight years to complete this vision through hard work that combines the development of complex technology and regulation.”

Nabalón compared the QES to the Euro, highlighting that the continent-wide currency served to unify the European single market to help facilitate exchanges between countries.

He continued, "The qualified signature has brought with it a common paradigm in the sense that what is valid in one country is also valid in another. A shared framework has been created that facilitates the exchange between member states and the companies that operate in them. A citizen will be able to create this strong digital identity in one state and be able to open a bank account or register with the public administration, travel across borders, or even vote in any member state."

Nabalón went on to emphasise how the expansion of QES will be a boost for companies looking to expand in Europe. He concluded, "We dare to say that this change is much more important than the homogenisation of the currency at the end of the last century."

Digital ID and market regulation

Due to the restrictions on face-to-face contact and working from home, Covid-19 has been a key driver of online and digital trends. To Nabalón, the push of the virus alongside developing technology have revealed the growing need for stronger digital identity, as with more people becoming more reliant on digital and online services, the risk of potential online attacks and hacks also grows - making the need for a bolstered online identity even stronger than before.

He said, "Digital identity has been around for many years. The difficulty is that it was not usable - it did not work on mobile phones, and it was very complex, it was not interoperable. It was also not accessible, as to obtain these digital identities you had to do it in person. The regulation we have been working on for years, the technology and the push of the Covid-19 crisis have revealed the need of this technology. Now, everything converges to make a strong but easy-to-use digital identity, accessible to citizens and very easy to use and integrate for the institutions that use it."

Nabalón stated the anti-money laundering regulation (6AMLD) and Europe's electronic identification and trust services (eIDAS) regulation have led the regulatory push to embrace such a user-friendly strong digital identity - adding Covid-19 has also driven it in "a huge way." He even claimed that "what we planned to happen in years is happening in months."

On whether regulations such as eIDAS and Second-Factor Authentication, which is part of PSD2, have helped improve online security consumers, Nabalón said, "I think we can say that having a Europe-wide



"The qualified signature has brought with it a common paradigm in the sense that what is valid in one country is also valid in another."

security framework and standardisation of processes is really helping to improve consumer security, but also to make consumers more confident in digital processes. This kind of regulation provides a common framework for not only consumers but also businesses to operate across Europe, creating a single market with common legislation."

Covid-19 recovery and future goals

While Covid-19 has created new pressing challenges for companies across the board, Nabalón remained relatively optimistic about the role digital identity technologies will play in the economic recovery.


He said, "Confinements have driven the need for such digital services in both private enterprise and public administration. The use of technologies, such as the mass use of a digital identity, will undoubtedly facilitate economic recovery: a recent study published by IE estimates that a state that extended digital identity in all its possibilities could increase its GDP by 13.6%".


"Imagine signing a mortgage remotely in a second, making a major investment, maintaining a relationship with the government or even voting in a referendum. This strong digital identity has enabled us to be truly digital and to be able to consume services in any country in the world. It is really being a disruptor of how relationships are going to be that need a certain amount of trust."


"Once the world returns to a level of normality, it is unlikely to go back to the ways of pre-pandemic. Companies and consumers alike are likely to continue to depend on digital services and with it, the level of acceptance, need and use of electronic identification and signature will only increase."


Looking to the future, Electronic IDentification claims it has set into the challenge to continue supporting various sectors - such as financial, public administration and insurance - as they digitise their processes both online and offline. This, Nabalón affirms, will help companies increase their conversion rates and reduce their acquisition and onboarding costs going forward. ●



 Founded 2017


 Employees: 11-50

 Subsectors: Employee Risk, Risk Assessment/Risk Management


 Regions of operations: North America, Australia, Europe, Asia

Elevate Security is the first Human Attack Surface Management platform. It was started by two industry veterans, Robert Fly and Masha Sedova, who have spent 20+ years each defending enterprises against sophisticated attackers. During that time they realized that employees were the biggest threat to running a successful security program and that simply training users and responding to their incidents wasn't a winning strategy. With that knowledge and experience building out successful solutions to that challenge, they built Elevate Security which enables enterprises to reduce the number of cyber incidents by driving benchmarked visibility into human risk and actively reducing it through proactive, tailored security controls and focusing their security investments on the areas of greatest exposure.

E N C L A V E

 Founded 2018

 Employees: 1-10

 Subsectors: Zero Trust, Endpoint Security, Cloud Security, Network Management, Identity & Access Management, Data Security/Data Governance

 Regions of operations: United Kingdom, EU, United States

Enclave is a scale-up company with a growing international customer base. The company's investors include private individuals, Swansea University, Start Up Bootcamp Amsterdam and Next Big Thing Berlin. Its patented technology radically disrupts the current mechanisms for managing network infrastructure, saving customer time and money by simplifying and automating network management using Zero Trust principles. Currently secure network connections rely on a "connect, then authenticate" architecture. This means that often systems that should be entirely private are visible on the public internet for anyone to connect to. Enclave reverses that architecture to "authenticate, then connect". The result is that private systems are invisible to the public internet. Organisation can operate invisible, stealth overlay networks that are less susceptible to discovery, targeting and attack.



 Founded 2016


 Employees: 11-50


 Subsectors: Data Security/Data Governance

 Regions of operations: United States, United Kingdom, Europe


Enveil is a pioneering Privacy Enhancing Technology company protecting Data in Use to enable secure data usage, collaboration, and monetization. Enveil's business-enabling and privacy-preserving capabilities for secure data search, sharing, and collaboration protect data while it's being used or processed – the 'holy grail' of data encryption. Defining the transformative category of Privacy Enhancing Technologies (PETs), Enveil's homomorphic encryption-powered ZeroReveal® solutions allow organizations to securely derive insights, cross-match, search, and analyze data assets without ever revealing the content of the search itself or compromising the security or ownership of the underlying data. Enveil is a 2020 World Economic Forum Technology Pioneer and its award-winning, market-ready solutions are delivering nation-state level protection to the global marketplace. Learn more at www.enveil.com.

eSENTIRE

 Founded 2001


 Employees: 251-500

 Subsectors: Threat Management/Security Operations, Endpoint Security, Cloud Security, Risk Assessment/Risk Management, Managed Detection and Response

 Regions of operations: Canada, United States, United Kingdom, Ireland

eSentire Inc is the global leader in Managed Detection and Response (MDR) cybersecurity services and keeps organisations safe from constantly evolving cyberattacks that technology alone cannot prevent. The company's Atlas Extended Detection and Response (XDR) cloud platform is the foundation for all eSentire MDR Services. The Atlas platform gathers, analyzes and correlates data from across hundreds of individual customers, helping to identify emerging threats, and then leveraging those learnings to protect all eSentire customers. eSentire's award-winning security services consist of the platform's patented, multi-signal correlation capabilities, the company's 24x7 threat monitoring, real-time cyber hunting, and automated threat response capabilities. Protecting more than \$6T in AUM, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

EXONAR

 Founded 2007

 Employees: 11-50

 Subsectors: Data Discovery, Data Mapping, Data Classification, Data Compliance, Information Security

 Regions of operations: United Kingdom, EMEA, United States


Exonar is the world-leading data discovery company building the crucial software financial services organisations use to discover their data at scale, keep it safe and realise its value. Every organisation faces the same problem; knowing what data they've got, and where it is stored. They are holding significant risk in a legacy, unmanaged and unstructured data stores representing a major security and regulatory breach potential. Exonar Reveal solves this by finding and revealing billions of items of structured and unstructured information; enabling businesses to 'know the truth' about their data in order to reduce risk, increase data management efficiencies and uncover business value. Founded in 2007, the company is backed and funded by Beringea, Amadeus Capital Partners, Winton Ventures and Downing Ventures. In 2021, Exonar was recognised by Tech Nation as one of the fastest growing tech scale-ups in the UK and securing additional funding from its investors.

ExtraHop

 Founded 2007

 Employees: 251-500

 Subsectors: Threat Management/Security Operations, Cloud Security, Network Security (Network Detection and Response)

 Regions of operations: North America, EMEA, APAC

ExtraHop, the leader in cloud-native network detection and response, is on a mission to arm security teams to stop breaches. Our Reveal(x) 360 platform combines the power of cloud intelligence with the simplicity of SaaS to help security teams eliminate blind spots and detect threats other tools miss. Built on cloud-scale AI, Reveal(x) 360 decrypts and analyzes all network and cloud traffic in real time to expose risks, from internal threats to external attacks. With this approach, we help the world's leading enterprises including Fiserv, BECU, and Regions Bank stop breaches 84% faster.



COMPANY RESEARCH PROFILE



PRODUCT NAME:
Firework

- Founded 2017
- Montreal, Canada
- www.flare.systems
- hello@flare.systems
- Employees: 11-50
- Regions of operation:
Canada, United States, Germany

KEY EMPLOYEES:



Mathieu Lavoie
Co-founder and CEO



Yohan Trépanier Montpetit
Co-founder and CPO



Israël Hallé
Co-founder and CTO

Subsectors: **Threat Management/Security Operations, Data Security, Fraud Prevention, Employee Risk, Digital Risk Protection**

OFFERING

Flare Systems works with enterprise customers and security service providers to help organizations improve their security posture by providing a comprehensive view of an organization's data exposure. Through real-time monitoring and prioritized alerts, defensive security teams and threat intelligence teams are able to detect information disclosures caused by human error and reduce the Mean-Time-To-Remediation for these incidents.

PROBLEM BEING SOLVED

Large organizations struggle with the detection and prioritization of external, high-risk technical and data leakage.

Employees and IT consultants tend to use public tools to collaborate and share technical information such as API keys, access tokens, and credentials. This increases the attack surface of an organization, due to the additional information available to a malicious actor during the initial access phase of an attack. This is an increasing problem driven by a growing remote workforce.

TECHNOLOGY

Flare Systems has developed strong AI-driven technologies to collect, classify and analyze data efficiently. Natural Language Processing (NLP) is used to autonomously understand the content of text documents and add valuable data points used for prioritization. Advanced Big Data algorithms have also been developed to quickly parse, store, analyze and retrieve billions of documents collected over four years on the dark, deep and clear web.

PRODUCT DESCRIPTION

Firework is a SaaS platform that identifies, enriches, prioritizes, and remediates technical data leaks and information disclosures. By collecting data on a wide range of sources on the dark, deep and clear web, Firework quickly identifies any security issue based on key identifiers related to an organization's critical assets. The product collects thousands of data points and structures them into an easy-to-use, searchable platform that reduces noise and false positives.

The system leverages a 5-point scoring system, AI and machine learning to enrich and prioritize findings. Security teams can focus on highly relevant alerts while the platform automates the process, including support for remediation. Firework also provides additional insights on malicious actors and their tactics to help with companies' mitigation strategy. A straightforward and efficient portal, combined with an alerting system, integrations, and a powerful API, Firework provides all the tools for SOC, defensive security, and threat intelligence teams.

TRACTION/GROWTH

- Flare Systems works with leading organisations in North America including (among others):



- The company has established partnerships with MSSPs such as Vars and In Fidem (ATOS), and have included the Firework product into their offer, so they can use their technology for cyber threat detection for their customers.
- Flare Systems is building a machine learning engine to contextualize and prioritize threat intelligence based on user feedback.
- The company is backed by leading investors such as:



How Flare Systems helps businesses reduce data leakage and boost their cyber hygiene



FLARE
SYSTEMS

With the escalation of cloud-based solutions and third-party services, protecting data has become increasingly complex. Preventing sensitive information from getting into the wrong hands before it leaves your organisation is more important now than ever.

Flare Systems CEO Mathieu Lavoie highlighted two major causes behind data leaks involving a company's processes and plans as well as employee and customer personal information. First, malicious actors are actively stealing data to resell it for profit on illicit markets such as the dark web. The second cause is data leaked following human errors by employees and partners. The global pandemic prompted employees to share and store information with third-party cloud services, making more data vulnerable for accidental leaks. According to [Varonis](#), nearly two-thirds of financial services companies have over 1,000 sensitive files open to every employee.

Consequently, using data leak detection and employing a robust digital risk protection strategy is key if organisations want to reduce the risk of accidental data exposure, Lavoie said. "Since malicious activity is not the driving factor behind human error, no known signature or pattern can be detected by most available tools, leading to an increase in an organisation's attack surface. It's mandatory for every company that has a digital presence to understand and control the information, making sure that the cybersecurity company you're working with has the capacity in place to keep the company's data secure."

Why use a cybersecurity expert?

Despite cybersecurity tools being easily available, companies are dragging their feet to secure their systems adequately. With new threats emerging every day, the risk of not securing files is more dangerous than ever, especially with

a remote workforce. The SolarWinds incident, GitHub bugs and Microsoft's disclosure of several critical vulnerabilities should serve as a wake-up call to businesses.

This laissez-faire attitude stems from the fact that only incumbents were targeted by online thieves up until a few years ago. Lavoie said, "Back in 2017 when we launched Flare, cybersecurity was a concern for larger enterprises. Witnessing a data breach was big news then. Sadly, it's not unusual today and with breaches happening from time to time, we are getting used to hearing smaller businesses falling prey as well."

Alongside financial and reputational damage, companies must be aware of global regulations. As a result, Lavoie said that "onboarding a cybersecurity company to overlook these should be a no-brainer." For enterprises with limited resources, managed security service provider (MSSP) and managed detection and response (MDR) services may help defend against complex attacks, source code leaks and protect brand reputation, he added.

How Flare protects its clients

Flare was launched to help financial institutions avoid security threats by automating data monitoring before a hack happens. Flare's flagship product Firework first detects technical data leaked online, then deploys proprietary techniques and algorithms to regroup and enrich the results. This capability enables prioritisation of alerts and supports remediation for most critical issues.

Lavoie stated the software automatically structures, organises and normalises millions of data points from darknet sources such as broadcasts of stolen information, private forum discussions, chat posts and cryptocurrency transactions, and combines it with its research in criminology insights. Given that source code, API Keys and technical leaks can go undetected for months before a company is finally aware of it, the real-time alerts they provide help organisations get ahead of cyber threats. "The goal is to take a holistic approach to the complete attack chain with tools that prevent and mitigate attacks on each link in the communication chain of criminals," he said.

A core differentiator of Flare is that it detects data on third-party websites before it becomes a doorway for cybercriminals. "Technical leaks expose your company's most sensitive secrets such as passwords and access keys. If either is leaked, it could enable malicious actors to penetrate your corporate network and steal sensitive and confidential information."

Most companies need to reassess their cybersecurity approaches to be more proactive. He concluded, "Businesses must understand it is cheaper to fix a security issue and rather prevent it than to later spend money on remediation and mitigation, only then will they get a better understanding why cybersecurity should be a priority." ●



A Leading Canadian Bank Chooses Flare Systems to Prevent Accidental Technical Leaks on Github

Case Study

THE CUSTOMER



Top 7 banks
in Canada



Over 400
branches



Over 25k
employees



Over \$8B in 2020
Annual revenue



Over \$300 billion
in assets

THE BANK PAIN POINTS

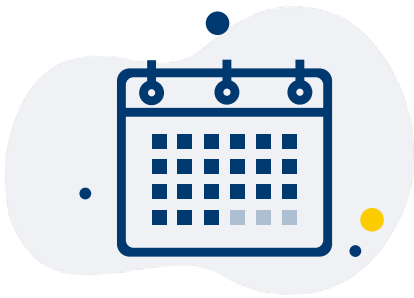
The bank needed to immediately improve technical leak detection on external public platforms, reduce response time, and save resources. Its cyber threat intelligence (CTI) team needed to reduce time spent on analysis and data collection to invest more in remediation actions. It also needed to make sure that it caught and had time to investigate all cyber threats. They came to us with 4 major pain points to resolve:

- **Confidential & sensitive technical leaks** were identified on version control tools and source code repositories due to the size of the development teams working on a variety of tools (ex: Github, Gitlab, Stack Overflow)
- Mean Time to Identify was measured in days and reducing this time to hours would limit the impact of the leaks.
- The coverage of the external threat landscape was limited
- Proprietary tools are often not user-friendly and need regular maintenance which took up significant time and resources, and affected real-time monitoring during downtime. Moreover, the knowledge of how these tools work and the ability to maintain them was at risk each time key personnel left the CTI team.

SOLUTION

Firework, Flare Systems' solution, has been deployed to detect source code leaks by automating the entire monitoring process and by expanding coverage. Firework replaced the bank's manual review process and sped up the delivery of real-time notifications on potential threats. The search functionality easily scans Github to detect technical leaks that may have been exposed online. Analysts were onboarded on Firework in a matter of hours and no integration was required. The bank's employees were able to set up custom alerts in minutes and did not have to share any bank or customer confidential information to receive tailored and prioritized alerts.

RESULTS



Firework saved each analyst 3 days of work per month



MTTI response time reduced from 24 hours to less than 1 hour



“Firework helped us reduce time we spent on in-house crawling software, increase our coverage and focus our time not on collecting data, but analyzing the results.”

-Threat Intelligence Manager at the bank

OUTCOMES



Run enhanced and customized queries: With its flexible identifier-based alert system, Firework goes further than simple keyword matching. Firework can run custom regexes and queries that cannot be run directly in the Github search function.



Expand repository coverage: Firework increased search coverage by not only monitoring recent commits, but scrutinizing a repository's entire commit tree.



Reduce noise: Firework reduced the number of alerts and noise CTI teams had to handle and help them prioritize by regrouping alerts based on repositories, projects, developers and items with the same content. Specific keywords could also be blacklisted through Firework's user-friendly web interface to further reduce noise.



Centralize functionality: Firework seamlessly integrated with the bank ecosystem and did not require any workflow changes. By centralizing functionality, it successfully reduced the number of tools involved in daily operations.

FUTURAE



Founded 2016



Employees: 11-50



Subsectors: Strong Customer Authentication, Threat Management/Security Operations, Identity & Access Management, Application Security, Cloud Security, Fraud Prevention



Regions of operations: Austria, Benelux, France, Germany, Italy, Switzerland, United Kingdom, IE

Users see login to your platform as a hurdle? Your help-desk costs are getting out of hand due to complicated enrollment and login methods? Your authentication is inflexible and does not cover all the cases of your multi-faceted user groups? With Futurae's innovative authentication and fraud detection platform, end-users can enjoy seamless secure login experience, signing transactions on mobile and web apps and via skills on their smart speaker devices. Futurae's modular API's allow for rapid design iterations. Companies benefit from convenient ways of enrolling or securely migrating end-users to a new device. This in turn reactivates the users' online services instantly, without any support problems. As around 40% of all support requests are due to authentication problems, Futurae can support companies by helping them massively save on operational and indirect costs. Futurae works with over 100 renowned international companies in the financial services, health, education and the public sector.



Founded 2012



Employees: 101-250



Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Application Security, Fraud Prevention



Regions of operations: United States, United Kingdom, Canada, Germany, France, Singapore

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. The company has the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today it verifies the humanity of more than 10 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.



Founded 2015



Employees: 11-50



Subsectors: Threat Management/Security Operations, Cloud Security, Email/Communication Security, Risk Assessment/Risk Management, Network Security




Regions of operations: United States, Canada, Australia, Europe, Asia, Latin America

HYAS, a First Nations word meaning "great and powerful," is the world's leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS has constructed what is arguably the world's largest data lake of attacker infrastructure including unrivalled domain-based intelligence. HYAS leverages its infrastructure knowledge to deliver a generational leap forward in cybersecurity. HYAS provides the industry's first security solution that integrates into an organization's existing security technology stack to proactively detect and mitigate cyber risks before attacks happen, and to identify the infrastructure behind the attacks. Threat and fraud response teams use HYAS to hunt, find, and identify adversary infrastructure while enterprises can proactively block both known and not-yet-launched phishing and ransomware attacks at the network layer.



 Founded 2018


 Employees: 11-50


 Subsectors: Risk Assessment/Risk Management, Governance, Risk and Compliance



 Regions of operations: United States of America, Benelux


Hyperproof has built innovative compliance operations software that helps organizations gain the visibility, efficiency, and consistency IT compliance teams need to stay on top of all of their security assurance and compliance work. With Hyperproof, organizations have a single platform for managing daily compliance operations; they can plan their work, make key tasks visible, get work done efficiently and track progress in real-time. Organizations using Hyperproof are able to cut the time spent on evidence management in half, using intuitive features, automated workflows, and native integrations. The platform also provides multiple ways for an organization to track risks — including a central risk register that documents risk mitigation plans and maps risks to existing controls, and a vendor risk management solution makes vendor due diligence, vendor risk assessments, planning, contract review, ongoing monitoring, and oversight as efficient and automated as possible.



 Founded 2017


 Employees: 1-10


 Subsectors: Identity & Access Management, Data Security/Data Governance, Fraud Prevention, Risk Assessment/Risk Management



 Regions of operations: Global


iComply is a global regtech software provider based out of Vancouver, British Columbia that helps companies improve their privacy, cyber-security, and identity access management resolution - up to or surpassing the regulatory thresholds for each jurisdiction in which a client operates. iComply has developed a new method of verifying the legal identity of both a natural person or a legal entity that combines artificial intelligence and edge computing to securely gather, validate, and encrypt user identity data and supporting documents before the data ever leaves their device. The company's iComplyKYC products provide secure, financial-grade KYC software to financial services, law firms, eCommerce, fintech, payments, capital markets, and other industries.



 Founded 2016



 Employees: 11-50



 Subsectors: Identity & Access Management


 Regions of operations: Global


ID R&D is a NY-based software company with global technological leadership in voice biometrics, voice and face liveness detection, and continuous multimodal authentication. ID R&D breaks through in a crowded cybersecurity market with science-driven biometric products that enable frictionless authentication while dramatically increasing security in mobile apps, web apps and conversational interfaces like chatbots. ID R&D's AI-driven capabilities include IDLive Face, a single image, passive facial liveness product that detects spoofing attacks during remote onboarding and authentication without the user having to do anything. Liveness detection occurs in the background, making it easy and effortless for the customer while preventing fraudsters from knowing when it's happening. The solution is ISO/IEC 30107-3 compliant, having passed iBeta Level 1 and Level 2 testing with a perfect score.



 Founded 2011

 Employees: 101-250


 Subsectors: Identity & Access Management


 Regions of operations: Global

IDmission provides solutions that orchestrate digital transformations for companies relying on identity and ID verifications. The company utilises standards-compliant security, passive liveness biometrics, AI, and its industry expertise to help organisations create an effortless end-to-end customer journey. The company provides best-in-class identity solutions that integrate directly with a client's existing workflows. Whether an organisation is looking for document verification, identity authentication, frictionless liveness detection, or deduplication, IDmission has a product to fit those needs. IDmission provides more than just identity solutions, the company orchestrates digital transformations for applications relying on identity and ID verifications. Solutions include CIAM, client and employee onboarding, and financial-based applications.



 Founded 2017


 Employees: 101-250

 Subsectors: Threat Management/Security Operations, Employee Risk, Risk Assessment/Risk Management

 Regions of operations: United Kingdom, North America


Immersive Labs empowers organizations to equip, exercise, and evidence cyber skills capabilities. With the Immersive Labs platform, organizations can align human capabilities against actual cybersecurity risks, battle-test teams against real-world threats and crises, measure their cyber expertise and build security culture in development and engineering teams. The company is backed by Goldman Sachs and Summit Partners and its customers include some of the largest companies in the world across financial services, healthcare, and government, amongst others.




 Founded 2016



 Employees: 11-50

 Subsectors: API Security

 Regions of operations: United States, Europe, APAC

Imvision enables enterprises to open up without being vulnerable. It's about making sure that every interaction between people, businesses, and machines can be trusted. Imvision's platform helps enterprise security leaders, including Fortune 500 companies, to discover, test, detect and prevent API breaches, automatically giving every API the protection it deserves - at any scale, across the lifecycle. Using NLP-based technology to analyze each API's unique dialogue and understand the application's behavior, Imvision supports security and development teams to stay ahead of attackers, focus on what really matters and minimize time-to-remediation.





Founded 2018

Employees: 11-50

Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Email/Communication Security, Fraud Prevention, Employee Risk, Risk Assessment/Risk Management

Regions of operations: North America, Brazil, Germany, APAC

Infiltron is your automated cybersecurity workforce. Infiltration doesn't just detect, they prevent and respond in real-time. Infiltron's solution is a combination of traditional detection and prevention tools activated before a compromise occurs, plus a post-compromise iterative process of searching for new threats missed by automated tools, can be highly effective. Infiltron maximizes the value of clients security solutions by delivering fully managed, individually tailored ongoing detection, prioritization, investigation, and response. Countering targeted attacks requires extensive experience as well as constant learning. Infiltron's customers can use the functionality of the dashboard to centrally initiate recommended response actions themselves or authorize Infiltron to automatically launch remote incident response for certain types of incidents.





Founded 2015

Employees: 1-10

Subsectors: Data Security/Data Governance, Endpoint Security, Cloud Security, Mobile Security

Regions of operations: United States, India, Middle East, Europe

KAPALYA empowers businesses and their employees to securely store sensitive files at-rest and in-transit across multiple platforms through a user-friendly desktop and mobile application. This ubiquitous encryption solution protects all your corporate data by seamlessly encrypting files on: End-points computers/mobile devices; Corporate servers and public cloud providers; With KAPALYA, users have the ability to share encrypted files across multiple cloud platforms; Integrated with Box, Amazon S3 and Microsoft Azure; Data recovery after a ransomware breach WITHOUT paying any ransom and WITHOUT any data leakage.





Founded 2018


Employees: 11-50

Subsectors: Threat Management/Security Operations, Risk Assessment/Risk Management

Regions of operations: Global


Formed in 2018, with a team consisting of some of the most distinguished leaders in the world of Internet banking, fraud protection, and cyber security; KYND has created revolutionary technology designed to make cyber risk management simple, easy to use, and affordable which has led to KYND being chosen and used by insurers, brokers and their clients globally. KYND's innovative, industry first and proprietary cyber risk management technology enables businesses to easily monitor and understand the cyber risks they face, take action when necessary and get real-time alerts for future risks.



 Founded 2015


 Employees: 11-50


 Subsectors: Application Security


 Regions of operations: United States, EU, APAC


L7 Defense is focused on helping customers secure their applications against the growing risk of exposing APIs to cyber-attacks. APIs have become the ultimate means for sharing data and integrating between applications. However, APIs function outside the “jail” of existing applications protection policies and are very sensitive to data manipulation, theft and operational damage. They present the main cyber security threat to companies today. L7’s team is comprised of experts in bio-informatics, machine learning, enterprise architecture and cyber security technologies. Inspired by the self-learning intelligence of the human “innate” immune system, the team developed an innovative AI solution that protects APIs, autonomously & INLINE, from cyber threats.



 Founded 2015

 Employees: 101-250

 Subsectors: Threat Management/Security Operations, Employee Risk, Risk Assessment/Risk Management


 Regions of operations: United States, Canada, United Kingdom, APAC


LogicGate is a leading provider of cloud-based solutions for automating governance, risk and compliance (GRC) processes. LogicGate empowers customers to transform disorganized risk and compliance operations into agile enterprise risk management programs, tailored to their business needs. Its proprietary Risk Cloud™ platform, an end-to-end suite of risk management solutions, blends the right mix of flexibility and out-of-the-box functionality, enabling organizations to manage their risk with confidence. Over 200 companies of all sizes and industries rely on LogicGate to accurately assess, monitor, action, and, when needed, rapidly pivot GRC processes, without the support of consultants or corporate IT. The Chicago-based company has been named a leading GRC Software Platform on the G2 GRC Grid for ten consecutive quarters, and was awarded Best Security Innovation in a SaaS Product by the SaaS Awards. LogicGate was also named in Gartner’s 2020 “Magic Quadrant for IT Vendor Risk Management Tools”.



 Founded 2017

 Employees: 11-50

 Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Endpoint Security, Cloud Security, Email/Communication Security, Fraud Prevention, Employee Risk, Risk Assessment/Risk Management

 Regions of operations: Global

LogSentinel SIEM is a cutting-edge next-generation Security Information and Event Management (SIEM) system offering simplicity, predictability, and innovation like nobody else on the market. By leveraging the latest innovations in technology including blockchain and machine learning, it helps financial organizations of all sizes to completely eliminate their blind spots and significantly reduce the time and cost of incident detection, investigation and response. Compared to the alternatives, LogSentinel provides very strong log integrity and privacy, flexible and practically unlimited retention, and simple and predictable pricing, based on the number of active users in an organization, rather than fluctuating metrics such as volume or events per second.

mimecast™



Founded 2003



Employees: 1,001-5,000



Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Cloud Security, Email/Communication Security, Fraud Prevention, Employee Risk



Regions of operations: United States, Canada, United Kingdom, Germany, Nordics, Netherlands, Belgium, Middle East, South Africa, Australia

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. The company built an intentional and scalable design ideology that solves the number one cyberattack vector – email. Mimecast’s Email Security 3.0 strategy helps IT and security professionals achieve a new and more comprehensive form of protection against email attacks by advancing from perimeter email security to a comprehensive, more pervasive discipline. Mimecast will continue to incrementally build capabilities and integrate with other security investments to defend organizations against email born attacks, fraudulent brand activity, and compliance challenges. The company is committed to continuously making things easier and more cost effective for its more than 36,000 customers around the world.

NAPIER



Founded 2015



Employees: 101-250



Subsectors: Anti-Money Laundering, Compliance Management



Regions of operations: Global

Napier is a new breed of AML and trade compliance tech provider. Its Intelligent Compliance Platform is transforming compliance from legal obligation to competitive edge. All Napier products are built on its third-generation intelligent compliance platform which can be delivered via public cloud, private cloud or on-premise. Its suite of tools dramatically reduce both false positives and false negatives and empower compliance teams to make validated decisions with unprecedented speed and accuracy. Napier’s Client Activity Review solution acts as a horizontal layer, straddling existing Customer Lifecycle Management (CLM), KYC screening and transaction monitoring systems. It aggregates data from any and/or all sources and measures the extracted data against the policy-based rule set. AI is used to filter results and achieve intelligent pattern recognition.

NetGuardians



Founded 2011



Employees: 51-100



Subsectors: Fraud Prevention, Employee Risk



Regions of operations: Switzerland, Singapore, Kenya, Poland

NetGuardians is an award-winning Swiss FinTech helping financial institutions in over 30 countries to fight fraud. More than 60 banks, including UOB and Pictet & Cie, rely on NetGuardians’ 3D artificial-intelligence (3DAI) solution to prevent fraudulent payments in real time. NetGuardians is the only company to reduce fraud from day one without stopping banks’ customer transactions. Banks using NetGuardians’ software have detected significantly more fraud cases, whilst reducing false positives by 83 percent and spending up to 93 percent less time investigating fraud. NetGuardians was listed as a representative vendor in Gartner’s 2020 Market Guide for Online Fraud Detection and a Category Leader in Chartis’ 2021 Enterprise Fraud Report. Headquartered in Switzerland, NetGuardians has offices in Singapore, Kenya, and Poland.



-  Founded 2018
-  Employees: 1-10
-  Subsectors: Threat Management/Security Operations, Cloud Security, Threat Detection & Response
-  Regions of operations: North America, EMEA, United Kingdom, APAC, ANZ

Netography delivers real-time protection against millions of network-based threats across an organization's entire infrastructure, both on-premise and in the cloud. As a result, network and security teams can have shared visibility into their security posture and effectiveness of their security controls at any and every point in time. Netography's Network Detection and Response provides network visibility, encompassing cloud and on-premises environments. With the network-wide visibility that Netography delivers, organizations can protect themselves, via instant and automated remediation, against a broad set of security threats, resulting in a 90-percent reduction in MTTR (mean time to resolution). Netography helps companies verify the effectiveness of their existing security and tools, share the same data in real-time across NetOps and SecOps teams, and easily protect their entire infrastructure as they scale, without adding expensive hardware.



-  Founded 2016
-  Employees: 501-1,000
-  Subsectors: Identity & Access Management, Cloud Security, Fraud Prevention, Log management, SIEM optimization
-  Regions of operations: Global


One Identity, a Quest Software business, helps organizations achieve an identity-centric security strategy with a uniquely broad and integrated portfolio of identity management offerings developed with a cloud-first strategy including AD account lifecycle management, identity governance and administration and privileged access management. One Identity empowers organizations to reach their full potential, unimpeded by security, yet safeguarded against threats without compromise regardless of how they choose to consume the services. One Identity and its approach is trusted by customers worldwide, where more than 7,500 organizations use One Identity solutions to manage over 125 million identities, enhancing their agility and efficiency while securing access to their systems and data – on-premise, cloud or hybrid.




-  Founded 2016
-  Employees: 1-10
-  Subsectors: Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Email/Communication Security, Fraud Prevention
-  Regions of operations: Europe, United States


OneVisage is a Swiss cyber-security company founded in 2013 by 3D computer vision experts, software veterans and executive managers. The company develops Transversal Strong Customer Authentication technologies and white-labelled solutions for large software/hardware integrators and Identity and Access Management (IAM) providers. Unlike any alternatives, OneVisage offers ethical, client-edge biometric solutions that performs verification (1 to 1) and complies with the strictest data privacy and protection laws, including GDPR (article 25), CCPA or CNIL in France (2019, article 7, template type 1).



 Founded 2015


 Employees: 51-100

 Subsectors: IoT/Connected Device Security


 Regions of operations: United States, United Kingdom/Ireland, Canada, Germany, France, Australia, Hong Kong, Singapore, Taiwan, New Zealand


Digital transformation has led to the explosive growth of connected devices. While some devices support endpoint security agents, the vast majority of devices are un-agentable or are newer, more vulnerable IoT, IoMT and OT devices that they are not built with security in mind, cannot be patched easily and often support outdated operating systems. Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT, with an agentless approach. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance, identify cyberattacks or lateral movement, and accelerate Zero Trust initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures.



 Founded 2014

 Employees: 51-100

 Subsectors: Risk Assessment/Risk Management

 Regions of operations: Germany (HQ), Poland, Austria, United States

Palturai addresses regulatory and risk management challenges by providing an innovative way where it views customers and business partners as interconnected nodes in a vast global network. This new way of looking at legal and business relationships can be applied to compliance, risk & fraud, research, sales, and data quality use cases utilizing trustworthy data from government and other public sources. The Palturai BusinessGraph connects all players in the economy to a large network based on public data. Powerful algorithms calculate relationships between entities in the solution, and the Graph Intelligence Engine enables users to interact with the data. Users match company business partners to the BusinessGraph and see in an easy-to-use graphic representation how they are connected. This gives organisations the power to discover paths, structures, and cross-connections which then can be used to enhance opportunities and reduce risks.



 Founded 2017





 Employees: 11-50

 Subsectors: Application Security, Cloud Security, Open Source Security

 Regions of operations: Global





Patchstack is leading the popular initiative called Patchstack Red Team to build an active security community behind WordPress. Patchstack maintains the free and open WordPress vulnerability database and provides automatic virtual patching for websites. Its goal is to eliminate the most common problem of WordPress security - plugin and theme vulnerabilities. Additionally, Patchstack helps plugin developers with professional security audits and penetration testing services.

PICUS

-  Founded 2013
-  Employees: 101-250
-  Subsectors: Threat Management/Security Operations, Breach & Attack Simulation, Red & Purple Teaming, Cybersecurity Assessments, Vulnerability Management, Endpoint Security, Risk Assessment/Risk Management, Network Security, Application Security
-  Regions of operations: United States, EMEA, APAC

Picus Security is a leading Breach and Attack Simulation (BAS) vendor, offering a transformative Security Validation solution that helps organizations gain proactive cyber defense capabilities. It continuously challenges organizations' cyber-security controls using over 10,000 up-to-date real threat scenarios. Picus Security Control Validation Platform also provides insights to build the right security strategy while revealing defense gaps and detection shortcomings before a real incident takes place. As of April 2020, over 250 large enterprises in the financial services industry use the Picus Platform as part of their cybersecurity operations. Gartner named Picus a "Cool Vendor" in 2019. In 2020, Frost&Sullivan cited Picus as one of the most innovative BAS players with its 21.7% market share in EMEA and consistent triple-digit growth rates. Raised \$8.2M to date (of which \$6.5M in Series A), Picus is a Series-A startup supported by Earlybird Capital and ACT.

pindrop[®]

-  Founded 2011
-  Employees: 251-500
-  Subsectors: Fraud Prevention, Voice Biometrics, Authentication
-  Regions of operations: United States, United Kingdom

Pindrop solutions are leading the way to the future of voice by establishing the standard for identity, security, and trust for voice interactions. Pindrop solutions protects some of the biggest financial institutions and other enterprises in the world using patented technology that extracts intelligence from the calls and voices encountered in the contact center. By doing so, it helps them to detect fraudsters and authenticate genuine customers using real-time fraud intelligence, enabling its clients with the ability to measure risk across every call. This provides an incremental reduction of fraud and operational costs, all while improving customer experience and protecting brand reputation. With solutions that serve both the back-end and front-end, Pindrop allows its customers to improve overall organizational security posture by defending against the latest fraud tactics and offering a cross-channel view of potential fraud across the enterprise.

PQSHIELD

-  Founded 2018
-  Employees: 11-50
-  Subsectors: Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Email/Communication Security, Risk Assessment/Risk Management
-  Regions of operations: Global

Originating from the University of Oxford, PQShield is a world leader in Post-Quantum Cryptography. The company provides quantum-secure cryptographic solutions for software, software/hardware co-design and data in transit. This is particularly important where long lifecycle, performance and lasting confidentiality are a priority, now and for years to come. PQShield helps customers transition their product lines from legacy RSA and Elliptic Curve cryptography to quantum-secure standards by offering ready-made and tailored IP for secure elements, IoT firmware, PKI and server technologies, and end-user applications.

COMPANY OVERVIEW

At PRODAFT, in response to the thousands of cyber incidents, cybercriminal fingerprints, and malicious activities we see on a daily basis, we have developed our own "to-the-point" technologies to prevent cyber threats.

Because attackers have no rules and are continuously developing new methods, the battle against cyber incidents must always be one step ahead of any potential threats. Focusing on the here and now makes it very challenging to keep pace with cybercrime.

To ensure the proactive nature of our solutions, our operational cycles are constantly reviewed and adapted to newly emerging challenges within the cyber arena.

"Repel cyber-attacks with Swiss precision"

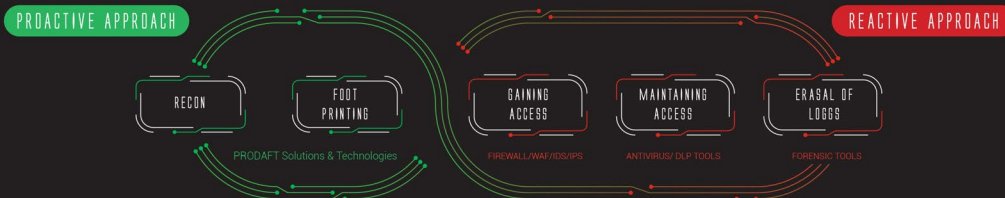


Since 2012, PRODAFT has been a key solution provider for various critical sectors, including banking and finance, fintech, aviation, insurance, IoT, defense, and telecommunication. Due to the "customized" approach of our solutions, client turnover of PRODAFT is virtually nil, as we recognize the priorities and requirements unique to each industry.

Our commitment in this regard is the main reason behind PRODAFT's popularity among high-profile organizations.

STEPS OF A "SUCCESSFUL CYBER ATTACK"

PRODAFT stops cyber-attacks in their tracks.



OUR VISION

PROactive Defense Against Future Threats

OUR MISSION

To protect citizens, businesses, and governments from major security threats by providing timely and accurate information.

Our solutions and services are preferred by organizations from numerous sectors, such as banking and finance, insurance, telecommunication, aviation, e-commerce, insurance, blockchain companies, IoT producers, and public institutions. Our team has the knowledge and experience to understand the technical structures and needs of companies across a variety of structures and business models. We tailor our services to each client's unique needs, as we know there is no magic piece of hardware or software that can mitigate the ever-changing dynamics of cybercrime.

Although cyber security is a niche and developing business area, we believe that an interdisciplinary team composed of cyber security experts is crucial for providing the best services and solutions. That's why we work with the finest technical talents in different areas of cyber security, globally recognized in their respective areas of expertise.

QUICK FACTS

YEAR FOUNDED: 2012

HEADQUARTERS:
YVERDON-LES-BAINS / SWITZERLAND | ISTANBUL / TURKEY



+100 CUSTOMERS IN 3 CONTINENTS:
EUROPE, ASIA, USA



Awarded as one of Europe's 100 most successful technology initiatives



Awarded Best Security Product of the Year for U.S.T.A. platform



National "One to Watch" winner representing Switzerland by the European Business Awards



PRODAFT is listed by Swisscom on the Swiss Artificial Intelligence Startup Map



www.prodaft.com
info@prodaft.com

Istanbul Office
Teknopark Istanbul, Sanayi Mah. 5A-301
+902162901832

Switzerland Office
Y-Parc, rue Gallée 7, 1400 Yverdon-les-Bains
+41225481923

U.S.T.A. (CYBER THREAT INTELLIGENCE PLATFORM)

U.S.T.A. is a cyber intelligence platform that relies on PRODAFT's award-winning deep web monitoring technologies. U.S.T.A. provides actionable and verified threat information with regard to cyber security, anti-fraud, and brand protection requirements.

These include:

- Malware and cyber-attack intelligence modules
- Strategic threat reports
- Stolen ID and credit card feeds
- Leaked credential notifications
- Deep web notifications



Awarded as "Security Innovation of the Year"

U.S.T.A. has been preferred by the following industries since 2012:

- Finance
- E-Commerce
- Aviation
- Telecommunication
- Insurance



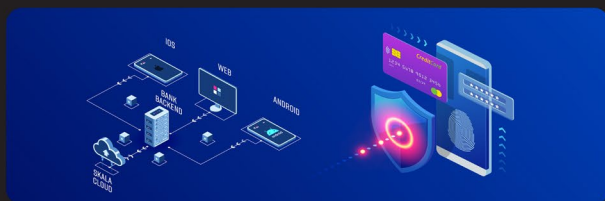
s.k.a.l.a (END USER DEVICE SECURITY SOLUTION)

SKALA is a malware detection platform developed by PRODAFT for the purpose of detecting malware on end-user devices on behalf of critical institutions, including banks, e-commerce organizations, airlines, and payment gateways. Thanks to its unique technology, SKALA instantly detects malware on an end-user device and simultaneously issues an alert to the company.

SKALA creates different fingerprints for most popular and high-end malware samples, then uses these fingerprints to detect their presence among end-users.

Whenever a malicious application on a device cannot be directly detected by common parameters such as package name or hash, SKALA analyzes other features of suspicious applications, including behavior and execution pattern, with 100% accuracy.

- Easy integration
- Retrospective analysis
- Heuristic detection approach
- GDPR compliant



PENETRATION TESTS

PRODAFT allows you to identify and eliminate vulnerabilities of specific software, hardware, and operation of your institution by security consultants with requisite expertise specific to your needs.

Visit pentest.blog for our 0-day researches



- Web application penetration testing
- Mobil application penetration testing
- External/Internal network penetration testing

CYBER ATTACK DRILL

You can employ a variety of hardware and software solutions to prevent your business from cyber-attacks. However, the efficiency of these cyber security tools is always followed by a question mark. PRODAFT ensures that you are constantly ready for actual attacks with real life simulations.

BLOCKCHAIN SECURITY

PRODAFT offers blockchain security solutions for those whose investments are too valuable to risk.

FORENSICS ANALYSIS

The PRODAFT forensics team helps your business rebound from cyber crises and identifies related issues with technical acumen to prevent resurgence.

IOT SECURITY

The use of IoT devices is increasing disproportionately day by day. The PRODAFT team has been conducting cyber security tests of global companies' IoT services and products since 2017.

RED TEAM

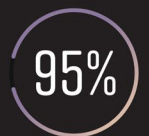
PRODAFT is the "first company in the EMEA region to" establish high-level physical and digital penetration testing team.

SECURITY TRAININGS

The weakest link in the safety of your cyberspace is always human errors. Risks that may arise from an unaware person should never be ignored.

PRODAFT offers instruction in the various required areas of information security with expert trainers. Instead of using standard educational materials, we create unique content to meet the needs of specific clients.

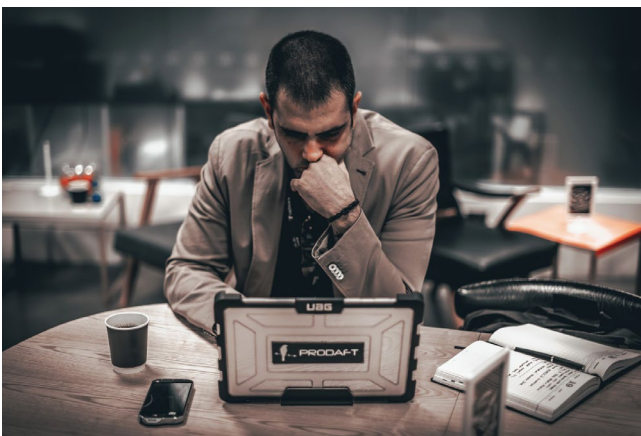
- Network Security Training
- Web Application Penetration Test Training
- Advanced Web Application Penetration Test Training
- Security Awareness Trainings
- Practical Penetration Test Training with Virtual Security Lab
- Malware Reverse-Engineering and Analysis Training
- Forensic Analysis Training
- Secure Coding Training with Examples
- Advanced Zero-day Research on Real-World Products Training
- Mobile Application Security Training



95% OF ALL SUCCESSFUL CYBER ATTACKS ARE THE RESULT OF HUMAN ERROR

PRODAFT underlines risk management as a silver bullet in fighting cybercrime

Swiss cyber threat intelligence company, PRODAFT, sets the global standards for proactive defense in the cyber space. Celebrating its 10th anniversary this year, PRODAFT focuses to repel cyber threats with Swiss precision and neutrality.



Cyber threats

The chief risk faced by companies of all sizes in the cyber space has been to ensure stability to ensure confidence among its investors and customers. According to Yildizli, these threats range depending on the company size.

He said, “There are different challenges for SMEs, private organisations, large enterprises, end-users and critical infrastructures. For example, supply chain attacks continue to be the biggest threat for large enterprises, while newly emerging mobile malware variants are on the rise for end users.

“Meanwhile, for SMEs, organised ransomware groups continue to be the biggest threat. Aside from all of these, we’re witnessing extremely well-crafted cyberattacks performed by advanced persistent threat groups against critical infrastructures.”

A lot of attention has surrounded critical infrastructure over the past few months, following a number of successful high-profile attacks.

Recently, two cyberattacks were directed at the Fujitsu company and Greater Tokyo-based Narita Airport. The former saw Fujitsu’s software ProjectWEB infiltrated by hackers. The platform holds around 76,000 email addresses from the government’s land, infrastructure and transport ministry as well as obtained data from the ministry’s internal mail and internal settings. The latter incident included hackers targeting the airport’s software to steal air traffic control data.

Elsewhere, Belgium’s Federal Public Service Interior recently claimed it suffered a ‘complex, sophisticated and targeted cyberattack’ to its IT system. The department identified an attack after it called in the Centre for Cybersecurity Belgium in March. After running further tests, it identified ‘subtle leads to questionable acts on the network of the PPS interior’.

Ireland’s healthcare service was also recently temporarily forced to shut down its computer systems as a precaution following a significant ransomware attack.



The founders – Can Yildizli, Koryak Uzan and Mehmet Ince - all came from various backgrounds in the security industry. But despite their differences, they all believed in a more proactive approach towards security, according to PRODAFT CEO Yildizli.

This led them to create USTA – the company’s threat intelligence platform. PRODAFT claims USTA has been recognised as one of the first threat intel solutions to be ever developed and has enabled exchange of cyber threat information among parties while detecting potential threats in the cyber underground.

When asked what sets PRODAFT apart from other cybersecurity and cyberintelligence firms in their field, he cites that the business is a ‘purely technical’ solution provider. Furthermore, Yildizli stated the company has always aspired to be the ‘high-end’ solution provider in their field, being a business that can achieve and resolve the most demanding challenges.

Risk management and trendsetting

A reason attacks like those mentioned are successful is down to a lack of awareness. Yildizli believes firms can tend to underestimate the real impact of a cyberattack, and they need to be more proactive before an attack happens.

He said, "It's all about managing the risk. Usually, companies tend to underestimate the actual impact of a cyberattack, leading to under-staffed, under-budgeted cyber defence capabilities. Cybersecurity is not a 'checkbox' that needs to be marked with regular intervals - it's a continuous condition that requires constant care and diligence. For this reason, it should be regarded as an inseparable part of an organisation's strategy like accounting or human relations. As an organisation grows, their cybersecurity strategies shall be grown as well."

Yildizli also remarked that he believes trends in the cybersecurity and cyberintelligence industries are not set by the providers but by the threat actors themselves. Providers can only try to adapt as well as possible by analysing current trends and forecasting future trends of the 'cyber-underground'.

He said, "For the last five years we have been witnessing an outbreak of threat intelligence providers. While this seems to be a very positive trend in the long-run, our industry has started to drown cybersecurity teams in intelligence data feeds. Therefore, I believe we will all be seeing more customized, "to-the-point" cyber intelligence providers who focus on a more specific threat type in the cyber space. This trend has already started.

"Right now; buyers are implementing very specific intelligence sources into their Security Operation Centers in the way they deem appropriate. For example, 90% of our client-base is comprised from organizations that have more than 5-10M retail customers, as USTA, our threat intel solution, is regarded as a highly-capable solution for preventing cyber-fraud against end-users."

National security

Alongside companies having to get to grips with the vital importance of cybersecurity is the even more pressing matter of national governments having to do the same. The US recently suffered a severe cyberattack after the Colonial Pipeline was hacked into by the DarkSide ransomware variant. The pipeline transports 100 million gallons of fuel daily to customers from New York to Texas and is the largest pipeline for moving gas and diesel products in the US at 2.7 million miles.

Uzan believes that the time to do something about cybercrime and its ever-growing risk has come and

gone. However, now that national governments have begun to take the issue more seriously, he believes it is important they formulate more partnerships within the private sector.

"The time to take it more seriously was in 2005. Yet, many governments around the world have approached cybersecurity as a regulatory challenge such as retirement or zoning programs. It took approximately 15 years for many states to realize that cybersecurity is an issue of national security. A never-ending battle with a nearly invisible, ever-changing enemy.

"Unlike conventional warfare scenarios - where it's possible for governments to source their own requirements - cybersecurity is an area that makes it mandatory for states to have strong bonds and connections with the private sector. That's why we have started seeing more open, transparent co-operations between governments and private sector members."

While cybercrime is most often than not completely remote, Uzan believes that this also means the solution can be remote too. He stated, "There are thousands of brilliant solutions against different threats. While some solutions are required to be sourced nationally and regionally, solutions such as cyber-threat intelligence shall be chosen and implemented from different providers with different perspectives.

Future goals

Going forward, PRODAFT highlighted its long-term goal is to transform PRODAFT into a global market leader in threat intelligence while also 'preserving its niche qualities'. Yildizli claimed this is why the company is constantly working on cases such as state-sponsored threat actors and organised cybercrime groups.

In the medium term, however, the company is looking to expand its already growing presence in the European market.

He said "For Europe, our medium-term goal is to enhance brand recognition by providing effective resolutions to high-profile threats in the region. We have already started achieving this goal to a certain extent by becoming the first company to discover and map demanding threats such as FluBot, BrunHilda or SilverFish. By doing this, we would like to introduce the region to our threat intel platform, USTA, which is the market leader in different countries of the Middle East and North Africa region."

The company also introduced SKALA earlier this year, a solution which PRODAFT believes will be a 'gamechanger' in battling mobile banking malware in end-user devices. ●



Founded 2003



Employees: 11-50



Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Application Security, Cloud Security, Employee Risk, Risk Assessment/Risk Management



Regions of operations: Global

Proteus-Cyber are specialists in Data Privacy, the GDPR, CCPA, LGPD, PDPA, RGPD regulations, plus others and own the award-winning software Proteus®NextGen Data Privacy™, the software that provides everything you need to manage your data privacy compliance in order to avoid a data breach. It really is the Gold Standard of data privacy compliance. With In-built Privacy Impact Assessments & Data Privacy Impact Assessments (PIA/DPIA), it can automate parts of the process to enable the DPO to perform mapping of personal data and assess how and why the personal sensitive data that exists is processed, and more importantly, how it is secure. Proteus®NextGen Data Privacy™ is a Fully integrated enterprise scalable software solution with features like, Data Discovery & Categorisation, Automated PIA/DPIA & risk assessments, 3rd party audits, DSAR management, privacy-by-design, Breach notification, Free privacy research, Threat-intelligence, Pro-active Breach protection, Cookie management, Consent, Easy reporting and supported in over 100+ languages.

QOMPLX:



Founded 2015



Employees: 101-250



Subsectors: Threat Management/Security Operations, Identity & Access Management, Risk Assessment/Risk Management



Regions of operations: United Kingdom, United States

QOMPLX makes technology that helps the world's leading companies identify and defeat sophisticated cyber adversaries including cyber-criminal groups and nation-state actors. These groups are exploiting critical IT infrastructure including Microsoft Active Directory to establish long-term residence on sensitive networks, often disguised as privileged users or applications. With QOMPLX, financial institutions can integrate disparate data sources across their enterprise to spot malicious activity and the earliest stages of a cyber attack. The company's advanced streaming analytics technology uses rules, algorithms, simulations, and machine learning tools to help financial institutions identify attacks on Active Directory and other core infrastructure in near real-time. QOMPLX's advanced algorithms, simulations, and machine learning tools help the world's most demanding firms solve the toughest challenges in cyber security, insurance underwriting and finance.



Founded 2020



Employees: 1-10



Subsectors: Application Security, Cloud Security, Risk Assessment/Risk Management



Regions of operations: Europe, United States

Quantimatter provides a Cybersecurity testing "as-a-Service" platform using Robotic Process Automation to assess Cybersecurity maturity and mitigate exploits in days, instead of weeks. The company helps small and medium sized businesses build digital resilience through vulnerability testing for online infrastructures and active penetration testing as well as testing for Quantum Computing readiness. Users can subscribe to the platform for a monthly fee and run unlimited assessments and ongoing tests to validate for new exploits and threats, and receive detailed dashboards and reports with critical issues in their online infrastructure, including plain-language instructions to remediate them.



COMPANY RESEARCH PROFILE

REDSCAN

A **KROLL** BUSINESS

PRODUCT NAME:
ThreatDetect™
- Managed Detection and Response

Founded 2015
 London, United Kingdom
www.redscan.com
info@redscan.com
 Employees: 101-250
 Regions of operation: EMEA

KEY EMPLOYEES:



Andrew Beckett
Head of EMEA Cyber Risk,
Kroll



Mike Fenton
CEO, Redscan



Gubi Singh
COO, Redscan

Subsectors: **Threat Management/Security Operations, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Incident Response**

OFFERING

Redscan is an award-winning provider of security services, specialising in Managed Detection and Response (MDR), penetration testing and red teaming.

By understanding how attackers behave and offering high-quality support and insight, Redscan's cyber security professionals help organisations in the financial services industry to enhance cyber resilience, rapidly respond to threats and achieve compliance with the latest information and data security standards.

PROBLEM BEING SOLVED

In the face of more persistent and better-resourced adversaries, every organisation's cyber risk is increasing. To avoid potential operational disruption, as well as financial and reputational damage, the ability to rapidly detect and respond to threats that are capable of evading security defences is more important than ever.

Redscan ThreatDetect™ is an outcome-focused MDR service that supplies the personnel, technology and cyberoffensive intelligence that financial services firms need to hunt for, disrupt and eliminate threats across IT environments - swiftly and effectively, 24/7.

TECHNOLOGY

CyberOps™, Redscan's threat management platform, is central to ThreatDetect.

CyberOps provides extended detection and response (XDR) by ingesting and enriching security data from networks, endpoints, applications and cloud environments.

Suspicious events are investigated by Redscan's team of security operations centre (SOC) experts and, if identified as malicious, raised as prioritised incidents for client attention, complete with actionable mitigation guidance and automated response actions.

PRODUCT DESCRIPTION

Redscan's ThreatDetect™ solution is an outcome-focused Managed Detection and Response service that supplies the support, insight and automated actions organisations need to swiftly detect and respond to cyber threats across networks, endpoints and cloud environments.

Integrating experienced SOC experts, a cloud-native technology stack and real-time curated cyberoffensive intelligence, the service helps expand threat coverage and visibility plus contain and eliminate threats before they are capable of causing damage and disruption.

By proactively identifying breaches, ThreatDetect helps financial services firms to comply with a wide range of information and data security requirements, including those mandated by the Financial Conduct Authority, the Bank of England, the PCI Council and SWIFT.

ThreatDetect has a Net Promoter Score (NPS) of 63, distinguishing the service as 'great'.

TRACTION/GROWTH

- ThreatDetect clients range from FTSE 100 companies to mid-sized organisations and start-ups. Redscan clients in the financial sector include banks, hedge funds, wealth management firms and fintechs.
- Redscan's acquisition by Kroll in March 2021 marks a period of significant business growth that has also seen the company recognised by Gartner® as a representative vendor in its 2020 MDR Market Guide.
- In the last five years, Redscan has received over 20 industry awards, including Cybersecurity Service Provider of the Year at the Cybersecurity Excellence Awards 2021.

Focus on threat detection and response to help beat the clock after a cyberattack

Speed is vital during a cyberattack. The quicker a company can respond to an incident, the greater the chance to minimise the negative impact it has, according to Kroll head of EMEA cyber risk, Andrew Beckett.



REDSKAN A KROLL BUSINESS

Despite the amount of attention around cybersecurity, attacks are growing in volume and complexity and the Covid-19 pandemic has exacerbated the difficulties. With a large portion of staff working remotely, it has become more challenging for companies to safeguard their data and gain visibility of threats across networks and endpoints. On that point, 93% of organisations suffered a compromise of data over the past 12 months and of those, 49% were hit by at least four incidents, according to research from Kroll. Worryingly, 82% of security leaders fear their organisation is still vulnerable to attack.

Beckett sees remote working as one of the biggest challenges facing firms today. Remote employees may no longer be under the same watchful gaze of the information security team, their new working devices and home networks are likely to be less protected than at the office, opening many new opportunities for attackers to compromise users and subsequently, the corporate network.

Another problem with remote working is that staff are increasingly reliant on personal devices. While adopting a bring your own device policy may save costs

from not having to buy computers for all remote staff – it means security staff may lose visibility of users’ behaviours. A personal IT system will not have the same level of monitoring as a corporate device. Besides the increased risk of compromise, there is also the problem of how to ensure data is properly stored and then deleted from a personal computer. If an employee leaves, how can a firm be certain they deleted all private information saved on the computer, or that documents were properly stored and backed up?

Beckett said, realistically, for the next two years businesses are going to be fighting to restore normality. They will need to understand where their data is now and what is stored on hardware outside of their control.

This is why it is crucial for companies to implement a threat detection and response system that can increase visibility for security leaders and help track access to systems and resources. Threat detection services like those offered by Redscan, which was acquired by Kroll earlier this year, empower organisations to log and track suspicious activity, such as network connections from unknown locations and whether data is being copied to external devices. Also, if there is a successful phishing attempt or breach, companies can detect it and respond to it quicker, thereby minimising potential damage and disruption.

“In medical terms, you talk about the golden hour after a heart attack or after a stroke. That is very much what we’re delivering here - early detection and early response. The quicker you can respond, the better you can minimise the negative impact of a cyber incident on your organisation. You can quickly start to contain the malware, stop the attacker moving laterally across your network and then throw them out.”

However, threat detection and response systems can be tough to implement correctly due to their technical complexity. An organisation can have thousands of endpoints, systems and applications. Monitoring therefore needs to be unified to give a holistic view of what is going on in an organisation. For most companies, this is beyond their capacity to handle in-house. Kroll research showed that 76% of organizations use third-parties as part of their detection and response

process, and 55% of respondents identified improvement in the time to contain and remediate threats as the key benefit of working with third-parties.

Specialist providers of Managed Detection and Response (MDR) services, like Redscan, monitor networks, endpoints and cloud environments on behalf of their clients 24/7/365 and use their experience to proactively identify external attacks as well as unusual user behaviour. Beckett said, "For every zero day that is used for the first time, there are literally tens of thousands of repeat attacks that have been seen before. If you've seen it before, you know how to respond. If you know how to respond, your responses are faster."

The damage of an attack

It is tough to assess what the biggest risk firms will face following a breach. It depends on the scale of the incident, the firm itself and how quickly everything was resolved. However, most boards will always be concerned about any negative connotations associated with the brand following an attack, Beckett said. In a recent research from Kroll, 64% of security leaders identified reputational damage as their greatest fear following a cyberattack.



"Threats are more sophisticated and persistent than ever. Companies need to be improving their ability to detect suspicious activity early."

Another major worry for boards is the reaction from regulators. When a company suffers a breach, there are often complex regulatory requirements to report the incident to relevant supervisory authorities. Following an investigation, the regulator will assess whether any penalties should be imposed, such as increased regulatory scrutiny or the imposition of substantial fines. Ultimately, the compliance costs are "going to go through the roof," Beckett said.

However, this doesn't have to be the case. If a firm has a threat detection capability in place, the brand damage and response from regulators could be minimised. Redscan's MDR platform gives companies the ability to detect breaches early but also helps to evidence what has happened during the incident. This includes information such as what systems and files were accessed, what they read and importantly, if any data was exfiltrated. By understanding the true extent of a breach and being able to forensically prove what data and systems an attacker accessed, a company can strengthen their defence narrative and potentially minimise the impact of regulatory

actions. Having appropriate controls and procedures in place to proactively identify attacks can also demonstrate a mature approach to cyber security and data protection.

Beckett said, "We have historically seen that where we've provided those services, regulators have taken a very fair stance. When we demonstrate that the client has complied with regulations, taken appropriate steps to safeguard data, and that they have not been fast and loose with personal data, the regulator is more inclined to accept that they have been hacked and should be considered a victim. That puts you very much on the front foot with the regulators rather than on the back foot."

Setting up the team

While each company is different, there are a few additional measures a company can implement to ensure they are best prepared. Staff awareness training comes near the top of that list. Staff are the first line of defence and their training can prevent a lot of attacks. Human error caused around 90% of cyber data breaches in 2019, according to research from CybSafe. If companies better train their staff on how to spot attacks, how to report suspicious activity and what to do once an attack occurs, they can go a long way to minimising risks.

However, cyber awareness does not just stop at the general workforce. Beckett believes the best approach to cybersecurity is to have the board lead by example. He said, "We see companies where there's a security policy in place for the staff to comply with, but the board ignores it because it gets in the way. They ask why they should have to use multi-factor authentication to see their emails, but they're the ones most likely to be targeted by phishing attacks."

Not only should they abide by cybersecurity procedures, Beckett believes the board should also be talking about cybersecurity on a regular basis. They should question if they have the right security in place, how many incidents they have had, what can be learned from breaches, whether to adjust budgets. They should also ensure there is a cyber incident response plan in place and that it is regularly practised. It is no use having a plan if it has not been rehearsed, Beckett explained. "When you practise them, you build that institutional muscle memory, to enable the response to be faster so that golden hour can be effective. It prevents time spent running around asking who's got this, what has happened and where do I find the information?"

Beckett concluded, "Security professionals have known for years that a security strategy centred around prevention is no longer effective. Threats are more sophisticated and persistent than ever. Companies need to be improving their ability to detect suspicious activity early. Whether that is through increased awareness of staff or the deployment of EDR/MDR systems, early detection and rehearsed response greatly increases the chances that an organisation can contain the threat and respond before serious damage is done to their data, systems or reputation." ●

Case study

Enhancing an asset management firm's security visibility with MDR

OVERVIEW

A UK-based asset management firm wanted a proactive security monitoring solution that could provide centralised threat visibility across its on-premises networks, endpoints and cloud environments. By choosing **ThreatDetect™**, Redscan's award-winning Managed Detection and Response (MDR) service, the business now benefits from a unified monitoring capability and additional expertise to identify and respond to security incidents, 24/7/365.

The challenge

The firm was looking to gain more complete security visibility across its IT estate and ensure that it was meeting the compliance requirements of the Financial Conduct Authority and other regulatory bodies.

While it had always taken cyber security very seriously, the business had no dedicated security team. Past investments in detection technologies had therefore failed to achieve the security improvements it was looking for.



Across the whole service, whether the SOC or the technical account management team, Redscan looks after us very well."

IT DIRECTOR

The solution

A proof of concept confirmed that **ThreatDetect™**, Redscan's MDR service, provided the technology, expertise and outcome-focused approach that the firm needed. Redscan's Security Operations Centre (SOC) team investigate and triage alerts generated by the detection tools deployed as part of the service 24/7/365, providing actionable remediation advice and automated response actions to support a swift and effective response to incidents.





CyberOps™, the threat management platform included as part of ThreatDetect, has helped the business to centralise security visibility, as it now receives all security alerts generated across its endpoints, networks and cloud environments via a single platform. All notifications are analysed and triaged by Redscan's SOC professionals, enabling the company's in-house team to focus on remediating incidents rather than discovering them.



INCLUDES





- Monitoring of cloud services
- Weekly threat intelligence reports
- Log storage for compliance



-  Founded 2018
-  Employees: 11-50
-  Subsectors: Data Security/Data Governance, Email/Communication Security
-  Regions of operations: North America, EMEA, Asia-Pacific





Quantum Xchange gives commercial enterprises and government agencies the ultimate solution for secure communications. Its complete key management system, Phio Trusted Xchange (TX), is uniquely capable of making existing encryption keys quantum safe and supports both post-quantum crypto (PQC) and Quantum Key Distribution (QKD) for true crypto agility and quantum readiness. As the operator of the first quantum fiber network in the US, Quantum Xchange also holds the unique distinction of being the only company in the world to make QKD commercially viable by solving the distance and delivery limitations inherent with all other offerings. With a dynamic security infrastructure in place, organizations can enhance their existing encryption environment, select the level of protection needed based on their risk tolerance, and seamlessly scale to QKD at any time, across any distance, between multiple transmission points.

RED SIFT

-  Founded 2015
-  Employees: 51-100
-  Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Email/Communication Security, Fraud Prevention
-  Regions of operations: United Kingdom, United States, Australia

Red Sift is a global company aiming to democratize technology essential for cybersecurity. Products on the Red Sift platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence. Founded in 2015 by serial entrepreneurs Rahul Powar and Randal Pinto, Red Sift is headquartered in London, UK, and boasts an impressive client roster including Wise (previously Transferwise), Telefonica, Pipedrive, ITV and top global law firms.



-  Founded 2020
-  Employees: 11-50
-  Subsectors: Cyber Regulatory Risk & Reporting
-  Regions of operations: United Kingdom, Portugal, India

Regulativ.ai is a CyberTech, RegTech, and InsurTech company based in London, set up to help organisations transform their cyber regulatory compliance processes. The founding team of multi-disciplinary industry experts has been delivering complex solutions to banks, asset management, maritime, and government for the past three decades. The company offers cyber-regulatory compliance automation and cyber-insurance solutions across all sectors and markets. The solution enables customers to ingest regulatory policy information, form a trusted view of cybersecurity posture, and leverages leading-edge machine learning algorithms to automate narrative generation using proprietary data processing and governance technologies. The platform does the hard work. Security analysts oversee the process, review and approve the generated responses. CISO security specialists achieve up to 80% time savings in complying with security regulations, audits and other control reviews.

How Regulativ.ai is helping companies fix their cybersecurity processes

A Q&A with Regulativ.ai co-founder Mark Weston.



Where did the idea for Regulativ.ai come from, was there a lightbulb moment?

A global tier 1 bank provided the product's genesis early in 2020; recognising the colossal demand of cyber team resources for cybersecurity governance, regulation and compliance, they put out a request for proposals. We responded and were selected as the best solution. Having scanned the market, we realised that there was a real problem to be solved and a gap in the market.

How cyber risk is evolving?

Cyber threats are spiralling, and becoming high profile – a couple of recent examples are the colonial pipeline ransomware attack and the solar winds breach. Damages are increasing. Total global losses this year are estimated to reach between 2 and 6 trillion dollars. Enormous at any rate. Financial Services institutions are critical targets for cybercriminals – so governments and their regulators are responding with an ever increasing and demanding set of policies, regulations, directives and guidelines.

What was the problem in the market Regulativ.ai wanted to solve?

The business problem is an operational efficiency issue deriving from poor data management and inefficient manual processes - particularly acute in medium to large organisations that must comply with many

regulations. Most mature jurisdictions have some form of cyber-resiliency regulatory policy. The process to submit a cyber-resiliency assessment to the regulator is fraught with problems; huge data collection, analysis, summarisation and alignment to regulatory requirements and how the response needs to be drafted and prepared. This all takes significant time and money.

How does the company differentiate itself from other solutions?

Regulativ.ai is a start-up with a dynamic attitude to delivering product. Our core team has decades of experience, having completed more complex solutions under more challenging environments previously, using similar technologies. The team has won numerous industry awards and an outstanding delivery track record. Regulativ.ai has partnered with Birlasoft, a leading Digital & IT Services Firm, to develop the product and go to market. Birlasoft has a strong track record in working with clients globally across the Banking, Financial Services and Insurance space. In addition to the Digital (Data & Analytics, AI and Automation) capabilities, Birlasoft also has strong experience in the overall GRC (Governance, Risk & Compliance) and Regulatory Reporting space. Birlasoft adds deep technical & Financial Services industry expertise, global scale and the credibility of being part of the multi-billion dollar CK Birla Group.

Our products are designed to service large complex companies and function within an ecosystem of apps. We understand the challenges in building and delivering solutions into this environment; we have been there and done it for many years. Innovation is at the heart of the company. We approach all problems with out of the box thinking, using AI, innovative data governance, analytics, all combined with the latest in cybersecurity technology.

What were the initial reactions to the platform?

Following a comprehensive selection process, the tier 1 bank liked our solution and selected it above others. We have had further feedback from CISOs indicating that our product solves a problem that others solutions have not.

Are there any examples of customer successes stories?

None at the time of going to press, but with a couple of client engagements underway, we expect these to become sterling customer success stories for Regulativ.ai.

What was the biggest challenge the company faced in its development, and how did it overcome this?

COVID-19 has been the primary challenge we faced from company inception until now. Leading a development team spread across 9 locations in 3 countries, with no opportunity to co-locate, has impacted our velocity. Despite this, we have made fantastic progress and are racing towards our Beta and MVP product goals.

What are the company's growth plans for the next year?

With our joint Go-to-Market plans with Birlasoft, our initial focus is on North America and the UK. We plan 5-10 customer implementations as part of our Beta programme. This will help us further prove the solution and demonstrate value to our customers. Building on this, we plan to have three full implementations in the next 12 months to lay a solid foundation in the financial services sector.

Does there need to be more regulation around cybersecurity, and if so, what is required?

Yes, this is well overdue. Whilst cybersecurity has been on companies' agendas for 50 years, it has been largely voluntary. With business digitisation accelerating, the systemic risk of cyber threats has become too big not to be addressed by governments. Regulated companies must appoint a security team appropriate to the size of their business. Mandatory controls and capability assessments are essential, along with breach reporting. All jurisdictions need to step up and have dedicated cyber self-assessment regulations, with strict enforcement. This is the only way systematic risk can be monitored and managed effectively across a jurisdiction, region and globally. There also needs to be a real push to standardise reporting of cyber resiliency, IT security risk and third party supplier risk, which at the moment is lacking and is decades behind other regulatory reporting standards. Regulativ.ai is well-positioned to drive this streamlining effort.

Despite cyber-attacks often causing massive fallout for victims, why is there little regulation focused on improving protections?

Our research tells us that regulators are just behind the curve. They typically lack experience, the platforms and expertise to establish the right level of regulations and recommendation protections. There are some stand-out regulators in the cyber-space, namely in the US, UK, Singapore, Hong Kong and Australia, but the rest are far behind. Covid-19 has put more pressure on regulators to accelerate their journey. Many of the G20 & OECD nations are now fast-tracking their investments into digitising society and all core services (banking, payments, finance, social, e-commerce, education, healthcare, central government services). This pivot to

a fully digital society comes with exponential cyber-risks with inadequate cover by regulations or cyber-insurance currently, leaving organisations exposed to losses and potentially bankruptcy.

What can regulators and firms do to try and curb the number of successful attacks happening?

Regulators:

- Fast track cyber legislation, with customisations for SMEs where required.
- Strict enforcement, using a platform like Regulativ.ai to providing the ability to track and monitor ALL regulated entities in a jurisdiction.
- Penalise organisations in breach of the cyber regulations and where data breaches have happened to enforce the correct cyber resiliency behaviours.
- Knowledge exchange with all other regulators to share information on upcoming threats, changes in attack vectors and provide concise and accurate guidance to organisations to adopt and adapt their cyber defences.

Firms:

- Number 1 – adapt your mindset to accept that you will be hacked. The focus needs to be on minimising the impact and damage to the organisation.
- Doing nothing and hoping that your company won't be hacked the same as hoping that the sun won't rise in the east.
- Establish cyber infrastructure, get in experts to evaluate the risks, gaps in your cyber controls, prepare an assessment and implement the recommendations.
- Establish or use a continuous monitoring and resolution platform like Regulativ.ai.

Do firms need to reassess how they handle cybersecurity?

Yes, this is an essential first step and an ongoing activity for any that manages its risks. If you are not sure how to do this, come and talk to us at Regulativ.ai. We will give you honest feedback.

Is there a lack of awareness across all levels of businesses, and if so, how damaging is this?

This was undoubtedly the case 3-5 years ago, however since the recent spate of cyber-attacks, ransomware and phishing, in particular, risk managers are now often aware of the threats and potential impacts to their organisations. That awareness must be converted into a solid action plan to put in place the technology investment, investment in people and skills, and staying ahead of the curve on cyber threats. Regulations, an increase in scrutiny from regulators and enforcement of penalties will help ensure that these necessities happen. ●

Regulativ.ai + Birlasoft

AUTOMATING CYBERSECURITY REGULATORY REPORTING WITH AI

New revelations of major cyber breaches are now a daily occurrence globally. As cybersecurity threats increase exponentially, so do the number and extent of the regulations that seek to protect organizations and their customers. Financial services institutions are critical targets for cybercriminals and must navigate both an increasing number and an increasingly complex system of regulations & standards. Now they have a targeted solution to help them demonstrate compliance with multiple regulations while also reducing associated time, effort, and ultimately, cost.

Solution Overview

In partnership with Birlasoft, Regulativ.ai is transforming the cybersecurity reporting function across regulated industries. We have created a lightning fast, scalable and cost efficient governance platform using leading edge AI technology and an innovative multi-cloud platform to streamline cybersecurity self-assessment processes.

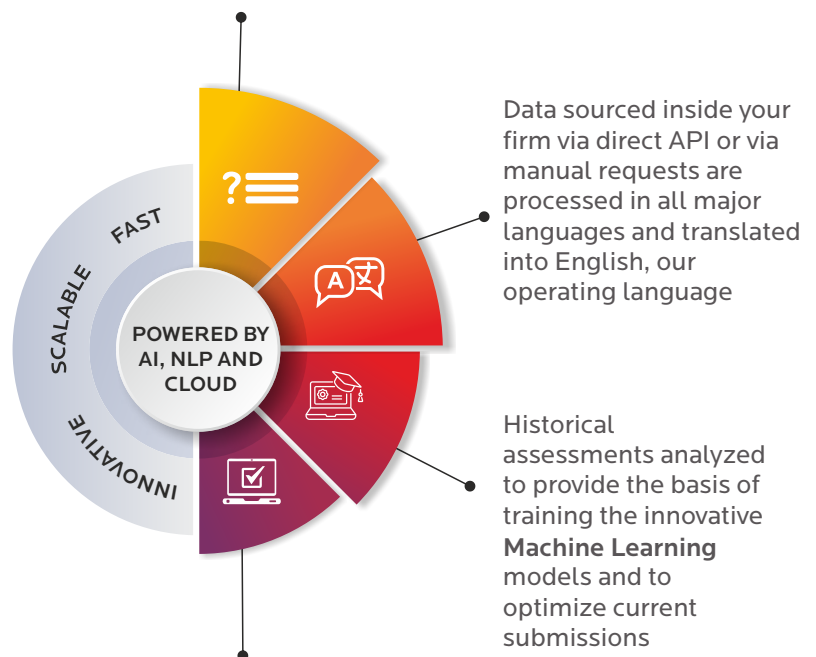
Business Challenges

- CISO teams are under increasing time and budget pressures
- Cybersecurity teams are spending hundreds, if not thousands, of hours in manual effort to become compliant with rules and regulations across multiple jurisdictions
- Individual cybersecurity self-assessments are taking up a large part of the cyber team effort and typically take hundreds of hours of manual effort to complete
- Third-party supplier risk assessments are typically lengthy, time-consuming and difficult to manage & co-ordinate
- Significant skills shortage in cyber teams and increasing outflow of critical cyber skills from the profession due to exhaustion and burn-out

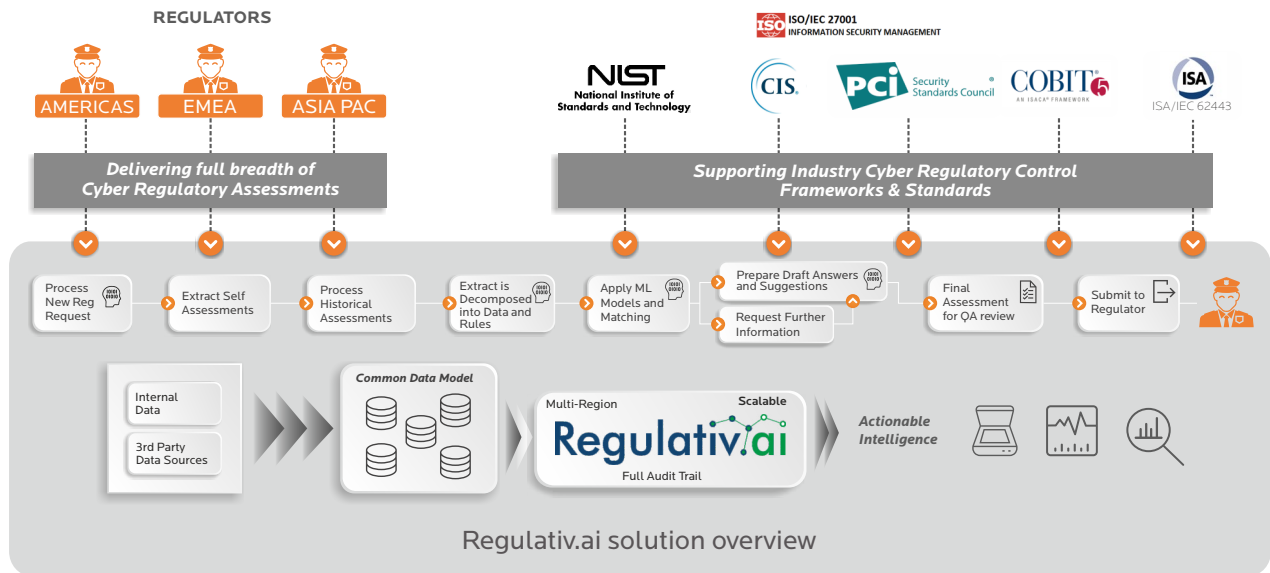
Key Features

Regulativ.ai analyses and abstracts the raw requirements issued by regulators and other standards setting organizations.

Regulativ.ai provides fast and cost-effective responses to regulators using all available historic and current data, across all regulators, using latest **Machine Learning** models.



Final review of the completed assessment performed by security analyst before finalization and submission to Regulators via an electronic or manual interface



Key Benefits



COST EFFECTIVE

Regulativ.ai and Birlasoft can enable savings in excess of 40% across current cybersecurity self-assessment processes



SCALABLE

Data quality, availability & re-use can be improved for internal cyber governance and optimized for cyber insurance coverage



AUTOMATION

CISO teams can re-focus valuable resources, people, and budgets on proactive cyber threat detection, defense, and management



COLLABORATION

Co-ordination of responses between different teams is streamlined via an integrated workflow solution

AVAILABLE REGULATIONS IN BANK

REGULATION ID	REGULATION NAME	REGULATOR	COUNTRY	STATUS	UPLC	ACTIONS
1001	CQUEST - Cyber Resilience Questionnaire	Financial Conduct Authority(FCA)	United Kingdom	PENDING FOR REVIEW	104	View
1002	Cyber Resilience Assessment Framework(CRAF)	Hong Kong Monetary Authority(HKMA)	Hong Kong	APPROVED	114	View
1003	Cyber Security Self-Assessment Framework	Office of the Superintendent of Financial Institutions(OSFI)	Canada	SAVED AS DRAFT	124	View
1004	Cyber Security Self-Assessment Framework	Monetary Authority of Singapore	Singapore	PENDING FOR REVIEW	19-0	View
1005	Supervisory Requirements for IT in Financial Institution	Federal Financial Supervisory Authority(BaFin)	Germany	INPROGRESS	20-0	View
1006	Checklist for Small Firms Cyber Security Program	Financial Industry Regulatory Authority(FINRA)	USA	SAVED AS DRAFT	21-0	View

Dashboard

CANADA ASSESSMENT OVERVIEW (OSFI Cyber Resilience)

- Open Questions
- At RFI Stage
- At Draft Review
- At Final Stage

UK ASSESSMENT OVERVIEW (FCA Cyber Resilience)

- Open Questions
- At RFI Stage
- At Draft Review
- At Final Stage

CANADA RFI METRICS (OSFI Cyber Resilience)

- Pending With CISO: 16
- Pending With Platform: 22
- Pending With Infrastructure: 25

CANADA RFI METRICS (FCA Cyber Resilience)

- Pending With CISO: 44
- Pending With Platform: 22
- Pending With Infrastructure: 25

Snapshot – Regulativ.ai

For more information on Birlasoft's AI - led Cybersecurity Services, please write to us at contactus@birlasoft.com



RESOURCES


contactus@birlasoft.com | birlasoft.com

Enterprise to the Power of Digital™


Birlasoft combines the power of domain, enterprise and digital technologies to reimagine business processes for customers and their ecosystem. Its consultative and design thinking approach makes societies more productive by helping customers run businesses. As part of the multibillion dollar diversified The CK Birla Group, Birlasoft with its 10,000 engineers, is committed to continuing our 159-year heritage of building sustainable communities.



 Founded 2012


 Employees: 11-50


 Subsectors: Data Security/Data Governance, Encryption


 Regions of operations: Global


SafeLogic is focused entirely on cryptography that meets and exceeds the NIST (National Institute of Standards and Technology) FIPS 140 benchmark. The company's solutions are available in a variety of flavors, including hardware (HSM) form factors like PCIe cards and open source compatible software modules. Popular replacement scenarios include OpenSSL, Bouncy Castle, NSS, and Libgcrypt. The company's tandem offering of the encryption module paired with certification services yields massive cost, time, and effort savings for customers. Companies ranging from tech titans like Hewlett Packard Enterprise to disruptors growing exponentially like Okta rely on SafeLogic to take care of their encryption requirements.



 Founded 2019


 Employees: 11-50

 Subsectors: Fraud Prevention, KYC/AML, Compliance, Intelligence


 Regions of operations: United Kingdom, France, Poland, the Russian Federation


Schwarzthal Tech is an innovative London based RegTech startup building an AI-driven platform that provides financial crime intelligence. It aims to revolutionize the way compliance works in the financial sector by bringing a paradigm shift from the traditional KYC towards a new concept: Know Your Network. The company employs graph-based data to assess and investigate complex cases. The technology can also be used to monitor transactions. Schwarzthal works with several high-profile clients, including private banks, VCs and exchanges. The startup is accelerated by Startupbootcamp, a leading European accelerator in the space of fintech innovations. The company's technology is empowered by Amazon and Neo4j.



 Founded 2017

 Employees: 11-50

 Subsectors: Threat Management/Security Operations, ADR Attack Detect Response

 Regions of operations: North America, Latin America, Europe, the Middle East, Africa and Asia-Pacific

SCYTHE enables you to turn cyber threat intelligence into reality through a common platform, providing a single pane of glass to identify security blindspots. With SCYTHE, security teams can quickly create realistic adversarial campaigns that cover the spectrum from simple to APT-level complexity and stealth. The company is providing all the building blocks for red, blue, and purple teams: a common platform and workflows to test and validate their security controls and investments against real world threats targeting their enterprise, tailored to what is specifically targeting them. The campaigns are created through a simple to use, drag and drop timeline that includes pre-saved actions that replicate real-world TTPs from the MITRE ATT&CK framework and an SDK to build your own modules and TTPs.

Why Schwarzthal Tech is betting on KYN to fight financial crime

Dr. Marius-Cristian Frunza left the commodities brokerage market after being disappointed by the helplessness of banks and law enforcement to tackle financial crime. This led to the creation of Schwarzthal Tech – a company building an AI-driven Know Your Network (KYN) platform to take on financial crime.



During his time in the commodities brokerage market, he claimed fraudsters from a range of backgrounds exploited the weaknesses of the banking and financial system – with billions of dollars misappropriated by transnational organised financial crime.

He said, “Both banks and law enforcement seemed helpless and unable to take the right actions. When I got insights about what tools and processes banks were using to tackle financial crime, it was clear they were not even close to understanding the underlying risks.”

Frunza noted that most financial institutions and large companies have a ‘box-ticking approach’ when it comes to dealing with matters related to financial crime, claiming this passive approach is a fertile ground for criminals and abusers looking to game the system.

This led to the creation of Schwarzthal Tech in 2019, with its focus being to leverage Frunza’s understanding of the way financial crime works and to use the right technology to help businesses efficiently tackle financial crime.

To meet this challenge, the company is currently building Wunderschild – an AI-driven platform that uses ‘cutting-edge’ algorithms to enable users to assess hidden connections with suspicious or criminal networks, perform in-depth assessments and better qualify and score risks better.

According to Frunza, Wunderschild provides the next generation in financial crime intelligence and leaps ahead of Know Your Customer and introduces Know Your Network.

He commented, “Our turnkey solution uses advanced algorithms that gather global multilingual data including companies’ ownerships, disqualifications, insolvencies, adverse media and sanction lists and allows you to visualise, assess and analyse the network and the underlying risk of a counterparty.”

Wunderschild employs advanced multilingual name matching algorithms and entity resolution methods to search and detect hidden connections between entities and is continuously drilling to find new connections and hidden links between parties.

Frunza added, “Leveraging a network-driven vision using graph-based technology, Wunderschild serves both investigators and compliance professionals in their quest for deep-dive analytics tools. Investigators are able to assess the hidden connections within criminal networks and explore their dynamics in the foreseeable future. Compliance officers are using the platform to analyse quantify the exposure to financial crime risk of their clients.”

Pitfalls of KYC

While KYC and Anti Money Laundering (AML) have a vital role in addressing financial crime risk, Frunza believes most teams in banks are underperforming on this matter, citing the big financial losses due to criminal behaviour.

He said, “Financial crime has leapt ahead of the financial institution in the race for globalisation and sophistication. Therefore, classic tools like KYC are not

as efficient in the current environment. It generates a high number of false positives and false negatives and is not capable of assessing criminal networks.

"It will always fail, for example, to show that a previous director is disqualified from another jurisdiction, or an investor is related to a sanctioned individual. Put simply, financial institutions do not have the right tools to distinguish between 'good' and 'bad' clients.

Intelligence to tackle crime

Many companies and banks have continued to look for the silver bullet in figuring out how to reduce their potential exposure to financial crime. To some, spending more on defences and hiring more experts has been the chosen route. However, Frunza believes that more doesn't always mean better.

He said, "Financial criminals are already a few steps ahead of law enforcement and compliance officers. The rapidly changing geopolitical equilibrium weakens the efforts of legal businesses to manage their exposure to financial crime risk.

"Therefore, companies need to step up their game and act smarter. When dealing with a superior opponent the only way is to use better intelligence. The financial system needs to move away from the regulatory-driven box-ticking approach and engage in a top-bottom strategy."

Frunza stated the critical aspect in really getting to grips with financial crime would be to assess the real threats and the crime typologies that an institution is exposed to. Based on this, the companies could employ sound technologies - supported by the vision of subject matter experts - to properly manage the risk rather than filling huge databases that become 'useless' when threats become real.

One of the biggest game-changers not just in the world of finance but across a range of other industries has been AI and machine learning, and more specifically their capabilities for making processes and tasks less complicated and more streamlined.

However, the Schwarzthal CEO believes that while some companies have the ability to use AI and ML-driven solutions, the solutions aren't currently best suited for tackling financial crime.

He said, "Only a very few big tech firms have the ability and the resources to develop, test and implement bespoke AI and ML-driven solutions. Most tech firms are leveraging existing infrastructure and libraries developed by providers like Amazon Web Services.

"While such turnkey AI solutions have undisputed advantages, they are not calibrated to deal with financial crime risk. Therefore, even banks using very advanced tools have big issues when onboarding new customers or assessing their existing ones. Most banks are

spending between 5-10% of their revenue on compliance, but they end up with low performance and high-cost solution."

Frunza remarked that he believes there is 'definitely a place' for AI and ML-driven solutions, however, the industry is still in a very early stage. For an AI and ML-based revolution in fighting financial crime, he believes tech giants such as Amazon or Google will need to step in in order to drive real change.

National stability

Beyond banks and companies, there is an ever-growing threat not just to personal security but to national and international security. Many countries are coming to grips with the new world of financial crime, and there is a pressing need for national governments to stabilise themselves from such threats.

Frunza said, "National governments are facing unprecedented challenges. While most countries are trying to keep away criminals by addressing such threats with tougher regulations, some other countries are exposed to the risks of being hijacked by groups specialized in financial crime.

"Both the economy and crime are globalised, therefore a material threat in one country will eventually affect other regions of the world. In such a matter, national governments should move to proactive approaches and not rely entirely on financial institutions to tackle threats like global money laundering or uber-terrorism."

Frunza cited that with the ever-growing digitalisation of the economy and the democratisation of financial services, the world is witnessing the phenomenon of 'uberisation' of financial crime, leading money laundering and financial terrorism to become more decentralised than ever before.

Furthermore, he remarked that individual people and companies from all walks of life can now knowingly or unknowingly be engaged in illegal endeavours, and that financial crime is the first beneficiary of the new 'gig economy'.

He added, "When dealing with such threats, governments should encourage their underlying intelligence agencies to share proactively critical information with companies that are in the front line of the war against financial criminality."

Looking toward the future, Frunza said Schwarzthal is aiming to add new types of data to its Wunderschild platform. This, he claims, will include information about ships, cargos, vehicles and real estate properties. The platform will also propose sound tools for asset tracking.

Frunza concluded, "At Schwarzthal Tech, we will continue to serve diligently our current clients and to enrich our portfolio with new customers from various sectors, including investment companies and law firms. We aim to become a leading global provider of financial crime intelligence." ●



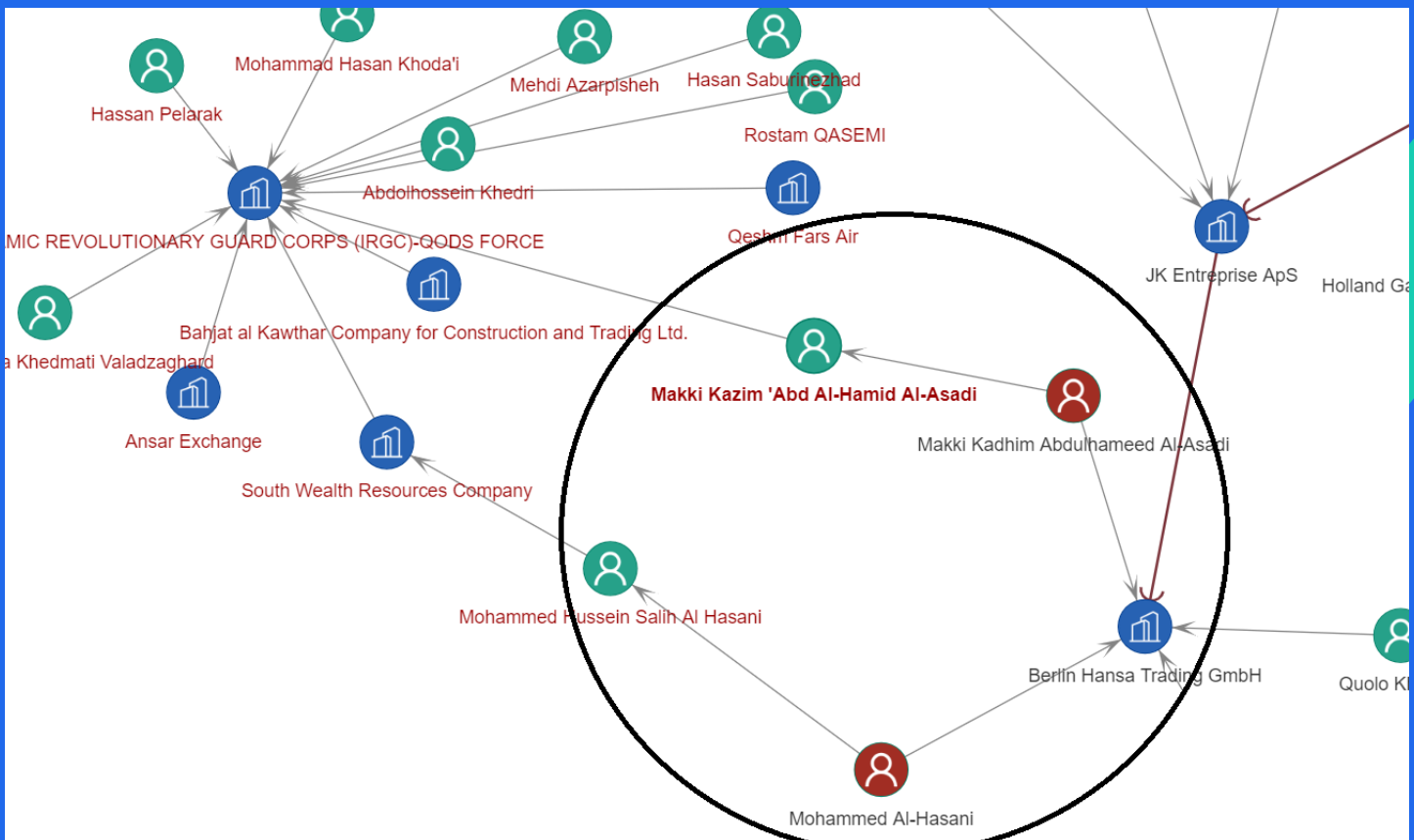
Case study: German company managed by terrorists

Synopsis

⚠️ A joint investigation led by the German team of Business Insider and by the Danish newspaper Jyllands-Posten unravelled another massive case of terrorism financing about VAT fraud.

In the centre of this investigation stands Berlin Hansa Trading, a German company with two directors figuring on the OFAC sanctions lists. Mohammed el-Hassani and Makki al-Assadi have been flagged as related to the Iranian Revolutionary Guard Corps, an organisation designated as terrorist. Berlin Hansa Trading had several ties with Iran but also with Danish companies that defrauded the Nordic country of 300 million Danish kroner in unpaid VAT and company tax.

Know Your Network TM





Name transliteration and synthetic identities

- ⓘ There are many challenges when assessing and investigating counterparties from Middle Eastern countries. The most underrated problem is the transliteration of names written in languages using the Arabic alphabet. Name transliteration from Arabic or Persian to a Language using Latin alphabets is not bijective, thereby generating many versions for one name. Thus, it is impossible to build a fully-fledged picture of their interests and connections without a comprehensive multilingual name matching tool when assessing such persons.

Transliteration is a real weapon facilitating the creation of multiple identities. In other words, versions of the same person's name in various languages allow them to create different identities.

Trade-based money laundering and VAT fraud

- ⓘ Trade-Based Money Laundering is a recent trend in Money Laundering aiming to circumvent the conventional banking system. The US extraterritoriality laws pushed European banks to turn down transfers to or in relation with Iranian counterparties. BNP Paribas, a leading French bank, paid one of the most significant fines in history for breaching Iranian sanctions imposed by the US.

TBML employs trade transactions. Criminals do not transfer the proceeds of their crime via monetary transactions but through trades, whereas merchandise is sent to a counterparty.

TBML and VAT fraud are a deadly combination because the last step in a VAT carousel corresponds to the stage where proceeds are laundered and transferred in another jurisdiction as merchandise. Both TBML and VAT fraud target products with low storage cost and high economic value.

SecurityCompass



Founded 2004



Employees: 251-500



Subsectors: Application Security, Cloud Security, Risk Assessment/Risk Management, Balanced Development Automation, IT Governance, Risk and Compliance, Threat Modeling, Compliance Management



Regions of operations: North America, South America, and Europe

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India. For more information, please visit www.securitycompass.com.



Founded 2017



Employees: 51-100



Subsectors: Identity & Access Management, Fraud Prevention



Regions of operations: Global

Shufti Pro is one of the most noticeable providers in the field of anti-fraud and KYC/AML/KYB solutions in Europe, Asia, the Middle East & the US. The company has developed a Hybrid system of AI/ML that performs fast, accurate, and compliant customer due diligence online. Its technology helps online services all over the world with legal and regulatory requirements, increase conversion, prevent fraud, and ensure client trust. Shufti Pro verifies 7 billion people from 232+ different countries in 30-60 seconds with 99.6% precision and verifies them by 3,000+ documents in 150+ languages and screens them against 1,700+ watch lists in competitive and customized pricing.



Founded 2017



Employees: 11-50







Subsectors: Risk Assessment/Risk Management



Regions of operations: Global

Sigma Ratings provides a new, smarter way to continuously evaluate risk and build trust in any relationship. Using advanced real-time risk analysis and monitoring technology, Sigma actively screens thousands of global data sources and puts essential compliance insights into a single stream of risk intelligence, thereby reducing manual workflows, enriching existing client data, and helping teams make clearer, more timely decisions in investigations, relationship management, and onboarding. Founded at MIT in 2017 by industry experts, Sigma has a talented team of engineers, data scientists and experts in international finance, technology, and regulation.



-  Founded 2017
-  Employees: 11-50
-  Subsectors: Risk Assessment/Risk Management
-  Regions of operations: Global





Simudyne is a simulation technology company based in London. It uses advanced analytics and AI alongside agent-based modelling and simulation to help institutions, exchanges and governments to generate greater insight and foresight. It helps them to solve complex problems and drive better strategic execution, operational performance and financial results. With a realistic simulated environment, institutions can integrate modelling and simulation into the fabric of their decisions because they can model feedback and learn to train their intelligence (whether human or artificial). They can then evaluate scenarios to enable fast convergence on the best outcome and understand the best path forward before committing people and resources.



-  Founded 1993
-  Employees: 1,001-5,000
-  Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Application Security, Endpoint Security, Cloud Security, Email/Communication Security, Fraud Prevention, Employee Risk, Risk Assessment/Risk Management
-  Regions of operations: United Kingdom, EMEA, APAC, United States

Softcat believes in enabling its customers to move fast securely. The company does this by reselling products and with its own range of services and solutions. For those products which the company resells it acts as a consultant tactically advising customers within that technology space as to what is best of breed and most appropriate to their requirement helping them make more effective decisions faster. Softcat has a clear vision: to help its clients to Build, Implement and Maintain an ongoing program of work, to reduce Cyber Risk in a way that is right for their business. Through its assessment services, (encompassing people, process and technology) the company provides pragmatic ongoing programmes of improvement, bespoke to that customer. Additionally, the company can optionally supplement this strategic approach through its managed security services, encompassing Managed SIEM, Managed Endpoint Detection & Response (MDR), Managed Firewall, and Vulnerability Scanning Service helping teams scale in an industry with critical skills shortages.



-  Founded 2014
-  Employees: 11-50
-  Subsectors: Threat Management/Security Operations
-  Regions of operations: Americas, Europe, APAC

Source Defense, the leader in Client-side Security, enables secure digital innovation, and ensures customer and payment data privacy via a real-time prevention solution against website supply chain attacks. The company provides its customers with a fully automated and dynamic set of rules and policies that control access and permissions of all Javascript based 3rd-party tools operating on a website.




Founded 2014



Employees: 51-100



Subsectors: Identity & Access Management, Fraud Prevention, Voice Biometrics



Regions of operations: Switzerland, Germany, Italy, Spain, United Kingdom, Russia, United States

Spitch is a global provider of B2B and B2C voice and text conversational AI and cyber security solutions, headquartered in Switzerland with a presence in many countries across Europe and North America. Spitch helps enterprises to better understand and serve their customers through the use of AI (NLP, NLU and ML). Spitch offers end-to-end products such as virtual assistants, voice biometrics (for identification, ID verification and fraud prevention) and speech analytics. These are parts of a unified Spitch omnichannel conversational platform based on a microservice architecture that can be deployed both in-cloud and on-premise for additional data protection. At the heart of Spitch's philosophy lies a commitment to provide its customers with tangible cost savings and customer experience improvement, delivering a strong ROI. Another key differentiator for Spitch is very fast delivery thanks to its out-of-the-box products and advanced development tools.




Founded 2018



Employees: 1-10



Subsectors: Identity & Access Management, Authentication in payment, mobility, military and IoT



Regions of operations: United Kingdom, South Korea, Indonesia

swIDch is an authentication technology startup for enterprises which aims to eliminate digital identity-related fraud through its patented algorithm OTAC (One-Time Authentication Code). OTAC is a unique, unidirectional and dynamic token generated from a user's device (e.g. mobile) that identifies and authenticates users securely and efficiently. It does not duplicate with anyone else at any given time and it identifies a user with the code alone, even in a networkless environment. It provides strong security to its clients as well as saves costs from fraud losses, integration and operation of their legacy system for authentication. The ability to generate a dynamic code without a network, which can accurately identify a user had previously been deemed impossible before swIDch created this innovative solution. Since the technology is provided in the form of API/SDK, it can be easily altered to apply across multiple verticals such as payment, mobility, IoT, and so on.




Founded 2008



Employees: 11-50



Subsectors: Financial Crime



Regions of operations: North America, EMEA, APAC

AyasdiAI, a Symphony AI portfolio company, empowers banks and financial institutions with a complete picture of customer, third party and user behavior to discover crime, risk and competitive opportunity through unparalleled, predictive insight. Using a uniquely powerful combination of artificial intelligence and machine learning, AyasdiAI customers dramatically reduce the time to achieve genuine transparency, with full explainability. Ayasdi Sensa™ leverages unique combinations of topological data analysis, time series and leading analytical innovations to give organizations absolute fidelity for competitive discovery, risk detection and efficiency optimization. With full visibility, firms can definitively pinpoint risk, drastically cutting costs while protecting their standing with regulators and brand reputation with customers.



-  Founded 1999
-  Employees: 51-100
-  Subsectors: Data Security/Data Governance, Email/Communication Security, Fraud Prevention
-  Regions of operations: Global

TeleMessage is transforming business mobile messaging with its messaging solutions which include:





- Mobile Archiver – effectively addresses mobile phone text and call archiving for compliance, regulatory and eDiscovery response requirements. It reduces risk across a variety of industries, capturing mobile content from BYOD and corporate phones; Enabling the capture and archival of: SMS, MMS, Voice calls, as well as WhatsApp, WeChat, Signal and Telegram apps.
- Secure Enterprise Messaging – enables secure enterprise chat for co-workers by using user-friendly mobile apps and a range of APIs that connect to any operational IT system.
- Mass Messaging – provides tools to deliver multi and omni-channel bulk messaging across: SMS, MMS, Voice calls, Faxes, Email, and Mobile Apps.



-  Founded 2017
-  Employees: 11-50
-  Subsectors: Data Security/Data Governance, Email/Communication Security, Employee Risk, Risk Assessment/Risk Management
-  Regions of operations: United States, United Kingdom, EU, Canada, Australia

Theta Lake is a purpose-built security, risk, and data privacy solution that automates detection of misconduct, data leakage, regulatory and data privacy risks in what is shared, shown on screen, spoken, or written in modern communications. Natively integrated with leaders in unified communication (Cisco Webex, Microsoft Teams, RingCentral, Zoom, Slack, and others), Theta Lake's multi-patent pending AI analyzes audio, video, and collaboration chat to power risk and data leakage insights, identify phishing and malware links, as well as prioritize risk review and remediate content that violates policies from the UC platforms. With long-term SEC 17a-4 compliant archiving, legal hold, and robust eDiscovery capabilities, Theta Lake adds efficiency and scale to the compliance review and supervision process, driving down the cost of compliance. Safety COVER helps firms manage platform security settings and provides best practices to maintain safe and secure collaboration. The Theta Lake Compliance Suite is SOC 2, Type 2 compliant.



-  Founded 2016
-  Employees: 1-10
-  Subsectors: Employee Risk - Uniquely Real-time Security Awareness and Behaviour Change
-  Regions of operations: United Kingdom

Founded at the end of 2016 by the ex-global Heads of IT and InfoSec from the Cyber arm of BAE Systems (previously Detica), Think Cyber Security deliver secure behaviour change for their customers. The company's award winning Redflags™ Real-time Security Awareness software applies behavioural and learning science theory to deliver context-sensitive, just-in-time guidance. For example when users are about to click links, visit certain web pages, enter their username into a web page, handle attachments, etc. Redflags™ offers the toolkit financial services firms need to: manage operational risk from cyber-attacks directed at staff; meet compliance goals; keep content refreshed and relevant; target specific behaviours and specific users; all whilst allowing staff to get on with their jobs, to achieve business goals.



COMPANY RESEARCH PROFILE



PRODUCT NAMES:
ThreatQ and ThreatQ Investigations

- Founded 2013
- Reston, VA, United States
- www.threatq.com
- info@threatq.com
- Employees: 101-250
- Regions of operation: US, France, UK, Germany, Australia, Saudi Arabia, United Arab Emirates, Spain

KEY EMPLOYEES:

- Wayne Chiang**
Co-Founder and Chief Architect
- John Czupak**
President and CEO
- Jonathan Couch**
Senior Vice President, Strategy & Corporate Development

Subsectors: **Threat Management/Security Operations**

OFFERING

ThreatQuotient offers a platform which accelerates and simplifies investigations and collaboration within and across teams and tools. Integrating an organization's existing processes and technologies into a unified workspace, ThreatQuotient's solutions reduce noise, highlight top priority threats and automate processes to provide greater focus and decision support while maximizing limited resources. ThreatQuotient's threat-centric approach supports multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability management, while also serving as a threat intelligence platform.

PROBLEM BEING SOLVED

Analysts are bombarded with millions of threat data points every day from multiple sources in multiple formats. This includes external data from commercial sources, open source, industry and existing security vendors as well as internal sources. Each point product within their internal layers of defense, SIEM and other systems within their security infrastructure generates a massive amount of log and event data and alerts. ThreatQuotient empowers organizations to understand their unique threats, and prioritize and act upon the threat intelligence that is most relevant to them.

TECHNOLOGY

ThreatQ is the only platform using analytics and machine learning to determine relevance and priority for specific companies. This is the basis for the platform's dynamic scoring and self-tuning capabilities. As more data and context is captured in the Threat Library, the platform will re-prioritize the data to ensure appropriate actions are taken. ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other structured and unstructured data, along with an SDK and APIs for custom connections.

PRODUCT DESCRIPTION

ThreatQuotient offers the ThreatQ platform and ThreatQ Investigations, a cybersecurity situation room.

- **ThreatQ** - Security operations teams use the ThreatQ platform to prioritize threat intelligence, quickly deploy threat data to existing sensor grids, and focus workflows to reduce time to detection (TTD) and time to response (TTR). The ThreatQ platform provides a unique combination of capabilities that streamline threat operations and management to accelerate security operations. Beyond the threat intelligence platform use case, ThreatQ can be leveraged for a number of security operations priorities: threat hunting, incident response, spear phishing, alert triage and vulnerability prioritization.
- **ThreatQ Investigations** – the industry's first cybersecurity situation room designed for collaborative threat analysis, shared and accelerated understanding, and coordinated response. Built on top of the ThreatQ platform, ThreatQ Investigations allows for the capturing, learning and sharing of knowledge. Use cases for ThreatQ Investigations include anticipation situations that accelerate understanding of emerging threats to update defense posture proactively; response situations that enable the right responses to be determined and acted upon faster than previously possible; and retrospective analysis to learn what can be improved in the future.

TRACTION/GROWTH

- Leading global companies use ThreatQuotient's solutions as the cornerstone of their security operations, including Fortune 100/500, major retail and hospitality, healthcare, technology, finance, and defense customers globally.
- As a result of using ThreatQuotient's solutions for process optimization, customers experience an ROI of 2-3 full-time employees (FTEs). ThreatQ's ability to minimize adversary dwell time provides additional ROI of 3 to 4 FTEs.
- ThreatQuotient works with leading distributor/MSSP partners such as:



- The company raised \$22.5m in April to bring new capabilities to the ThreatQ platform and accelerate global go-to-market strategy. Currently 50% of the company's business comes from outside the US.

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.

How ThreatQuotient is transforming the use of threat data and intelligence



Threat data and intelligence are some of the most valuable tools in cybersecurity, but in order to leverage them successfully companies need to evolve their security operations. While working together in the cybersecurity industry, prior to founding ThreatQuotient, co-founders Ryan Trost and Wayne Chiang used threat intelligence to protect a large enterprise from cyberattacks. During this time they realized there was a lack of solutions enabling cybersecurity teams to aggregate, organize and maintain their cyber threat intelligence. Most security appliances lacked flexible or well-documented APIs, forcing analysts to copy and paste indicators from websites, blogs and emails into spreadsheets for storing.

ThreatQuotient Senior Vice President of Strategy and Corporate Development, Jonathan Couch said, "Ryan and Wayne realized that if they were experiencing this problem, other defenders were most likely sharing the same challenge." Following the epiphany, the pair went on to found ThreatQuotient in 2013 with the goal to create a tool to make security more manageable and productive.

Couch shared, "We believe that threat data and intelligence are the most valuable tools to detect, prevent and respond to threats. It provides the context and foundational understanding that is needed for effective security operations. However, to make use of this, organizations need an approach to security operations that relies on a single, systemic security architecture that supports all teams and use cases while continuously improving." This is where ThreatQuotient comes in. It fills the gap as the first platform to enable a shared understanding across teams and tools within an organization's infrastructure.

Reactions from ThreatQuotient's clients have shown just how beneficial using ThreatQ is. They are often stunned

at what can be automated, how much better teams can collaborate and how it even pushes people to do more and further their own innovation. ThreatQuotient is always seeking feedback to further support clients and better their solutions. "We would not be anywhere near where we are today without taking a 'what have you done for me today' kind of attitude toward the platform. What we can do now is amazing compared to when we started, but where we will be in the future will be even more amazing."

To continue meeting all their customers' needs, the company recently launched ThreatQ TDR Orchestrator. Their data-driven approach to SOAR and XDR accelerates threat detection and response across disparate systems for more efficient and effective security operations. Couch explained, "we are facing a shortage of security personnel, which has become a fact of life for every security organization. Meanwhile, security operations centers (SOCs) are increasingly focused on detection and response. Automation is a key strategy to offload repetitive tasks and empower humans to conduct advanced security operations tasks."

Currently, most security automation and orchestration approaches are focused on automating processes, Couch explained. Unfortunately, when this is applied to detection and response, process-focused-playbooks are inefficient. This is simply because decision-making criteria and logic built into playbooks need to be updated. This is why ThreatQuotient believes "automation is more than just running processes." Automation should include inputs and outputs to processes as well as cover the full security lifecycle, and is exactly why ThreatQuotient takes a data-driven approach to automation.

To overcome the universal challenge of operationalizing threat intelligence, Saudi Investment Bank (SAIB) based its cyber threat intelligence strategy on ThreatQuotient's centralized platform that would allow it to proactively mitigate risk. ThreatQuotient is supporting SAIB to make more informed business decisions to ensure security gaps are addressed, reduce alert fatigue, increase productivity, and accelerate detection and response.

Most recently, ThreatQuotient closed a \$22.5m funding round to support its continued global growth. The company currently has 50% of its business coming from outside the US, but the goal for 2022 is to increase this international presence.

Through its continued growth, the company will also continue to support various rhino conservation efforts. The ThreatQuotient team is passionate about the animal, which also serves as its mascot and they even go by the name of The Crash – the term for a group of rhinos. ThreatQuotient frequently conducts activities like, auctioning rhino plushies at RSA, to donate the proceeds to related charities.

Couch concluded, "It is important that we remind ourselves often that it isn't about us - it's about things we are passionate about: cybersecurity, our families, and the world around us." ●

CUSTOMER SUCCESS STORY

The Saudi Investment Bank Makes ThreatQ the Core of its Threat Intelligence Program

To overcome the universal challenge of operationalizing threat intelligence, Saudi Investment Bank (SAIB) based its cyber threat intelligence strategy on a centralized platform that would allow it to proactively mitigate risk.

Challenge

The Saudi Investment Bank (SAIB) faced two primary challenges with respect to threat intelligence — being able to use it to proactively prepare for and prevent attacks they were seeing in the wild, and ensuring compliance with SAMA and government regulations that required a complete threat management program. Charged with helping to lead the execution of a three-year strategy to address both challenges, Ayman Al-Shafai, Head of Security Operations Center for SAIB, wanted to take a threat-centric approach to security operations.

Learning from the pitfalls he had seen other organizations face, Ayman knew that they needed to mature the program to address the digitalization initiative and align with SAIB's strategic direction. The most effective path forward would be to start with a platform that could help them gain better visibility into the threat landscape for analysis and action, dynamically enhancing their security controls to protect and prevent potential threats and provide secure services to their

customers. Like most organizations, SAIB had access to vast amounts of threat intelligence to analyze and make actionable. Therefore, they needed a centralized platform to help them aggregate, curate and share intelligence across several teams and provide reports to support strategic, tactical and operational decision making.

Solution

Before initiating a thorough evaluation of the solutions available in the market, SAIB identified the following success criteria:

- Intuitiveness, meaning it is easy for threat intelligence analysts to learn and use the tool and share information in a format that is simple for other teams to use.
- Compatibility with standards, such as STIX and TAXII, which are extremely important to the ability to import and aggregate threat intelligence into a platform.

“Achieving compliance is important, but we wanted to go beyond checking boxes and truly utilize and benefit from threat data. We needed a deeper and better understanding of the threat landscape — the who, what, how and relevance to SAIB — so we could proactively mitigate risk to our customers and the organization.”

– Ayman Al-Shafai, Head of Security Operations Center, SAIB

OVERVIEW

INDUSTRY: Financial Services
CUSTOMER SINCE: 2019
EMPLOYEES: 1,437*
TOTAL INCOME: 2.9 Billion SAR*
LOCATION: Riyadh, Saudi Arabia

CHALLENGE

Proactively prepare for and prevent attacks in the wild and ensure compliance with the Saudi Arabian Monetary Authority (SAMA) and government regulations.

SOLUTION

As a centralized platform to aggregate, prioritize and share intelligence across teams; foster collaboration; and enrich all SAIB's security tools and technologies with IOCs and related actionable intelligence, ThreatQ provides a deeper understanding of threats and enables faster and automated actions.

OUTCOME

- ✓ More informed business decisions
- ✓ Reduced alert fatigue and increased analyst productivity
- ✓ Proactive detection and minimized time to respond
- ✓ Streamlined operations and better ROI on security infrastructure

*SAIB Integrated Report 2019

CUSTOMER SUCCESS STORY: SAIB Makes ThreatQ the Core of its Threat Intelligence Program

- Integration with various, different security solutions so that investigations and preventive actions can be performed from the platform instead of having to move between multiple solutions, reducing time to detect and resolve cyber incidents.
- Prioritization to understand which threats matter most to the organization and reduce alert fatigue.
- A strategic partnership and level of engagement that ensures issues are prioritized and resolved quickly.

SAIB determined that ThreatQuotient and the ThreatQ platform met all the criteria and was most aligned with their needs.

Working with ThreatQuotient's Professional Services team, within the first six months the bank deployed the ThreatQ platform and integrated it with a majority of the security controls within their ecosystem. They also completed integration with a range of threat data sources including multiple commercial and open source intelligence feeds as well as national CERT information and MITRE ATT&CK.

SAIB's strategy to initially focus on using ThreatQ to understand the broader, dynamic threat landscape quickly began paying dividends. Ayman shares, "With threat intelligence, you can feel like you're looking at random pieces of a jigsaw puzzle. But now, if we observe something within our technology infrastructure and bring it into ThreatQ to correlate it with other relevant data, we can put the puzzle pieces together, take that intelligence further for corrective action and share it more broadly."

With threat intelligence management as a solid foundation, SAIB is using ThreatQ Investigations to achieve additional key objectives, such as incident response and threat hunting. "Visualizing and connecting the dots to identify indicators and attack patterns with ThreatQ Investigations is extremely beneficial for accelerating a comprehensive response and preventing similar attacks in the future," Ayman explains.

The threat intelligence team is also collaborating with different teams within the bank to support various levels of activities. For example, sharing actionable intelligence to help protect against fraud and support risk management, as well as providing reports to support strategic initiatives such as digitalization.

"The ThreatQ platform is at the core of our threat intelligence program, helping us gain a deeper understanding of different threat actors so we can actually predict what may happen, rather than be in reactive mode and firefighting all the time."

- Ayman Al-Shafai, Head of Security Operations Center, SAIB



Outcome

More informed business decisions

ThreatQ reports, delivered in language that resonates with business leaders, allows senior management to make more informed business decisions and take specific actions. For example, ensuring any security gaps are addressed as new services are designed and prepared for launch to customers.

Reduced alert fatigue and increased productivity

As a centralized platform for data aggregation, correlation and prioritization, ThreatQ reduces false positives and allows analysts to focus on what matters. The ability to take corrective action directly from within the platform allows analysts to handle more incidents and be more productive.

Proactive detection and accelerated response





Collaboration during the investigation process, sharing of intelligence with other teams and integration with existing security tools and controls enables SAIB to leverage ThreatQ to optimize threat management, incident response, threat hunting, fraud management, vulnerability management and risk management.

Integration with security infrastructure to streamline operations and increase ROI

Bi-directional integration enables cyber defense teams to quickly act on threat intelligence, allows the ThreatQ platform to serve as organizational memory and continuously learn and improve, and enhances the value of all security investments.

ThreatQuotient's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA. For more information, visit www.threatquotient.com.



-  Founded 2015
-  Employees: 51-100
-  Subsectors: Threat Management/Security Operations, Identity & Access Management, Data Security/Data Governance, Fraud Prevention, Risk Assessment/Risk Management
-  Regions of operations: CEE, DACH, LATAM, Turkey, United Kingdom, Canada, United States

ThreatMark brings trust to the digital world by providing cutting-edge fraud prevention solutions based on a modern cognitive security user-centric approach. ThreatMark delivers a combination of evidence-based cyber threat detection capabilities and behavioral profiling, including behavioral biometrics, making a perfect fit for combating the ever-changing threat landscape of modern banking applications. Major banks use ThreatMark's AI-powered technology to build secured banking experiences by precisely validating their legitimate users, seamlessly across all digital channels. ThreatMark ensures that the entire digital journey (onboarding, authentication, account management, transactions...) is trusted and safe for both end-users and businesses. ThreatMark's advanced solution is complemented by their own Security Operations Center, a team of fraud & cybersecurity experts who vigilantly watch for new malicious activities across devices, throughout the digital landscape.



-  Founded 2008
-  Employees: 101-250
-  Subsectors: Fraud Prevention
-  Regions of operations: United States, Canada, United Kingdom, Germany, Australia, Caribbean, Latin America, parts of Asia, Kenya

Alessa by Tier1 Financial Solutions is a comprehensive solution that includes identity verification, due diligence, sanctions and watch list screening, transaction monitoring and regulatory reporting capabilities – all critical functions needed by financial institutions to fight financial crimes and comply with anti-money laundering (AML) regulations. Alessa is used in more than 20 countries and is the solution of choice as it offers the ability to integrate data from disparate IT and business systems and detect non-compliant or fraudulent transactions. In addition to monitoring transactions for fraud and compliance, Alessa offers the capability to screen individuals and businesses against internal and third-party sanctions and watch lists in order to identify sanctioned or high-risk entities that pose an increased financial crime risk. Organizations can choose to screen at the beginning of the relationship, as well as, periodically to ensure that there are no new risks. To learn more about Alessa's financial crime fighting capabilities, visit us at www.tier1fin.com/alessa/.



-  Founded 2014
-  Employees: 1-10
-  Subsectors: Identity & Access Management, Data Security/Data Governance
-  Regions of operations: Global

Torsion is an information security and data governance software provider, created in 2014, to solve the problem of sprawling access to files and folders by integrating with collaboration systems such as Sharepoint, Teams and Office 365, to monitor and control access. Torsion works with collaboration tools to automatically monitor and detect any inappropriate access, out of date folders and permissions, or the movement of files. If anything doesn't look quite right it will promptly alert a business user associated with the file and shut down any potential breaches. Other than that, it can run seamlessly in the background until and unless it is required. Owners or creators of files and folders can certify and revoke access themselves, taking the responsibility away from the IT function.



**COMPANY
RESEARCH
PROFILE**



PRODUCT NAME:
Virsec Security Platform

- Founded 2015
- San Jose, CA, United States
- www.virsec.com
- info@virsec.com
- Employees: 101-250
- Regions of operation: Global

KEY EMPLOYEES:



Dave Furneaux
CEO



Satya Gupta
Co-Founder, CTO

Ray DeMeo
Co-Founder and SVP,
Public Sector Business

Subsectors: **Application Security, Cloud Security, Container Security, Application-aware Workload Protection, Memory Protection, Server Protection, Runtime Protection**

OFFERING

Virsec delivers application-aware workload protection that provides system integrity assurance, runtime application and memory protection in a single solution -- delivering in-depth visibility across the entire workload. Virsec's unique technology defends against both known and unknown attacks, with no signature or prior knowledge required. The solution secures all critical business applications, from legacy to COTS to custom, in any environment.

PROBLEM BEING SOLVED

As businesses have prioritized speed and performance of their software applications, the ability to effectively protect workloads has not kept pace.

Virsec is the only vendor to protect the entire attackable surface of the application — including at the Host, Memory, and Web layers — during runtime. The company's platform enables businesses to consolidate their security infrastructure while dramatically reducing analysis time and labor resources.

TECHNOLOGY

Virsec's patented AppMap® technology maps applications in-depth across the complete application stack. Virsec automatically identifies the correct files, scripts, directories, libraries, inputs, processes, memory usage, and more. This comprehensive application-awareness protects workloads in any environment and is applied in real-time, as application code executes.

Virsec eliminates the need to use multiple threat hunting tools or spend time analyzing what threat is happening – instead, the solution immediately recognizes there is a threat the moment the code deviates from expected execution and stops it.

PRODUCT DESCRIPTION

The Virsec Security Platform is the first and only application-aware workload protection platform that incorporates System Integrity Assurance, Application Control and Memory Protection into a single solution. Virsec delivers in-depth visibility across the entire workload in any environment and blocks threats that are both known and unknown that go undetected by heuristic and endpoint security solutions.

Virsec's patented technology maps the legitimate execution of all applications, file libraries, operating systems, processes, and memory. The automated platform instantly detects any code deviations during runtime and stops them. The Virsec solution detects and stops advanced and evasive fileless and zero-day techniques, including remote code execution exploits, memory attacks, buffer overflow attacks, stack smashing, DLL injections, return-oriented programming (ROP) and ROP gadgets, side channel attacks and corruption of configuration data.

Virsec also offers full-stack application security for Managed Security Service Providers (MSSP) that streamlines the management of the Virsec platform, enabling MSSPs and their end-users to secure enterprise workloads and centralize the management of customer deployments, gaining a deeper level of visibility of those deployments in one dashboard. These MSSPs can onboard and manage Virsec's application-aware workload protection for all of their customers from one console, avoiding an entire step of deploying a Central Management System for each customer.

TRACTION/GROWTH

- Virsec Systems works with leading partners and customers including Raytheon Technologies, Tech Mahindra, Aveva, GDIT, Schneider Electric, Broadcom and more.
- Virsec established partnership with Yotta Infrastructure, the managed colocation and cloud service provider that operates the world's second largest Uptime Institute Tier IV designed data center, to bring end-to-end, real-time application security to Yotta's Enterprise Cloud and Colocation customers.
- Virsec has won over 20 prestigious awards for its ground-breaking technology, including Cyber Defense, Cyber Excellence, Info Security, Homeland Security, GSN, and CRN.

This document is being provided for information purposes only. It is not designed to be taken as advice or a recommendation for any specific investment or strategy decisions.

How Virsec is protecting companies and their digital infrastructure from black hats

As new strains of malware grow, enterprises need to ensure they're implementing appropriate security measures to eliminate any weaknesses that make them vulnerable to an attack. And it's imperative to develop security plans with the knowledge that the attackers are already inside networks.



The only reliable way to stop bad actors in their tracks is to first determine whether the executing code came from the application's developer or was it generated by a bad actor. Once that is decided, take the necessary steps. That's when the seeds for Virsec's unique technology were planted in founder Satya Gupta's mind. It was the need of the hour to spawn a cybersecurity solution which detects threats before it touches an application. Gupta believes "it [was] time to reimagine security and start protection from the inside, where it matters most."

Fast forward to 2021 and the firm now has a presence in 16 countries and has north of several dozens of customers.

Challenges facing the online world

It's no secret that malware writers today are far more sophisticated compared to those a decade ago. The scalability and low entry costs of software applications have changed businesses forever. While entrepreneurs have increasingly prioritised cybersecurity in the past few years, the ability to effectively protect applications has not kept pace. The main reason is that current tools being used are no longer adequate.

"Frankly, they're fighting yesterday's battle," Virsec's CEO, Dave Furneaux said. "Perimeters are now so porous that NIST has told us to assume that the attackers are already present inside the environment. If the attackers are already inside the network, we need to have the means to protect the software itself."

For decades, security tools have used backward-looking methods, such as signatures that could only identify previously known attacks. And, to mount an effective cyber defence, businesses would need to have prior knowledge of the same attack. "Or just plain get lucky and guess. And guesswork is hardly a recipe for success in any endeavour," Furneaux said. "If you have a signature or rule to identify a cyber threat, then you can stop it, but the caveat is that it hasn't changed since the last time your system saw it. And how often does that happen? This method is inherently unable to look forward or prevent previously unseen attacks."



Eighteen years have passed since the SQL Slammer worm was released and nothing has ever come close to the speed at which it brought down most of the world's servers and networks. When Slammer overflowed a SQL server, it used that computer to search for and infect every other computer it could reach. To fight the malware, cybersecurity companies were frantically releasing signature updates every ten minutes. According to Virsec's CTO Satya Gupta, "Attempting to fight a polymorphic worm that was rapidly mutating was like taking a fire extinguisher to put out an inferno."

"That was when we realised that all those cyber defenders who rely on profiling attackers' techniques through the signature of network or system call behaviour were in an asymmetric battle that they had zero ability to win. An attacker can create new malware orders of magnitude faster than defenders can analyse," he added.

Tellingly, companies can no longer afford to rely on antiquated approaches. In today's growing threat environment, it is imperative that organisations focus on adopting new methods to ensure the protection of their assets and infrastructure.

In addition, given that most insidious attack techniques are undetected at runtime, companies require a security system that can monitor potential attacks before they damage the software. Furneaux added that security control deployed by businesses must have deep enough visibility in runtime to map and monitor the intended execution of software code and stop any deviation. "We need to be able to stop attacks the moment they attempt to execute – not identify them after the fact," he added.

In simple words, until organisations can account for every execution of every bit of software and application code at runtime deep in the memory layer, they cannot consider themselves protected.

Another challenge is that applications are not adequately checked for bugs and vulnerabilities. Web marauders looking to penetrate an app know where to find and exploit a vulnerability. In fact, a [Contrast Security report said 90%](#) of apps aren't tested for vulnerabilities during their development and quality assurance stages and even more go unprotected during production.

With so many vulnerable apps running in the enterprise, it's key for network defenders to have effective application-aware protection, ensure the acceptable execution of each application and protect them at the memory level during runtime. "We must be able to identify when the bad guys are injecting code or manipulating processes and stop them from hijacking servers and derailing applications. This is impossible unless you are application-aware; if you don't know what your application is supposed to do, you cannot recognise when it deviates from its expected execution," Furneaux said.

He added that the security solution deployed by a firm must be able to detect anomalies before they can execute and during runtime. "Any deviation from the norm [should be] instantly detected, treated as a threat, and blocked," he said. And this is what Virsec aims to do.

How Virsec aims to disrupt the security industry

In Furneaux's words, Virsec's solution prevents application workloads from being hijacked or infiltrated and protects memory, files, processes and data from the inside. "Virsec is the first security solution to provide comprehensive protection of applications during runtime. Virsec's patented AppMap® technology maps what an application is supposed to do," he said.

Virsec incorporates system integrity assurance, application control and memory protection into a

single solution. Its solution provides real-time memory protection and stops memory-based attacks in real-time, regardless of the threat vector. Alongside detecting advanced attacks across the full application stack including the web, memory and host layers, it blocks any unknown threats, fileless malware or ransomware – including those that go undetected by heuristic and endpoint security solutions. "This provides an advanced, turn-key solution for a wide range of enterprise applications that otherwise do not exist," Furneaux detailed. "Unlike EDR/EPP and other perimeter security controls, Virsec's source of trust is the application's code itself. Once a developer delivers an application, the Virsec source of trust never changes. This stands in contrast to conventional security controls, which depend on a moving target of threat feeds."

In addition, the startup also provides security for managed security service providers (MSSP) enabling MSSPs and, ultimately, their end-users, to secure enterprise workloads while gaining a deeper level of visibility of those deployments in one dashboard. Furneaux added, "These MSSPs can onboard and manage Virsec workload protection for customers from one console, avoiding an entire step of deploying a central management system for every customer."

What sets Virsec apart is that it defends against the widest range of unknown and unknown attacks, including remote code execution exploits, memory attacks, buffer overflow attacks, stack smashing, DLL injections, return-oriented programming (ROP) and ROP gadgets, side-channel attacks and corruption of configuration data, with no prior knowledge required. "By protecting the entire server workload – we secure all your critical business applications – from legacy to COTS to custom," Furneaux said.

Nipping the threat in the bud

With the Covid-19 outbreak impacting the cybersecurity threat landscape, more organisations are looking to protect their critical infrastructure.

As a result, it's more important now than ever to deploy zero-trust and application-aware workload protection. "This is your warning sign. Waiting until after the attack has happened or stating that you've never seen an attack like this is no longer a valid excuse," Furneaux added. He believes that application-aware workload protection is the way of the future for cybersecurity and is the only proven technology to protect against any type of cyberattack.

As Furneaux said, "you can't stop what you can't see." Only by being able to efficiently protect the entire digital infrastructure, organisations can be sure that their most valuable assets are safe. Advising head honchos, he concludes, "Protect your application workloads from the inside out, ensure the integrity of all workload components, and protect them continuously during runtime by only allowing authorised processes to execute." ●



Founded 2014



Employees: 101-250



Subsectors: Identity & Access Management



Regions of operations: Global

Transmit Security, the identity experience company, is at the forefront of creating frictionless identity experiences for both customers and workforce across all channels. Its user-centric solutions, which include the industry's first app-less biometric authenticator, are proven to ensure an effortless and truly passwordless experience - effectively reducing all forms of identity attrition and saving enterprises substantial costs. Transmit Security was co-founded by serial entrepreneurs and investors, Mickey Boodaei and Rakesh Loonkar in 2014 with the aim of changing the security identity landscape. In 2020, Deloitte recognized Transmit Security as the 5th fastest growing company in North America. Today, the company's powerful technology is used by millions of end-users worldwide spanning across all industries and platforms.



Founded 2016



Employees: 11-50



Subsectors: Threat Management/Security Operations, Identity & Access Management, Email/Communication Security, Fraud Prevention, Employee Risk, Risk Assessment/Risk Management



Regions of operations: Global

TypingDNA is a behavioral biometrics company protecting online users based on how they type on their keyboards. TypingDNA provides a low-code authentication API suitable for securing login, enforcing reset passwords, and biometric authentication. The newly launched product, TypingDNA Verify, is a smarter 2FA method that replaces SMS codes, improving the user experience while reducing costs by an order of magnitude. TypingDNA's products are implemented by companies in various industries, financial and banking institutions, as well as cybersecurity companies and educational organizations. TypingDNA's technology expands the limited biometric authentication options without requiring specialized sensors or advanced hardware. More than 70% of millennials prefer written communication over phone calls. TypingDNA is on the quest to better this human interaction, ensure security, and facilitate a seamless user experience. In early 2020, TypingDNA raised a \$7M Series A from Gradient Ventures, Google's AI-focused venture fund, and other participants such as GapMinder, Techstars Ventures, and other prior investors.



Founded 2006



Employees: 11-50



Subsectors: Identity & Access Management, Fraud Prevention



Regions of operations: Global





Veratad Technologies is the leading provider of global age and identity solutions. Veratad makes high-end technology accessible with a full suite of trusted and highly flexible solutions. With Veratad, data, documents, out-of-wallet questions, mobile two-factor authentication and biometrics come together to solve the toughest identity problems. Privacy matters at Veratad. The company's solutions verify age or identity in seconds while protecting sensitive personal data and promoting a high level of consumer privacy. Veratad's goal is to keep clients safe without losing focus on their goals of increasing profits, reducing costs, preventing fraud and enhancing compliance.



- 
Founded 2012
- 
Employees: 101-250
- 
Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Endpoint Security, Cloud Security, Risk Assessment/Risk Management
- 
Regions of operations: North America, United Kingdom, Europe, APAC

Wandera provides a unified, cloud-delivered security solution that secures the new way of working. The service was designed to protect remote workers and devices from cyber threats, to enforce acceptable usage policies, and to enable zero trust access to all applications. Wandera operates a globally distributed Security Cloud that is optimized for the modern enterprise, where fewer applications are hosted on-premises and more users are working remotely. Unified security capabilities include threat protection, content filtering, and zero-trust network access. The Wandera Security Cloud enables threat defense, secure network connectivity, and robust data policies through a single cloud security platform.



- 
Founded 2015
- 
Employees: 11-50
- 
Subsectors: Threat Management/Security Operations, Data Security/Data Governance, Email/Communication Security, Employee Risk
- 
Regions of operations: Switzerland, Germany

xorlab's defense system understands people's communication relationships and behaviours. xorlab uses that understanding to proactively protect organizations against spear phishing, zero-hour malware attacks, accidental data loss, data exfiltration and non-compliance. With hundreds of signals gathered from every email, xorlab provides a level of visibility and control that allows security teams to efficiently automate threat analysis, prioritization and remediation, and realize a positive ROI on email. One mid-size private bank, for example, estimates that it can reduce its security operation efforts by up to 360k per year with xorlab, which is equivalent to 2 FTE. xorlab was founded by ambitious security and software engineers with the mission to redefine corporate cyber defence. The company started with email because that's where the majority of companies suffers the most with 90% of all security breaches involving email at some point during the attack.



- 
Founded 2015
- 
Employees: 101-250
- 
Subsectors: Data Security/Data Governance, Email/Communication Security, Risk Assessment/Risk Management
- 
Regions of operations: The Netherlands, United Kingdom, Germany and Belgium

Zivver delivers the comfort of safe communications for thousands of organisations using email and file transfer and video conferencing through their secure communications platform. Zivver customers meet compliance with data and privacy legislation when their employees send digital communications. This includes privacy-sensitive personal and banking information sent to clients, KYC communications, PII, or confidential M&A information. Typically security applications don't get used because they are too complex. Zivver's radical usability and unintrusive approach means users enjoy using Zivver for authentication and encryption, before, during and after a communication takes place. The platform prevents human error, the cause of over 75% of data leaks in the financial sector (source: ICO). With offices in London and Amsterdam, Zivver is the solution of choice for securing communication at over 4,000 organizations including Banks, Insurers, Accountancies and Financial Advisors. In 2020 Gartner named Zivver as a Global Representative Vendor for Email Data Protection.



ABOUT US

FinTech Global is a specialist data and research provider. FinTech Global offers the most comprehensive data, the most valuable insights and the most powerful analytical tools available for the global FinTech industry.

We work with market leaders in the FinTech industry – investors, advisors, innovative companies and financial institutions – and enable them to get the essential intelligence they need to make superior business decisions.

We cover every industry development, every investment, every exit and profile of every company in every FinTech sector around the world.

For more information, please visit:

www.FinTech.Global



ABOUT US

This summary was produced by RegTech Analyst.

The RegTech Analyst platform offers business intelligence on the RegTech, risk management tech and cybersecurity sectors. RegTech Analyst is the pre-eminent provider of data, research and analysis on the global RegTech market. We cover every trend, every investment and profile every company that provides a technology solution for compliance, risk management or cybersecurity. We deliver essential intelligence for mission-critical business decisions.

For more information, please visit:

www.RegTechAnalyst.com





For more information contact info@fintech.global

