imperva

EBOOK

Cyber Security and Compliance Guide for Financial Services

Introduction

The financial services industry is a high-value target for cyber criminals and securing data is a signifcant challenge for the financial services firms. This is not surprising given the vast amounts of sensitive data – customer transactions, account information and private personal data – that banks, payment card providers, payment processors and other financial institutions collect, process and store. According to the recent Cyberthreat Defense Report, nearly 66%[1] of IT security professionals believed that their organization's network would likely be compromised by a successful cyberattack.

As financial services organizations shift to digital channels, protecting data becomes even more challenging. Online banking applications, mobile transactions and multi-channel customer service are critical for revenue growth and improved customer experience. They also expand the attack surface, giving cyber criminals additional avenues to steal data and gain unauthorized access to financial accounts.

In addition to being in the crosshairs of cyber attacks, financial institutions face a growing number of signifcant regulatory requirements. These include Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI-DSS), the Monetary Authority of Singapore Technology Risk Management (MAS-TRM) and the new EU General Data Protection Regulation (GDPR). These data protection and privacy mandates, designed to safeguard consumers from fraud and protect the integrity of financial records by ensuring the security of sensitive data, increase regulatory compliance costs and risks for financial services organizations.

Financial services security challenges

- Defend against a constant barrage of cyber attacks and prevent data breach. Compounding this situation is the ever-changing volume, velocity and variety of attacks, which range from denial of service to malicious insider theft.
- Enable new digital channels while minimizing the security risk. While new online and mobile services are imperative to business growth, they also expand the potential attack surface.
- Demonstrate compliance with a growing number of government and industry regulations in a consistent and cost-effective manner

[1] Source: Cyberthreat Defense Report, Cyber Edge Group, 2019

What's at stake?

With the increasing number of high-profle security breaches impacting financial institutions globally, cyber security has shifted from being purely an IT issue to a board-level concern. The ramifications of data breaches are far reaching. Beyond the actual dollars spent to investigate and remediate a security breach, financial services firms can be impacted in many other ways:

- Financial losses that result from stolen funds.
- Lost customers and business revenue due to a lack of trust that the financial institution can and will adequately protect sensitive data.
- Drop in stock price as a result of lost business and reduced revenue.
- Reputation or brand damage that results when data breaches make the headlines.
- Legal costs associated with law suits fled by breach victims.

Even if data is not stolen, regulatory non-compliance can result in steep penalties for both the organization and executives. Consider the following:

- SOX non-compliance: SOX section 906 outlines penalties for certifying a misleading or fraudulent financial report. Under SOX 906, penalties can be much as $5M in fines and 20 years in prison.[2]
- PCI DSS non-compliance: Payment card providers can levy fines ranging from $5,000 to $500,000 for non-compliance. [3]
- EU GDPR non-compliance: Financial fines of up to 4% of annual worldwide revenue.[4]

Financial services industry is highly regulated and has one of the highest cost-per-record-breached among other industries - at $206 per record, which is % more than the global average.[5]

[2] Sarbanes Oxley Act of 2002, 30 July 2002, United States Congress

[3] "PCI noncompliance consequences," Focus on PCI

[4] Breaking news: EU agrees 4% fines for breaching data protection regulations, SC Magazine, 16 December 2015

[5] 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute

imperva

Multiple attack methods to reach the ultimate goal – Your data

At the end of the day, cyber criminals are after your valuable data. Why? Because they can monetize it. Approximately 88% of data breaches have a financial motive.[6] Whether it's selling personally identifiable data on the dark web, extorting money by holding sensitive data hostage or using stolen data to commit fraud, cyber criminals compromise applications and users to steal and monetize data.

Entire underground hacker markets exist for the sole purpose of monetizing stolen data. The black market for stolen credit and debit cards continues to thrive. Premium cards from major brands with magnetic stripe data sell for $15 - $110.[6] Internet bank account credentials are also popular items for sale. Cyber criminals sell stolen bank credentials for accounts located around the world. These compromised credentials, which can be used for account takeover attacks, sell for anywhere from 1 percent up to 5 percent of the account balance.[8]

As mentioned above, with their wealth of valuable data—customer information, banking and trading information, and confidential documents, financial institutions are prime targets for cyber attackers. It is imperative that financial institutions defend against a wide range of cyber threats.

Imperva addresses financial services organizations' critical needs for data and application protection as well as regulatory compliance as shown in the following table.

Imperva addresses financial services' needs

USE CASE	BENEFIT
Stop Denial of Service (DDoS) attacks	Shield critical online assets from a wide-range of DDoS attacks with always-on, scalable service
Protect Web Apps	Protect online banking applications from account takeover and exploitation of vulnerabilities
Safeguard Data	Defend against data breaches by pinpointing critical threats to your data and monitoring data activities in real-time
Mitigate Insider Threats	Detect and contain malicious, careless, and compromised users
Simplify Regulatory Compliance	Streamline audit and compliance for a number of regulations including, but not limited to, SOX, PCI, and MAS

6 2019 Data Breach Investigations Report, Verizon, 2019

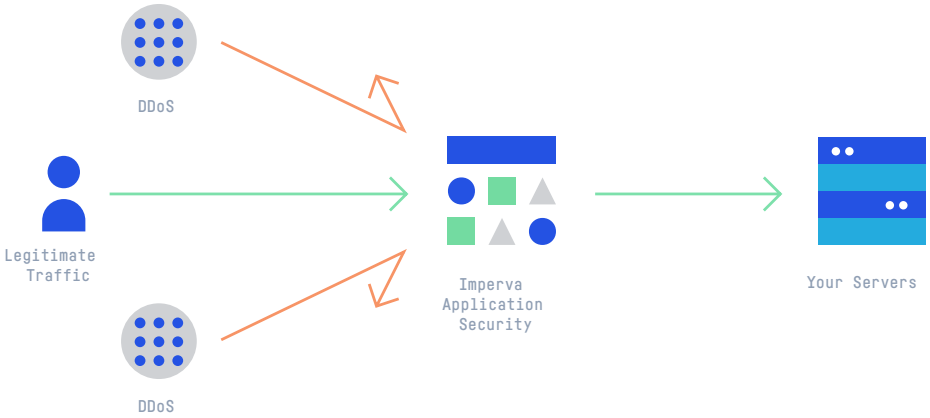
7 The Hidden Data Economy: The Marketplace for Stolen Digital Information, Intel Security, 2018

8 Ibid

Defend against DDoS attacks

DDoS attacks are designed to compromise the availability of a financial institution's public website. These attacks cause slow website response times and prevent customers from accessing an institution's public website to make transactions or open accounts. As more banks and consumers adopt online banking and trading applications, DDoS attacks are a major concern for financial services organizations. Denial of Service is the most common attack pattern for the financial services industry. This industry has also experienced the largest DDoS attack bandwidth and packet counts.[9]

The primary motivation of DDoS attacks is extortion. Cyber criminals threaten to launch a DDoS attack unless a financial institution pays the specified ransom. DDoS attacks also serve as a diversionary tactic for criminals attempting to steal money or data. DDoS attacks result in business disruption, reputation damage, lost revenue and reduced customer confidence.



Take for example, the DDoS attack against HSBC's online banking system in the United Kingdom back in 2016. HSBC was attacked on the last working day of month, a popular payday, and two days before the U.K. tax return deadline. Filers face a 3 percent penalty if taxes are not paid on time. As a result of the attack, customers were unable to access their accounts, transfer funds or pay bills during the attack.[10]

In response to the rising DDoS threat against financial institutions, the Federal Financial Institution Examination Council (FFIEC) issued guidance requiring banks and financial institutions regulated by the U.S. Federal Government to address DDoS protection as part of their ongoing information security and incident plans. Specifically, the FFIEC outlined six steps that financial institutions should follow for DDoS readiness. These steps include monitoring internet traffic to the institution's websites to detect attacks and activating incident response plans with Internet Service Providers (ISPs) to mitigate such attacks.

[9] 2019 Data Breach Investigations Report, Verizon, April 2019

[10] HSBC online banking down: Company's systems knocked offline by cyberattack," International Business Times, 29 January 2016

Imperva helps financial institutions shield critical online assets against DDoS attacks by:

- **PROTECTING AGAINST A WIDE-RANGE OF DDoS ATTACKS** including layer 3,4 volumetric attacks, low and slow attacks, and layer 7 application attacks.
- **SCALING BANDWIDTH ON-DEMAND** to absorb peaking attack traffic, which can be 10 to 100 times greater than standard Internet traffic levels.
- **MONITORING APPLICATION AND NETWORK TRAFFIC** to detect and stop malicious users and requests.

"When it comes to DDoS attacks, support is one of the most important factors is choosing a service. Imperva provides us with fantastic 24x7 support. We know that if something goes wrong, they are available."

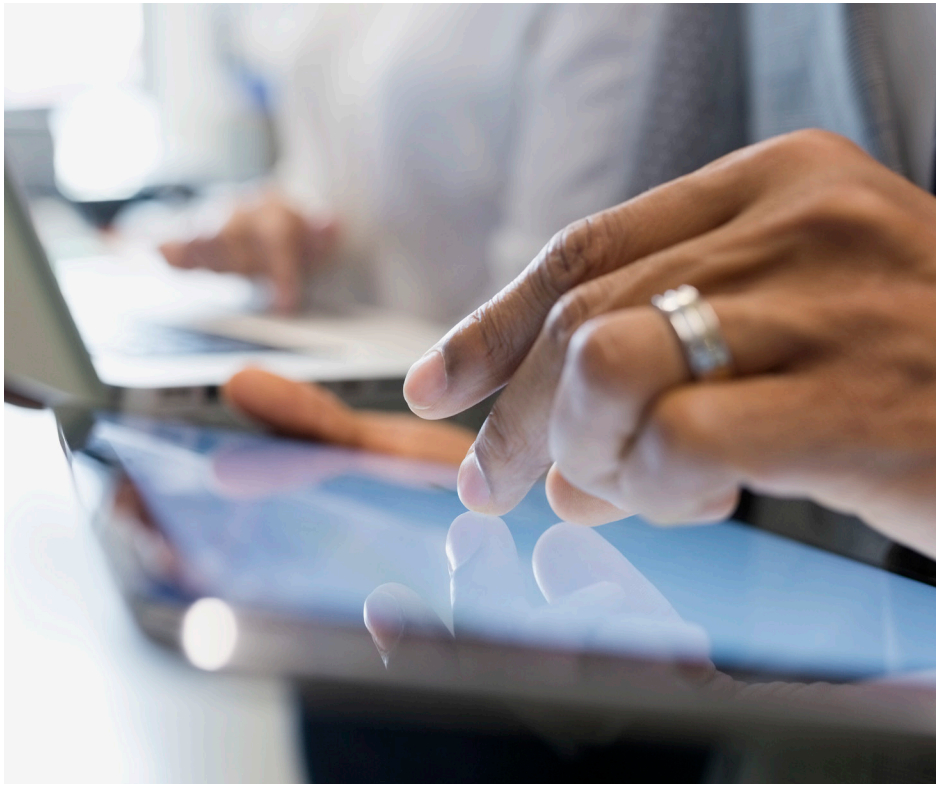
JONATHAN ASSIA,
CEO, ETORO

Protect web applications

Web applications such as online banking and brokerage accounts are popular targets for cyber criminals because they are the highway to critical data repositories. In fact, web application is one of the top three attack patterns and the number one source of data breach for financial services firms.[11] When it comes to financial web applications, two key attack vectors include account takeover and the exploitation of vulnerabilities in the application code.

Account takeover is usually the first step to committing fraud. Account takeover attacks involve the use of stolen credentials and bots to gain unauthorized access to customer accounts. Once criminals have successfully hijacked a customer's bank account, they continue on to commit fraudulent transactions.

Cyber criminals also exploit application vulnerabilities. Many online and mobile banking applications are custom-developed applications created by an in-house application development team or external, third party developers. When vulnerabilities are found in these applications, it can take months to develop, test and implement code fixes. That also leaves the web application exposed to attackers for months.



[11] 2019 Data Breach Investigations Report, Verizon, April 2019

Imperva includes the following capabilities to help financial institutions protect against web attacks:

- **WEB APPLICATION FIREWALL (WAF)** defends against a wide range of web application attacks including account takeover attempts and technical attacks like SQL injections. Implementing a WAF also enables financial services firms to virtually patch application vulnerabilities, reducing the exposure window from months to days.
- **RUNTIME APPLICATION SELF-PROTECTION (RASP)** adds another layer of protection to combat sophisticated attacks and secure applications in production in real-time. It monitors applications at runtime and automatically neutralizes threats in production before they become attacks. Can be incorporated during the software development cycle, reducing pressure on developer teams to immediately fix critical vulnerabilities.
- **ACCOUNT TAKEOVER PROTECTION (ATO)** empowers organizations to mitigate malicious ATO attacks without affecting legitimate users in the process. A multi-layered process which includes reputational analysis, advanced client classification, and behavioral machine learning accurately determines if the interactions with a website have malicious intent. Malicious logins are immediately mitigated closest to where they originate, long before they reach critical infrastructure.
- **ATTACK ANALYTICS CORRELATES AND DISTILLS THOUSANDS OF SECURITY EVENTS** into a few readable security narratives. It employs artificial intelligence and machine learning to simplify application security event investigations, enabling IT organizations to mitigate and respond to real threats quickly and decisively.
- **THREAT INTELLIGENCE IMPROVES DETECTION ACCURACY** and improves security operations by identifying new attack vectors and blocking known malicious sources.

Safeguard sensitive data

Given the vast amounts of sensitive data financial services firms collect and process, data security is a top priority. Many organizations have implemented perimeter security, data loss prevention, intrusion prevention/detection systems and endpoint protection. But today's exponentially complex financial services IT environment adds new data security requirements to protect data at the source. With cloud migration, data now resides in hybrid environments, both on premises and in the cloud. Multiple relational and non-relational data stores, instances and versions, often from different vendors, and geographically distributed systems that require coordinated policies, monitoring and enforcement—create security gaps between systems and applications, leaving these data stores vulnerable to attack.

When financial institutions factor in cloud computing, data security becomes even more challenging. Whether it's Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS), sensitive data is now outside the secure perimeter. As financial institutions develop their cloud strategy, extending on-premises data security and compliance requirements to the cloud will be front and center.

Traditional security approaches, such as perimeter and role-based security technologies, tend to lock down everything by default. This interferes with legitimate data usage and limits business growth. While these security technologies deserve enterprise attention, securing the data itself must be front and center of enterprise strategy. As threat actors continue to find ways through the corporate edge and to hijack the accounts of legitimate users, protecting sensitive data and ensuring that authorized data access is appropriate are the cornerstones of mitigating enterprise risk.

"I personally would recommend Imperva to other financial institutions... based on the fact that it brings world-class support, best-of-breed technology, and truly a solution that I think is cutting edge to a high-risk environment."

VP OF INFORMATION SECURITY,
REPUBLIC BANK

imperva

Imperva helps financial institutions safeguard data and mitigate data breach risks by:

- **DISCOVERING WHERE SENSITIVE DATA LIVES** – in the cloud and on-premises. The first step in protecting data is knowing where an organization's sensitive data is. Automated discovery and classification are the only reliable way to routinely and consistently discover and classify new or modified database instances containing sensitive data.
- **MONITORING DATA USAGE ACTIVITY ACROSS A BROAD RANGE OF DATA STORES**. While databases are a prime target for criminals, sensitive data exists in many types of systems–databases, Big Data platforms, data warehouse etc. And this data lives both in the cloud and on-premises.
- **IDENTIFYING CRITICAL THREATS TO YOUR DATA**. With more users accessing more data, it becomes difficult to identify bad user data access behavior. Additionally, security professionals often struggle with event overload and alert fatigue. Data risk analytics helps reduce the time to identify high-risk incidents and detect breaches. It automates the processing of massive amounts of alerts to provide actionable insights.

- **MANAGING USER ACCESS**. Attackers look for easy opportunities to access sensitive data. They target privileged user accounts, users with excessive access rights and dormant user accounts. To limit lateral movement of attackers and reduce the risk of data breach, financial institutions must proactively monitor privileged users, identify users who have excessive privileges and deactivate dormant user accounts.
- **MASKING DATA IN NON-PRODUCTION ENVIRONMENTS.** Data masking reduces the attack surface by eliminating sensitive data in non-production environments. Rather than creating copies of sensitive data for test and development teams or for market research purposes, financial institutions can enable these groups by replacing sensitive data with fictional but realistic data while maintaining data utility.

Detect insider threats

Inside jobs have been around for as long as there have been banks, and insider threats continue to be a major security concern for today's modern, financial services industry. A massive 73% of respondents stated that insider attacks have become more frequent over the past year.[12] Whether they're motivated by monetary gain or by damaging company reputations, these individuals are already inside your perimeter defenses. They are employees, contractors and partners that have legitimate access to valuable data.

Take for example, the case of insider theft at Morgan Stanley. Between June 2011 and December 2014, a former wealth management advisor conducted nearly 6,000 unauthorized searches of confidential client information and uploaded the information on 730,000 clients to his personal server.[13] Morgan Stanley was fined $1 million by the SEC for client breach of data.[14]

While the malicious insiders get most of the limelight, it's critical to keep in mind that insider threats extend beyond the disgruntled employee and include compromised and careless users as well. That's why insider threats are one of the most difficult to detect.

No discussion of insider threats would be complete without looking at privileged user access. Privileged users are perhaps the biggest risk when it comes to insider threats. A recent survey indicates that 55% of security professional report that privileged IT users pose the biggest insider security risk to organizations.[15] The very nature of their roles and the often un-fettered access to critical systems and sensitive data, make system administrators and DBAs prime targets for attackers. Compromising privileged user credentials essentially gives criminals the keys to the kingdom.

60% of all cyber attacks are carried out by insiders and the financial industry remains to be top under attack.[16]

[12] 2019 Insider threat report, Bitglass', 2019

[13] Guilty plea in Morgan Stanley Insider Breach," BankInfoSecurity, 22 September 2015

[14] "Morgan Stanley Fined $1 Million for client data breach," Wall Street Journal, 8 June 2016

[15] Resource: 2018 Insider Threat Report, CA Technologies, 2018)

[16] Source: Financier Worldwide, 2017

imperva

Imperva enables financial institutions to detect and contain insider threats by:

- **GAINING VISIBILITY INTO WHO IS ACCESSING DATA**. While many financial institutions trust their employees, they must also verify that trust is well placed. Real-time monitoring of all user access—including privileged user access—to databases and files on premises or in the cloud gives IT visibility into which users are accessing what data.
- **ANALYZING USER DATA ACCESS BEHAVIOR**. Establishing a baseline of "normal" user patterns via Big Data, dynamic profiling, machine learning and peer group analytics allows IT to identify anomalous data access. For example, a DBA typically works between the hours of 9 a.m. to 5 p.m. Suddenly the DBA starts accessing a database that contains sensitive data between 2 a.m. and 4 a.m, using a service account that should only be accessed by applications. Data risk analytics would detect and prioritize this anomalous data access as suspicious by analyzing both user behavior and data activity.
- **MONITORING PRIVILEGED USER ACCESS**: Proactive monitoring of all privileged access to databases, files and cloud applications helps financial institutions keep a watchful eye on system administrators and DBAs and protect critical IT assets from advanced cyber-3attacks.
- **ELIMINATING EXCESSIVE ACCESS RIGHTS:** Financial institutions can reduce the risk of insider theft by granting access to sensitive data on a business need-to-know basis.
- **MASKING DATA IN NON-PRODUCTION ENVIRONMENTS**. Data masking reduces the unnecessary spread of sensitive data and enables organizations to implement least privilege by replacing sensitive data with realistic, fictional data—such as changing names and identifying information or credit card numbers.

Streamline audit and compliance

Regulatory and industry compliance are major drivers of security investment for financial institutions. While compliance is certainly not security, compliance can provide a solid foundation for an information security program. After all, many of the data protection and privacy mandates are intended to protect consumers by ensuring proper security controls are implemented.

Compliance remains a daunting challenge for financial services organizations. Security requirements are found within a broad set of regulations and mandates, including PCI-DSS, SOX and MAS-TRM. Financial institutions require automated, continuous compliance across ever changing regulations in a dynamic IT environment.

"Imperva Data Security was the easiest solution to deploy and configure, and delivered the best performance in our tests. When we learned about its ability to also monitor and protect databases, we expanded our project scope and deployed this functionality as well. With Imperva we have a complete solution for data security and PCI compliance."

JEAN-PIERRE ZAITER,
CIO, INTUITION SYSTEMS

Imperva provides industry leading solution that helps financial institutions streamline auditing, reporting and compliance.

REQUIREMENT	REGULATIONS	IMPERVA CAPABILITIES
Discovery of sensitive data and assessment of risk, security gaps and vulnerabilities	PCI 2 PCI 6.1 MAS 2.0.1 MAS 2.0.5 SOX 302 SOX 404 GDPR Article 25, 32, 35	• Database discovery identifies active databases services and regulated data stored in databases and cloud apps. • Database assessment calculates risk associated with each database asset by evaluating data sensitivity, configuration flaws and vulnerabilities. • Cloud app discovery identifies all sanctioned and unsanctioned cloud apps accessed by users and rates risk of each cloud app.
Implement security controls	PCI 3 PCI 6.6 PCI 7 PCI 8.5 PCI 11.5 MAS 5.1.2 MAS 5.1.7 (c, d, j) MAS 12.1.6 SOX 302 SOX 404 GDPR Article 5, 25, 32	• Web application firewall (WAF) protects public-facing web applications. • Virtual patching provides a compensating control and allows organizations to block web application vulnerabilities. • Runtime Application Self Protection (RASP) neutralizes threats in production. • Account Takeover Protection mitigates malicious ATO attacks without affecting legitimate users in the process. • Cloud-based application delivery service protects websites against DDoS attacks. • User rights management helps implement least privilege and business need-to-know access. • Data masking eliminates use of sensitive data in non-production systems, helping to restrict access based on business need-to-know.
Audit, monitor and enforce	PCI 10 PCI 12 MAS 5.1.2 MAS 5.1.7 (b, e, f, j) SOX 302 SOX 404 SOX 409 GDPR Article 25, 32, 33, 34, 35, 44	• Database and file activity monitoring collects and records database and file access and activity details. • Alerts and optionally blocking abnormal access to regulated data in databases and files helps reduce risk of data breach. • Pre-defined PCI and SOX audit policies provide automated audit trail and simplifies compliance. • Privileged user access auditing provides monitoring of all privileged user activity, including direct database server access. • User data access behavior baselining identifies normal user data access patterns so variances can be detected.
Reporting	PCI SAQ or ROC SOX 302 SOX 404 SOX 409 GDPR Article 32, 33, 34	• Pre-defined reports for PCI, SOX and other regulations eliminate manual, error-prone and time-consuming compliance reports. • SOX change reconciliation shows SOX auditors that databases changes can be traced to an approved change request ticket.

Imperva offers industry leading cyber security solutions for financial services

Imperva is a leading provider of cyber security solutions that protect business critical data and applications in the cloud and on-premises. Financial institutions around the world rely on our solutions to protect their data and applications. Our customers include:

- Five of the top 10 U.S. commercial banks
- Three of the top 5 global financial services firms

Imperva enables financial institutions to discover assets and risks, then protect their most valuable information–customer information, accounts and transactions and financial records. We ensure user experience by stopping DDoS and botnet attacks and enable faster application release cycles by neutralizing threats in production. With Imperva, financial institutions can comply with the myriad of increasingly stringent data protection regulations and mandates, as well as enforce policies, entitlements and audit controls.

Global bank cuts $90 million in excess IT costs with Imperva. Check out the case study.

READ CASE STUDY HERE

Summary

Financial services companies are already highly-regulated. Securing customer data and business-critical applications from costly breaches and non-compliance adds one more layer. Imperva data and application security solutions protect data and apps wherever they live and allow your legitimate users to interact with them without frustration. With Imperva, you can:

- Safeguard customer transactions by protecting your applications from web attacks
- improve user experience by stopping DDoS attacks
- Automatically neutralize threats during production
- Mitigate data breach risks by identifying true risks to your critical data
- Meet various compliance requirements and provide forensics details

Imperva gives peace of mind to you, your customers, and your board of directors. And through FlexProtect, our unique licensing model, you can deploy Imperva data and application solutions how and when you need it. Your data and apps are protected regardless of the number, location or type of devices or services used. FlexProtect helps protect your data and apps wherever they live- in the cloud, on-premises or in a hybrid configuration.

To learn more about Imperva cyber security solutions for financial services, visit: imperva.com/go/financialservices

Protect the pulse of your business.

Imperva is an analyst-recognized, cybersecurity leader championing the fight to secure data and applications wherever they reside.

+1 [866] 926-4678
imperva.com

imperva