

# A D

S E C



2  
0  
2  
0  
Harden . Detect .  
Respond .

# Active Directory has become the primary target of attackers who stealthily raid companies' most vital assets.

Our industry wrongly modelizes advanced attacks as flows that begin outside your organization, fly through networks and endpoints to eventually reach your data and vital assets.

Unfortunately, this model ignores the ubiquitous, all-powerful overseer that orchestrates literally everything in your IT infrastructure: **Active Directory**. Which, as a consequence, receives too little attention from IT security specialists, and far too much attention from hackers.

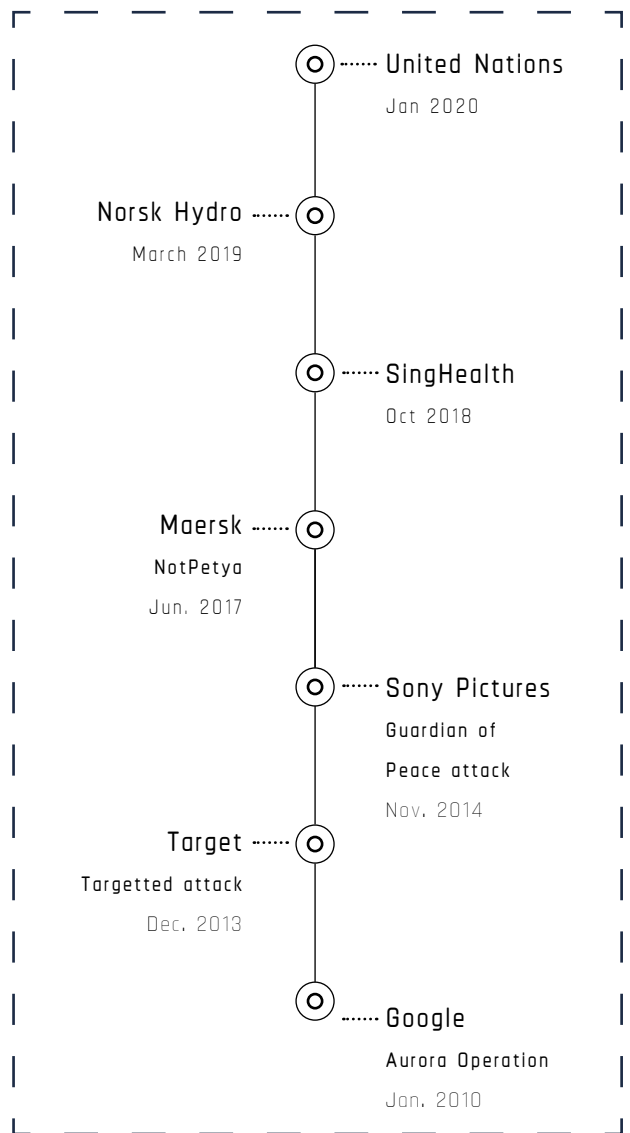
- 95% of Fortune 1000 is using Active Directory
- 100M security decisions are processed each day by large directory infrastructures
- 85% of administrators acknowledge that they have difficulty managing Active Directory's security models
- 10% of a company's annual turnover is the average cost of a remediation plan and it keeps growing

- 25 On 25 global enterprises audited...
- 95% 95% had a vulnerable AD
- 80% 80% had critical misconfigurations in place

## Why it matters

Active Directory infrastructures happen to be the focal point of your entire company security. User credentials, mailboxes, corporate or financial data: they are all ruled by the directory infrastructure, which acts as the master key holder for your company.

Yet, Active Directory's design makes it easily accessible and exposed to attackers seeking to reach your corporate network. It only takes one single compromised access to jeopardize the entire organization.



## Why current defense solutions are failing

- Most security tools focus on detecting attacks, but none of them improves the inner resilience of your AD architecture, or actually prevents attacks in the first place.
- Active Directory infrastructure is complex and evolves quickly. With thousands of concurrent security rules, a seemingly unimportant misconfiguration can cascade into several major vulnerabilities in a matter of minutes.

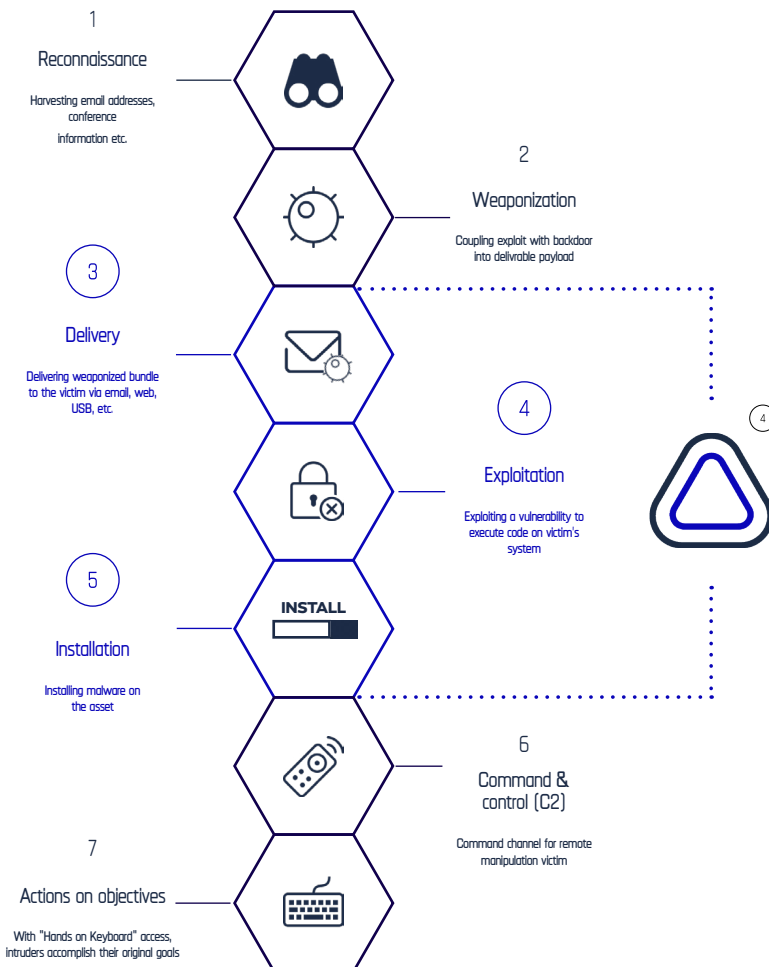
# ALSID re-invents AD security



Alsid hardens your directory infrastructure, enriches your SOC capabilities with AD threat detection, and empowers your incident response and hunting teams into investigating AD-related threats.



## Preventing the APT Kill-Chain using ALSID for Active Directory



### 3 Delivery

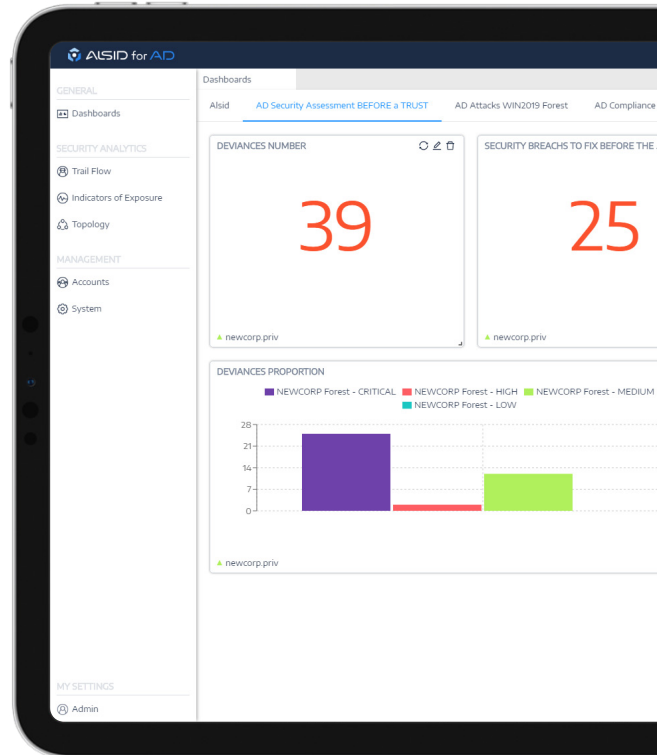
- 1. Prevent** - Alsid identifies exploitable delivery methods and notifies SOC teams in real time for preemptive fixing.
- 2. Detect** - Alsid detects on-going deliveries in real time and allows for immediate mitigation and remediation.
- 3. Respond** - Alsid's curated alerts and metrics empower IR teams to uncover root-causes as well as guide post-exposure responses and hardening processes.

### 4 5 Exploitation and Installation

- 1. Prevent** - Whether it's about misconfigurations or actual software vulnerabilities, Alsid guides SOC teams through the process of hardening their Active Directory and preventing exploitations.
- 2. Detect** - With the largest detection surface on market, Alsid spots on-going exploitations and triggers remediations at machine-speed.
- 3. Respond** - Alsid's detailed recommendations walk AD admins through the (otherwise complex) process of managing compromised objects, non-compliant servers, and toward hardening their infrastructure as a whole.

# Integrated platform

- Lightweight dashboard-oriented admin console.
- Centralized platform to manage multiple Active Directory infrastructures at the same time.
- Strong authentication mechanism thanks to MFA and isolated authentication database.
- Corporate, process-oriented outputs with built-in Excel to JSON export features.



## Customers speak highly of us

"Alsid integration was not only accomplished in a day, but it also provided efficient security monitoring on atomic infrastructures without any impact on the workload of security teams."

**Thierry Augier**  
Lagardère Deputy CIO & CISO

"Alsid's solution freed us from Active Directory security concerns so that we could focus on new business incorporation."

**Dominique Tessaro**  
VINCI Energies CIO

"Alsid is the answer to the two questions every CISO should be constantly asking – Are my domains adequately secured? And how can I independently prove it?"

**Jamie Rossato**  
VP, IT & Cyber Security



## About Alsid

Alsid is a cybersecurity vendor specializing in defending the common denominator of most attacks we see in the wild nowadays: Active Directory (AD) infrastructures. Our flagship cloud solution provides our users with step-by-step, tailored recommendations for hardening their AD, a real-time attack detection engine, as well as capabilities for investigating AD breaches when they unfortunately occur.

Today, Alsid is protecting more than 3 million users in more than 6 countries and helping major companies such as Sanofi, VINCI Energies or Lagardère stay safe against advanced attacks.

