



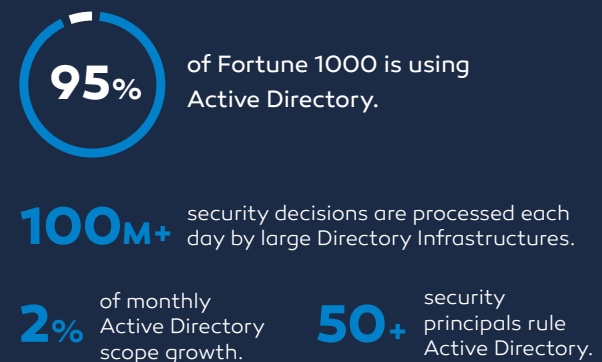
DETECT
ACTIVE DIRECTORY BREACHES
BEFORE ATTACKERS DO

Active Directory holds every key to your realms... ...and attackers know it.

Advanced attacks are based upon sophisticated methods, that go a way beyond malwares capabilities. However, common solutions continue to pursue the defense of endpoints (such as applications, network, mobile devices, etc.).

Meanwhile, advanced attackers will inevitably converge on the core system: Active Directory. They will gain access to all files and compromise the entire corporate network. Thus, by only protecting endpoints, your main gateway remains entirely unprotected...

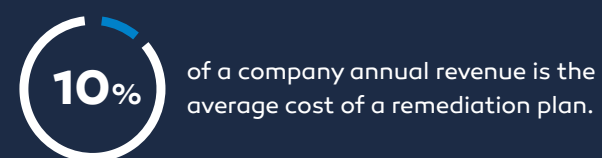
Facts



Nevertheless



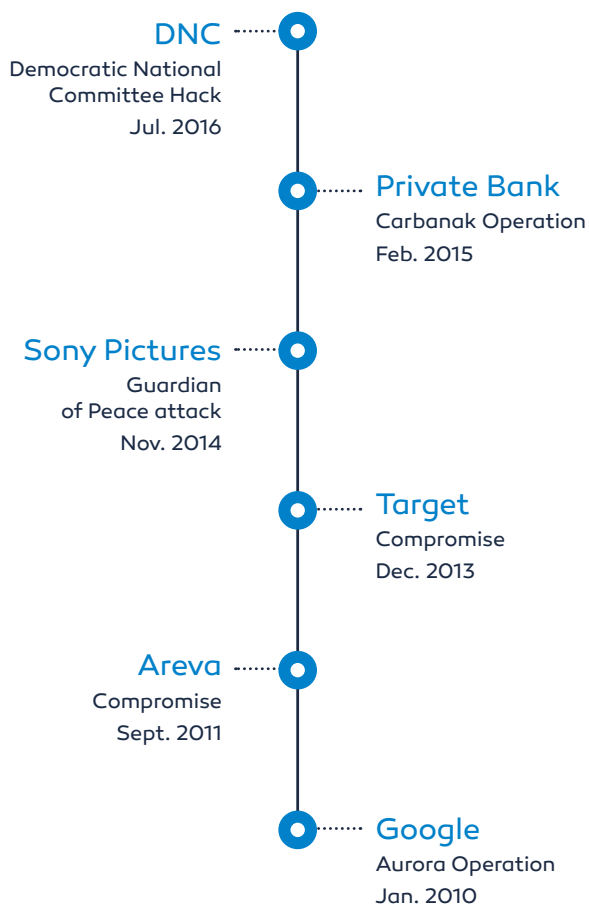
As a result



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 design makes it easily accessible and exposed to attackers seeking to reach your corporate network. Note: it only takes one single compromised access to jeopardize the entire organization.



Why current defense solutions are failing

- ▶ Traditional approaches focus on isolating Domain Admins and protecting credential theft from attackers who rely on unmanaged security configurations and access rights.
- ▶ Most security tools rely on detecting attacks. Reactive approaches never improve security; instead, they simply sound the alarm when the fire is already devastating your home.
- ▶ Active directory infrastructure is complex and evolving quickly. Made of thousands of security principals, boundaries can become major vulnerabilities in a minute when a misleading action is taken.

ALSID redefines real-time protection and security for Directory Services.

The first SaaS solution to isolate state-level breaches on your Directory Service and offer real-time a containment mechanism.

Key features



Measurement and in-depth understanding

- correct breaches before they turn into usable attack vectors
- reap the benefits of contextualized and efficient remediation plans



Self-improvement

- autonomously fits the curves and changes of your Active Directory as a whole.
- continuously probes for domain misconfigurations and known attack persistency tricks.



Alerting & monitoring

- proactively defeat new attack vectors (no more «false positive» or irrelevant reports).
- guarantee continuous oversight of your Directory Services



Upgradability

- continuously improved solution designed to quickly respond to threat evolution.
- continuously takes into account backdoor detection used by latest and most-advanced attack techniques.

How it works



How do we manage to do that?



Classic attack-defense paradigm reversing

Instead of waiting for attacks, DSC corrects breaches before they turn into usable attack vectors by monitoring, in real-time, every related security component.



Seamless deployment

Our non-intrusive, harmless solution just requires a basic user account and rights (same as an intern!), leaving your monitored infrastructure untouched. In addition, our solution is hardware-free and agentless.

A new breed of home-made and insightful indicators of exposure

- ▶ Unsecured trusts relationship
- ▶ Kerberos unconstrained delegation
- ▶ Weak trusted certificate authorities
- ▶ Security Descriptor

- ▶ Propagator consistency
- ▶ Bitlocker key access
- ▶ Privileged group membership
- ▶ DSRM account status

- ▶ Reversible password in GPO

... and 50+ more already released

ALSID integrated platform



Lightweight dashboard-oriented admin console.



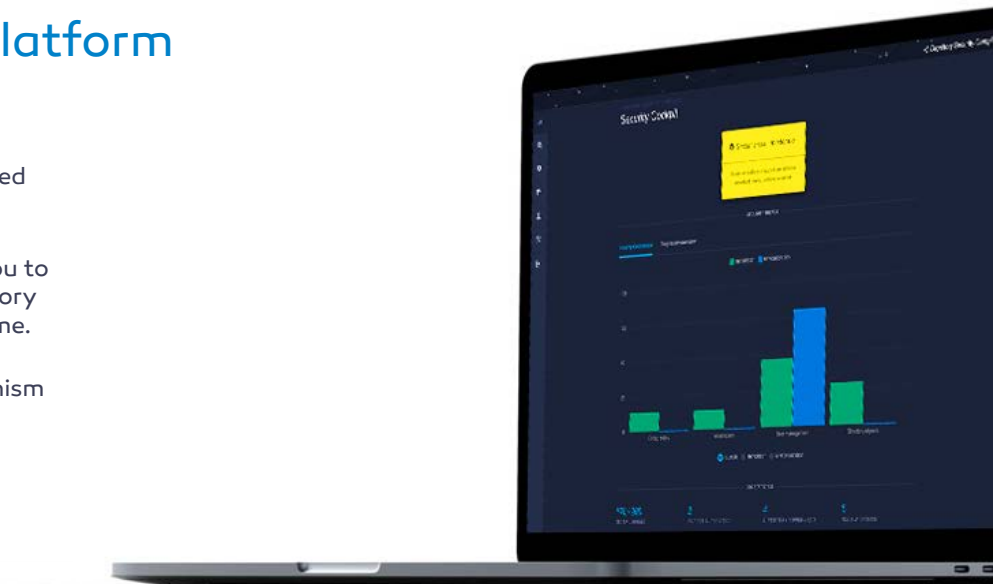
Centralized platform allows you to manage multiple Active Directory infrastructures at the same time.



Strong authentication mechanism thanks to MFA and isolated authentication database.



Corporate, process-oriented outputs with built-in Excel to JSON export features.



Strategic partners speak highly of us

- « AlsId's solution strikes the perfect spot by giving stakeholders a much-needed operational visibility on their corporate security.
- « By combining the founders expertise in Active Directory security with an innovative real-time approach, AlsId is able to prevent cyber attacks with a non-intrusive technology.
- « AlsId addresses a major governance and conformity issue using a robust and scalable technological platform.

Jean-Yves Poichotte
Global Head of ITS
Security at Sanofi

Pierre Polette
CEO at LEXSI Group

QuestionSecu.fr
February 2017

AlsId background

AlsId's founders are internationally renowned experts in Active Directory security. Before founding AlsId, they worked at ANSSI, helping dozens of major companies secure their infrastructures against advanced threats. Built on this field experience, AlsId's founders have pledged to redefine and upgrade the standards of security for Directory Services with their DSC software.

Learn more about us

 alsid.eu  [@AlsIdOfficial](https://twitter.com/AlsIdOfficial)  linkedin.com/company/alsidofficial

AlsId is endorsed by strategic partners

