Active Directory Holds the Keys to your Kingdom, but is it Secure?

A Frost & Sullivan White Paper

Swetha Krishnamoorthi, Industry Analyst, Cybersecurity, and
Jarad Carleton, Global Program Leader, Cybersecurity

FROST & SULLIVAN

CONTENTS

The Business Challenge 3

An Expanding Digital Ecosystem 3

Operationalizing AD Security 4

The Business Impact of Active Directory Attacks 5

Technology to Address the Business & Security Challenge 7

Intelligent Real-Time Active Directory Security is a Business Enabler . 9

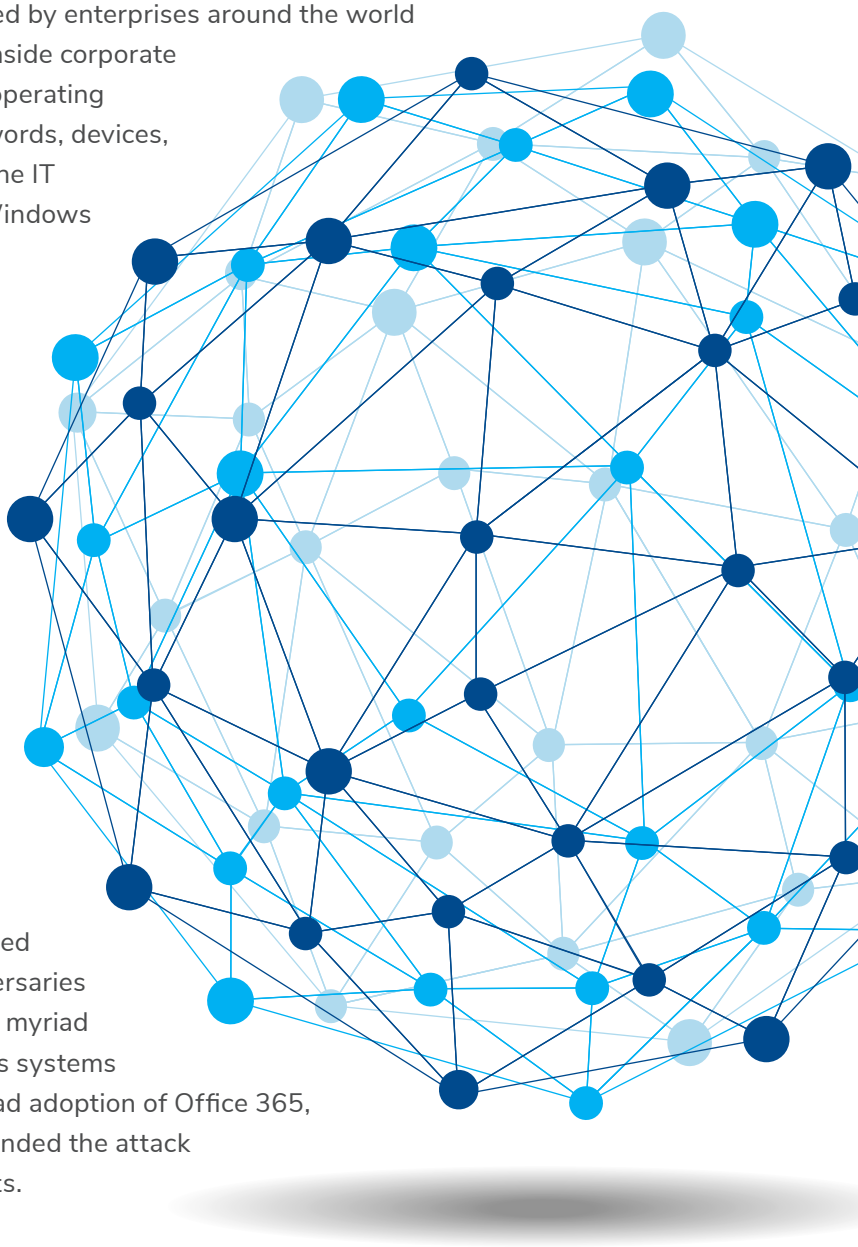
Alsid—Intelligent Automated Security for Active Directory . . . 11

Achieving Measurable AD Security Improvements with Alsid . . 12

An Alsid Customer Case Study 12

Conclusion. 13

Microsoft's Active Directory (AD) is widely used by enterprises around the world to connect and manage individual endpoints inside corporate networks. AD, built into the Windows server operating system, stores information about users, passwords, devices, applications, services, and operations across the IT infrastructure. It also and controls access to Windows networks, programs, and data.



To facilitate access control, Microsoft AD enables policy and data management with add-on modules such as Active Directory Users and Computers (ADUC) and Group Policy Management Console (GPMC). These modules help enterprises maintain visibility, security, and user experience for networked enterprise assets.

Today, Microsoft AD is the dominant mode of managing Windows domain networks. The use of AD is so common that approximately 90% of the Global Fortune 1000 companies use it as a primary method to provide seamless authentication and authorization.

Consequently, it has become a primary target for cyber adversaries to gain access to privileged company data. Once inside the AD, cyber adversaries can move across systems and gain access to a myriad of proprietary and business-critical data across systems managed by AD. Adding to this, the widespread adoption of Office 365, which uses AD to authenticate users, has extended the attack surface from on-premise to cloud environments.

THE BUSINESS CHALLENGE

An Expanding Digital Ecosystem

The IT infrastructure of enterprises is expanding in terms of volume and complexity. Diversity in endpoints, applications, and operations characterize the IT architecture of today's enterprises. Even workplaces are no longer limited to physical campuses. The trend of working outside of traditional office settings is accelerating in every region of the world, putting more demand on enterprises to provide remote network login capabilities for employees.

Unfortunately, many businesses are unable to extend their AD architectures to support modern digital workplace requirements. As a result, security teams are often faced with the choice of providing a relatively smooth user experience for remote workers accessing corporate assets or heightened security, which puts more restrictions on remote workers than for those inside a traditional office. In addition to those tradeoffs, an IT team has to manage issues such as privileged access for different

user profiles, and systems integration requirements where password-based or X.509 smart card-based authentication systems are not adequate for modern workplace requirements.

The AD requires continuous monitoring and analysis to stay on top of changes to environments and group policies. Adding to the complexity of a constantly-changing AD environment, Windows event logs from AD are technical and require manual searching or advanced PowerShell scripting skills. Further, it is impossible to collect and aggregate Windows event logs centrally at scale.

A cyber adversary attempting to take control of an AD environment will always be on the lookout for vulnerabilities after gaining entry into the network. For instance, the 2019 CrowdStrike Global Threat Report has introduced the concept of "Breakout Time." CrowdStrike defines breakout time as the time between an adversary's entry into the endpoint and beginning lateral movement[1]. It reported that in just 20 minutes, an adversary begins lateral movement, which implies that even a 20-minute delay between incident and notification could enable an adversary to gain control over the AD.

While it is essential to track in real-time every change in the AD environment, 80% of changes are benign. However, the high volume of AD event logs increases the challenge of pinpointing errors that could unintentionally increase the cyber risk for the organization and allow cyber adversaries to slip by undetected. Even when an organization has staff with the skill to use PowerShell scripts to aid in the detection of threats in Windows event logs, it is an inefficient and time-consuming process.

Operationalizing AD Security

Enterprise security budgets have grown in size over the past few years in response to the never-ending evolution of the cyber threat landscape. Although organizations have implemented numerous point solutions to gain visibility across systems and to detect and remediate threats, AD security has not kept pace with the growing complexity of the modern digital ecosystem. There are three common reasons for a poor AD security posture.

1—Many Highly Skilled AD System Administrators Are Not Security Literate

AD system administrators or managers focus on maintaining system uptime and too frequently lack an understanding of the security implications linked to their actions. For instance, when enterprises do not follow a policy-based approach to assigning user and administrative rights, some users may get privileged access to system-modifying features that should be restricted to specific administrators and user roles.

Access to domain controllers (DCs), servers that respond to security authentication requests within a Windows Server domain, should be restricted and highly secure. A cyber adversary with privileged access to DCs can modify, corrupt, or destroy the Active Directory and all systems and accounts managed by it. The challenge is that large enterprises with multiple branches and disparate information systems have many DCs to manage, and the problem can be substantially compounded following merger and acquisition activity.

Often there is not much difference in the privileges available for different administrator accounts such as workstation admin, server admin, exchange admin, help desk admins, or local admins. This, however, can contribute to a lack of visibility on any changes or privilege misuse in DCs, which can lead to a potential attack. With a haphazard privilege management policy and lack of clarity on individual user and domain privileges, the AD environment can be an easy target for cyber adversaries.

1 **https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/**

2—Active Directory Security Has Not Been a Top Concern

Although improperly configured Active Directory can allow cyber adversaries access to your keys to the kingdom, securing AD is not a top security concern for many enterprises. A study conducted by YouGov among 506 IT professionals in the UK confirms this hypothesis. Only 26% of survey respondents stated that AD security is a top priority for their organization[2].

Cyber adversaries have been able to begin their efforts to access the Active Directory of an organization with a simple web search. Many times, local administrators failing to practice proper security hygiene have made the jobs of cyber adversaries easier by using the same credentials across branches. Reuse of passwords has been so rife that in 2019, Microsoft found over 44 million Azure AD and Microsoft services accounts with compromised credentials that required a forced password reset[3].

In an ideal scenario, all administrator account credentials should be updated regularly. However, this is seldom the practice. The reason for the challenge: it is a cumbersome task to update all the various local and global admin accounts and their policies. Thus, anyone who may have received temporary access has a good chance of becoming a permanent inhabitant of the AD.

Of course, the chance of having long-term access privileges extends to cyber adversaries as well. For instance, in November 2018, Marriott revealed that one of its guest reservation databases (previously owned by Starwood) with over 500 million customer records was compromised as far back as 2014. A forensic analysis of the attack revealed that cyber adversaries took control of an administrative account and used the credentials to gain access to sensitive data such as credit card and passport information for over four years[4].

Despite a growing sense of password fatigue amongst workers, the use of simple and easy-to-guess passwords is increasing the cyber risk for organizations around the world. Based on the survey findings of the UK's National Cyber Security Centre (NCSC), 75% of organizations used passwords that were found in the top 1000 most common passwords in their Active Directory[5]. When such passwords are reused, cyber adversaries leverage them in password spraying to identify administrator credentials. Password spraying is a type of attack where cyber adversaries use a small number of common passwords against a large number of accounts.

3—Active Directory Security Specialist Shortage

Just as there is a global shortage of experienced cybersecurity professionals, the lack of focus on AD security has compounded the resource shortage for these types of specialists. IT teams and AD engineers have traditionally lacked the knowledge to incorporate security best practices and fully understand the scope of cyber risk associated with AD misconfigurations. Consequently, misconfigurations in the AD environment tend to go unnoticed, thereby significantly increasing the risk of attacks attributed to Advanced Persistent Threats (APTs).

The Business Impact of Active Directory Attacks

On March 19th, 2019, the aluminum giant Norsk Hydro, experienced production stoppages in its factories in Europe and the US. Upon investigation, the multinational company detected abnormal activity in its servers and realized it was in the midst of a severe ransomware attack.

2 https://www.helpnetsecurity.com/2019/11/06/active-directory-security/

3 https://www.microsoft.com/securityinsights/Identity

4 https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html

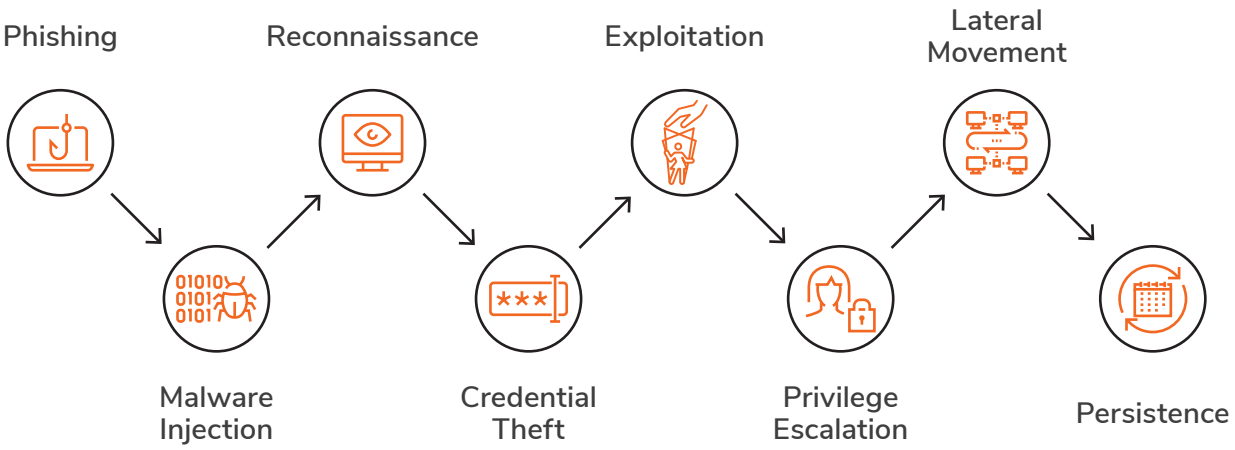
5 https://www.infosecurity-magazine.com/blogs/passwords-in-password-blacklist-1/

Through a targeted email attack called spear phishing, cyber adversaries installed ransomware called LockerGaga, which eventually spread throughout Norsk Hydro's network via Active Directory. The company had to disconnect approximately 22,000 computers from the network that control physical production units, forcing the company to switch to manual operations, and thus, disrupting production[6].

The company did not submit to ransom demands to restore production lines. Yet, the financial impact of the attack was massive. Operational challenges and financial losses during the recovery period put the impact estimate between $70 million to $72 million[7].

In 2019, reports of similar LockerGaga-based ransomware attacks were frequent. Some examples include the French Engineering Consulting firm Altran, Danish manufacturing company Demant, Government of Baltimore, and several others. A common thread running across many ransomware attacks is the exploitation of Active Directory vulnerabilities. Through a targeted phishing attack, cyber adversaries gain access to the network and then leverage commonly available toolkits such as MimiKatz, Metasploit, or Cobalt Strike to gain access to privileged user accounts. After getting access to domain administrator credentials, cyber adversaries can access Active Directory and plant ransomware. With privileged access, these cyber extortionists can disable any cyber defense mechanisms put in place by the company and move laterally across the network.

FIGURE 1: TYPICAL STAGES OF AN ACTIVE DIRECTORY ATTACK

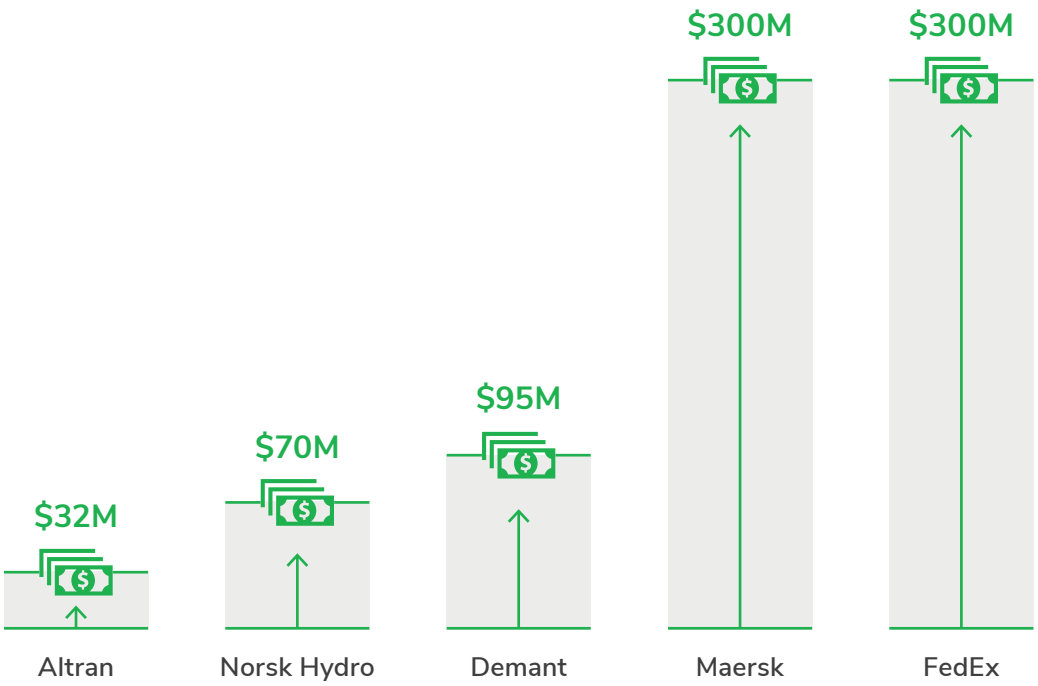


The number of such ransomware attacks exploiting AD vulnerabilities rose in 2019. A study by Emsisoft found that at least 621 government agencies, healthcare providers, and schools were hit by a ransomware attack between January and September 2019[8]. Besides, a report by NCSC claims that at least 1,800 businesses in the Netherlands were victims of a ransomware attack in 2019[9] alone.

When a poorly managed AD environment enables the lateral movement of the malicious software, the financial impact on enterprises can be significant. Exhibit 1 displays the publicly reported costs of a ransomware attack for five companies.

6 https://www.bankinfosecurity.com/hydro-hit-by-lockergoga-ransomware-via-active-directory-a-12207
7 https://www.hydro.com/en/media/news/2019/third-quarter-2019-ramping-up-production-in-brazil-declining-market-prices/
8 https://www.msspalert.com/cybersecurity-research/ransomware-attack-count-2019/
9 https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-3-ransomware-infecting-1-800-businesses/

FIGURE 2: FINANCIAL IMPACT OF RANSOMWARE ATTACK ON ENTERPRISES, 2019 (MILLION US$)



Thus, it is evident that cyber-attacks are not solely restricted to data theft. Most targeted ransomware attacks focus on extortion, business disruption, or physical damage to equipment. Moreover, the financial impact is severe and includes the cost of production disruption, information loss, revenue loss, damaged equipment, legal fees, cost of post-attack communication to end-user, compliance cost, and more. In addition to tangible costs, these cyber-attacks have damaged brand reputation. Frost & Sullivan statistical research examining the State of Online Digital Trust[10] has shown that cyber-attacks have led to a measurable loss of trust among customers that has a long-term moderate to strong negative impact on top-line revenues for almost 60% of all companies.

TECHNOLOGY TO ADDRESS THE BUSINESS & SECURITY CHALLENGE

Active Directory is a useful technology for the central management of disparate systems in the corporate network. At the same time, it does not include tools to quickly and easily identify security risks and system failures. Since administrators have wide-reaching access to confidential information, it is essential to keep a well-curated list of these accounts and their permissions so they can be continuously monitored for any suspicious changes. However, external cyber adversaries are not the only security risk. Indications of insider threats should also be monitored in the AD environment. Behavioral analysis technologies can help to develop standard behavior profiles for individual users and flag abnormal behaviors for closer examination.

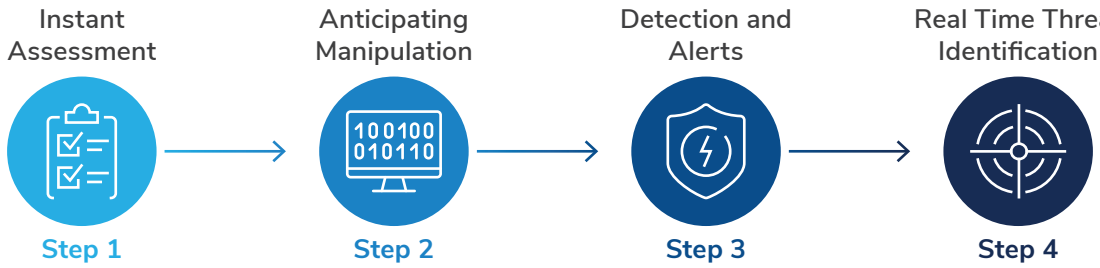
Detecting threats and vulnerabilities requires knowledge of the threat landscape that is continuously in flux. Understanding how the threat landscape is evolving is possible with threat intelligence feeds, but operationalizing that information is a common challenge, even in large enterprises with substantial resources.

10 https://store.frost.com/the-state-of-european-digital-trust.html

Further, weak password policies and leaked credentials are too frequently one of the root causes of AD security compromises. Requiring the use of unique complex passwords and regularly scheduled password updates will limit the probabilities of an attack, although these changes could necessitate the use of a password vault to help both administrators and end-users.

Watching account lockouts, individual user and group permissions, or any suspicious or noteworthy changes in the AD environment through command-line based queries is a daunting task, even for experienced security professionals. Further, malware begins lateral movement through the network as soon as it detects a bad configuration. Often, within a span of 4 to 5 hours, the malware can spread across the enterprise network. This means any change in the AD environment needs to be detected in real-time. PowerShell scripts can help to an extent, but are inefficient and lack the capability to monitor and detect changes in real-time. Often, IT or security teams do not have the expertise, resources, or time for manual maintenance and monitoring of AD environments, which contributed to increased cyber-risk for organizations. Unfortunately, the AD security challenge doesn't stop there because the expanding digital footprint of modern enterprise also requires continuous monitoring of cloud environments.

In a nutshell, to establish a proactive Active Directory security plan, the following steps should be followed:



Step 1—*Instant Assessment*

Instant assessment via an easy plug in solution for the AD to immediately identify existing AD misconfigurations that could lead to possible breaches. For instance, using the Alsid platform's indicators of exposure for immediate remediation of AD misconfigurations can dramatically decrease the risk score.

Step 2—*Anticipating Manipulation*

Anticipating whether "someone or something" is using an AD misconfiguration to manipulate organizational data. This can be addressed through an AD-SIEM integration feature, generating accurate AD-specific alerts, with no false positives that enrich the SOC operation.

Step 3—*Detection and Alerts*

Detection and alerts for attacks and changes within the AD that may open the system to vulnerabilities.

Step 4—*Real-time Threat Identification*

Proactive Threat Hunting to identify any changes in real-time. For instance, the Alsid platform includes a trail flow function that audits all ongoing AD changes in real-time and identifies any security events.

Many point solutions in the market only address specific aspects of AD security. For instance, some products conduct a gap analysis of AD security while some monitor changes in the environment or abnormal activity that should be analyzed by an administrator.

However, deploying or leveraging point solutions for each of these functions can be complicated, inefficient, and hard to manage. A holistic solution that addresses all AD security requirements is considered the best path for IT teams and security departments to achieve security maturity in AD environments.

FIGURE 3: FEATURE COMPARISON OF LEADING MARKET VENDORS

Alsid		Microsoft ATA
	Agent deployment	✓
	Requires account privileges	✓
✓	Security analysis of AD forests	
✓	Tracking all changes in AD environments	
✓	Tracking non-regular authentication	✓
✓	Misconfiguration detection	
✓	Realtime misconfiguration alerting	
✓	Routing alerts to SIEM	✓
✓	Visibility of administrator accounts	
✓	AD attack real-time alerting	✓
✓	Checking root domain permissions	
✓	Dynamic Dashboard and reporting	

Microsoft Advanced Threat Analytics (ATA) is a product tailored to the requirements of AD security. The company sometimes bundles this solution as part of its AD licenses for large enterprises. While the solution monitors and detects any behavioral anomalies, it does not go far enough to help organizations strengthen AD security.

The fast-paced nature of a cyber-attack combined with a critical shortage of AD security specialists means that organizations that are serious about hardening their AD security posture must embrace the use of advanced solutions, tailored to AD vulnerabilities. Intelligent, real-time AD security tools such as Alsid, enable enterprises to monitor and detect threats based on Indicators of Exposure (IoEs) and to integrate with SIEM or SOAR tools to support highly focused and contextualized remediation plans.

The use of intelligent real-time AD security tools helps enterprises understand where and how to harden AD security to detect insider threats as well as prevent AD environment attacks of external origin before attackers can inflict costly damage on a business. Also, the use of intelligent, real-time AD security solutions directly addresses challenges arising from the ongoing shortage of experienced AD security professionals.

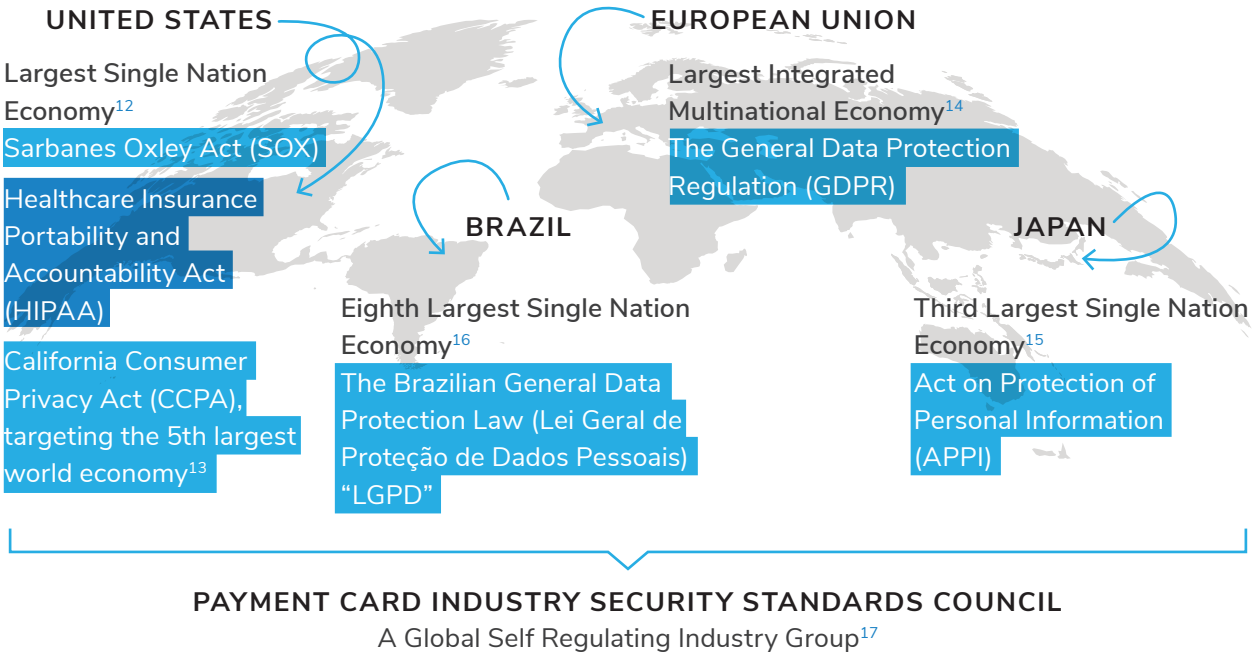
Intelligent Real-Time Active Directory Security is a Business Enabler

It is not a secret that the business impact of a compromised AD environment is high. In addition to brand damage, production stoppages, lost revenue, remediation expenses, potential fines, regulatory scrutiny, and medium to long-term impact on top-line revenue, a successful attack on an AD environment will significantly impact bottom line revenue.

It is also known fact that the cost of managing AD security in-house can be high, and that it has many potential limitations. The average cost of a security specialist with Microsoft Active Directory skills is about $65,000 in the United States and can go up to $90,000[11]. For large enterprises, changes in the AD environment happen frequently. It is essential to closely monitor changes in the environment to detect any potential risks or threats. However, the long-standing shortage of experienced cybersecurity professionals is getting progressively worse and for the specialty of AD security specialists, the situation is dire. An AD security specialist will have to execute 900 PowerShell commands to manage the AD environment proactively. Consequently, a security analyst can monitor changes in the Active Directory only once or twice a week as opposed to real-time monitoring. While robust scripts can help administrators gain control of the environment, the resulting complexity increases cyber risk because it is hard to manage. A common observation among enterprises is that there is only one person competent enough in the IT team to handle PowerShell scripts. This means that a scripting misconfiguration can easily go unnoticed, further increasing cyber risk in an environment that is already a favorite target for cyber adversaries.

In an acknowledgment that enterprise needs to become more secure, government regulations, and in some instances, industry self-regulation requires enterprises to ensure confidentiality, integrity, and availability of sensitive data. A brief look at some of the more well-known regulations and standards show that enterprise conducting business in major global economies or processing payment card transactions must be more proactive in closing security gaps.

FIGURE 4: WELL-KNOWN REGULATIONS AND STANDARDS



11 https://www.payscale.com/research/US/Job=Security_Analyst/Salary/308d520f/Microsoft-Active-Directory
12 https://www.investopedia.com/insights/worlds-top-economies/
13 https://www.bloomberg.com/opinion/articles/2019-04-24/california-economy-soars-above-u-k-france-and-italy
14 https://ec.europa.eu/trade/policy/eu-position-in-world-trade/index_en.htm
15 https://www.investopedia.com/insights/worlds-top-economies/
16 Ibid.
17 https://www.pcisecuritystandards.org/about_us/

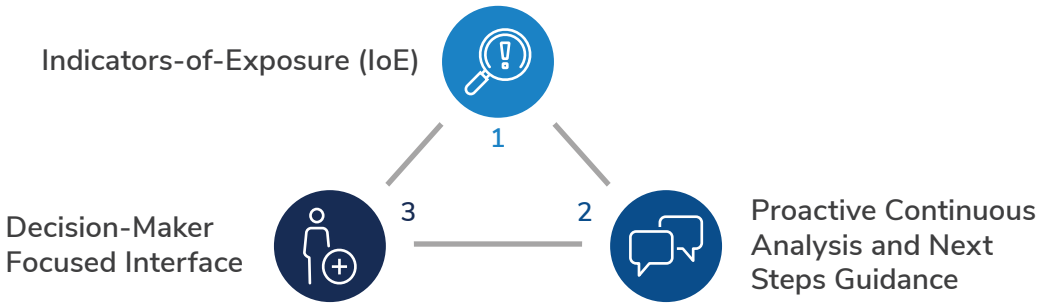
Each regulation requires enterprises to have infrastructure, policies, and processes in place to ensure that data is protected from destruction, loss, or unauthorized alteration. That includes things such as access control, auditing capabilities, and change management processes are critical aspects of these regulations. Failure to meet the minimum requirements of data protection mandates can result in significant fines and enhanced scrutiny by regulatory bodies.

Investing in an intelligent, real-time, and managed AD security solution is a business enabler for enterprises that understand the importance of eliminating chaos in enterprise AD environments that can unintentionally weaken an organization's security posture. Administrators can gain control over their network and prevent attacks without AD security specialists. Using Alsid's solution, even skilled AD administrators that are not security literate can monitor AD for suspicious changes, detect risks, threats, misconfigurations, and harden GPOs. With a managed service, CISOs or security teams need to spend a maximum of 30 minutes reviewing a vulnerabilities report to understand where and why changes should be made.

ALSID—INTELLIGENT AUTOMATED SECURITY FOR ACTIVE DIRECTORY

Headquartered in Paris, Alsid is a French security company that offers real-time active protection for AD infrastructure. Alsid's platform differentiates itself in the market by using an automated intelligent detection approach based on changes in the AD infrastructure rather than relying on Windows event logs.

Alsid's platform is based on three foundational pillars



1—Indicators-of-Exposure (IoE)

IoEs are potentially exploitable attack vectors such as misconfigurations or vulnerabilities that cyber adversaries can use to gain entry into the network. Alsid's solution scans the AD environment for IoE's and benchmarks enterprise AD security maturity against important security weak points.

2—Proactive Continuous Analysis and Next Steps Guidance

Alsid's AD security solution proactively scans and monitors the AD environment to detect well-known and emerging threats so administrators can be alerted in real-time to issues that increase cyber risk and can have severe negative impacts on business continuity. Simultaneously, Alsid can help enterprises improve AD security by assisting security teams to fix root causes and suggest remediation plans that have been developed by an Alsid team of AD security experts.

3—Decision-Maker Focused Interface

Alsid's platform provides administrators and CISOs with a valuable contextualized and consolidated view of AD environment security risks with recommended remediation plans. The platform also

integrates with SIEM or SOAR tools to provide benefits such as ease-of-use and an intuitive user interface.

ACHIEVING MEASURABLE AD SECURITY IMPROVEMENTS WITH ALSID

Alsid's team of Active Directory security experts continuously train the platform by adding new attack techniques and security best practices. The Alsid for AD security solution provides enterprise customers with advanced detection capabilities before they need it. With its API based integration to 3rd party security tools such as SIEM and SOAR, Alsid ensures that enterprise customers can secure AD environments via a single pane of glass.

Alsid's platform connects with the domain controllers of enterprise AD infrastructure. The platform employs an agentless installation to connect to the domain controller. With the help of a non-privileged account, Alsid scans and analyzes every object in the AD and rapidly pinpoints IoE. In as little as one hour, an organization can get a real picture of the weaknesses in its AD environment and understand where the most serious issues are. Following the initial baseline analysis, Alsid then shifts into monitoring mode where it detects any exploits and alerts the administrator. The administrator can then use an Alsid playbook or other industry best practices remediate potential threats.

An Alsid Customer Case Study

A European travel company with operations in 40 countries had a significant challenge in managing 20 different information systems across its organization. The absence of a unifying platform to centralize the management of information systems created a business-critical lack of visibility of end-user and administrative rights in the AD environment, which posed severe security risks. Without unifying a system in place to detect AD misconfigurations, the CISO's team was forced to rely only on open-source tools to paint an incomplete picture of AD infrastructure and potential security issues. However, even when an issue was discovered, the CISO struggled to find available resources to handle incident response and resolution.

Understanding that AD security is a critical business enabler, the CISO implemented Alsid as part of his strategy to rapidly improve the security maturity of his AD environments. Deployment of Alsid's platform took less than a day thanks to its agent-less, non-intrusive approach to connect to the customer's AD domain controller instance in the cloud. Preliminary results of a through AD infrastructure scan were available within 24 hours. Alsid accurately identified existing misconfigurations and vulnerabilities that could have exposed the company to attacks similar to those experienced by Norsk Hydro, Maersk, FedEx, Target, and the Democratic National Committee (US Democratic Party).

Post-implementation, the CISO was able to monitor system activity and, with the help of Alsid's dynamic reports, get an evolving and real-time overview of his organization's AD infrastructure. Alsid's recommended action plans to remediate potential threats and misconfigurations has measurably helped to decrease significant cyber risk factors that were present in the infrastructure, but previously hidden from view.

CONCLUSION

Active Directory is a business-critical component of modern IT infrastructure for both private and public organizations around the world today. Cybersecurity best practices suggest that business and government agencies using an AD should have real-time visibility of the security hygiene for AD environments, including user and administrator accounts, their policies, and privileges, abnormal behavior, policy violations, and unintentional misconfigurations.

While the use of PowerShell scripts is prevalent, it is also a tedious, expensive, and error-prone approach to detecting misconfigurations, vulnerabilities, and threats in real-time. Leveraging an intelligent and automated Active Directory security solution such as Alsid can springboard enterprises forward toward AD security maturity with full visibility and control over networked IT infrastructure and decrease cyber risk before it impacts business operations and revenue.

FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?