WHITE PAPER

How Active Directory Security Drives Operational Resilience

Why you need to strengthen identity threat detection and response (ITDR)

semperis

ISMG

The Need for Operational Resilience

As cybersecurity threats grow in sophistication and frequency, organizations are updating longstanding disaster recovery plans. While this is fundamental for responding to cyber incidents, it neglects the bigger issues of managing an incident, limiting its scope, and ensuring business continuity throughout its duration.

All of these steps are increasingly important in today's interconnected economy as organizations that depend on suppliers, vendors, and other third-party partners must ensure that they, too, are taking proper precautions.

The ideal big-picture approach for modern businesses now is operational resilience, which focuses on what must be done to keep a business running during a disruptive event. Operational resilience considers governance, risk management, crisis management, and the role of business partners — all in addition to best practices for cybersecurity incident response.

A cornerstone of operational resilience in the face of a cyberattack is identity — the IT function that enables users and systems to securely access mission-critical applications and services. When an identity service such as Active Directory (AD) must be shut down to stop a cyberattack from spreading, business operations screech to a halt. Quickly detecting and preventing identity-based attacks on AD enables organizations to reduce downtime, mitigate risk — and keep the business running.

> **The right Identity Threat Detection and Response (ITDR) tools and AD security best practices can speed recovery, automate incident detection, achieve significant cost savings, helping organizations better protect their reputations.**

How Active Directory Enhances Operational Resilience

As the primary identity service for 90% of organizations worldwide, "Active Directory is at the very core of your ability to operate and deliver business outcomes," according to Simon Hodgkinson, former CISO at BP and Strategic Advisor for Semperis. "It needs to be part of your operational resilience strategy instead of being treated as an island."

Entra ID, formerly known as Azure Active Directory, does for cloud-based resources what AD does for on-premises network resources.

Both are critical tools for modern identity and access management (IAM). They let organizations establish a single, role-based identity per individual user and — in theory — grant users access only to the resources they have permission to use for their role.

Top Challenges to Fixing Active Directory Vulnerabilities

- ✔ Lack of visibility
- ✔ Lack of time and resources
- ✔ Lack of attention from business leaders
- ✔ Complex inherited or legacy infrastructure
- ✔ Vulnerabilities missed in third-party audits

Source: 2023 Purple Knight Report

Unfortunately, AD is involved in 90% of cyberattacks.[1] Three characteristics of AD make it a common target. One is its prevalence. An attacker with the skills to break into AD can target most organizations. Another is its complexity, which stems from numerous configurable settings and features. The other is the presence of AD vulnerabilities, which are difficult to address for many reasons that range from legacy misconfigurations to weak passwords for privileged users.

Gartner has estimated that a third of organizations have no plans in place to defend AD from cyberattacks. AD breaches have hit organizations as diverse as Japan's Space Exploration Agency, MGM Resorts, energy firm Colonial Pipeline, shipping giant Maersk, and aluminum producer Norsk Hydro.

Anatomy of a Cyberattack

Attackers can hit an organization's AD installation in multiple ways, but one unifying factor in nearly all cyberattacks is the use of stolen or spoofed credentials to impersonate legitimate users.

Attackers often employ social engineering techniques such as phishing via email, text, or voicemail, or by creating fake Help Desk tickets.

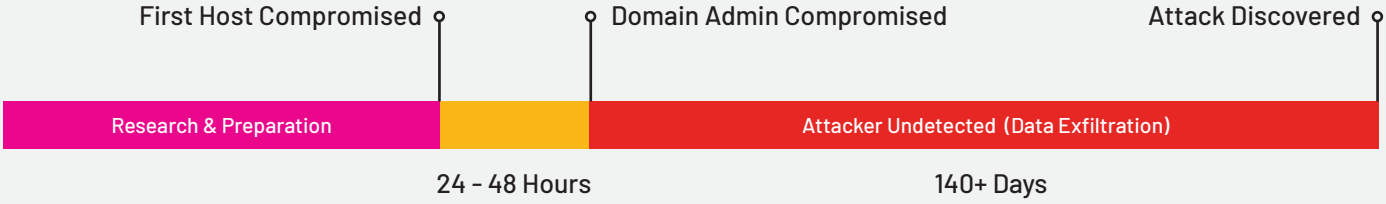
Once they gain network access, attackers work quickly to move laterally, searching for high-value accounts with elevated permissions. They use those privileged credentials to access the organization's domain controllers, which serve as the organization's central hub for identity and security authentication.

Within 48 hours or less, attackers can achieve their ultimate goal — control over critical assets, including the ability to manipulate operational systems, intellectual property, and sensitive personal information. Attackers may also deploy ransomware as a final step, encrypting critical systems after they have escalated their privileges and achieved control over key resources.

It's important to note that while some attacks move swiftly, others involve prolonged lag time, where attackers lurk around for weeks or months after initially gaining network access.

No matter how attackers get in or what they demand, the fallout can be severe, including significant downtime, revenue losses, legal and regulatory fines, and long-term reputational harm. In some cases, the cost of recovery can far exceed damages caused by the breach.

Typical Attack Timeline & Observations



ATTACK SOPHISTICATION

- ✔ Attack operators exploit any weakness
- ✔ Target information on any device or service

TARGET AD & IDENTITIES

- ✔ Active Directory controls access to business assets
- ✔ Attackers commonly target AD and IT Admins

ATTACKS NOT DETECTED

- ✔ Current detection tools miss most attacks
- ✔ You may be under attack or compromised

RESPONSE & RECOVERY

- ✔ Response requires advanced expertise and tools
- ✔ Expensive and challenging to successfully recover

Identity Threat Detection and Response

Gartner named identity threat detection and response (ITDR) as a unique cybersecurity market segment in late 2022. ITDR goes beyond the core identity management functions of an IAM by incorporating detection and response. It finds and closes vulnerabilities in the roles, privileges, and credentials assigned to individual identities in the IAM.

With so many organizations using AD, and with AD showing clear vulnerabilities, it's imperative for an ITDR strategy to provide specific protections for AD and Entra ID. From a technological perspective, ITDR includes but is not limited to real-time monitoring and assessment, automated detection and remediation, and risk-scoring capabilities to help IT and operational technology (OT) teams determine their next steps. Successful ITDR also depends on access to expertise, whether it's a battle-tested plan for AD recovery or a comprehensive post-breach analysis that helps organizations understand their vulnerabilities, reassess infrastructure, and make improvements to prevent future attacks.[2]

ITDR in Action: Altice Portugal

Telecommunications company Altice Portugal grew to 20,000 employees through mergers and acquisitions — a scenario that commonly creates vulnerabilities in AD ecosystems.

Given the ongoing threat of ransomware attacks, the company sought to make AD both secure and resilient. Altice Portugal turned to ITDR tools Directory Services Protector and Active Directory Forest Recovery from Semperis to leverage cybersecurity threat mitigation insights and recover AD five times faster than it did with its previous tools.

Source: Strengthening Identity Management System Defense at Global Telecom Altice Portugal

Comprehensive AD Protection Components

Shutting down operations to respond to an attack is untenable to many businesses today.That's why organizations should embrace an end-to-end strategy for AD and Entra ID protection. This type of strategy enables security leaders to take proactive measures before, during, and after an attack on a hybrid identity environment while at the same time seeking opportunities for continuous improvement.

Before an Attack

- Deploy automated and manual scanning tools to conduct an AD security assessment. Use the results to inform how the organization addresses exposure from a strategic and operational perspective.
- Discover vulnerabilities or risky configurations and use guidance from experienced AD threat researchers to close gaps before attackers exploit them.
- Develop procedures for provisioning, managing, and maintaining Tier 0 assets, along with access to privileged accounts.
- View disaster recovery from the context of identifying and resolving dependencies that may make it difficult to execute a DR plan in the moment.

During and After an Attack

- Analyze data from Splunk, Microsoft Sentinel, and other sources to detect advanced attacks, such as lateral movement through the AD environment, attacks that bypass agent- or log-based detection, or suspicious Help Desk tickets.
- Automate remediation in high-risk situations, such as changes to role assignments, group memberships, and user attributes, which are often an indication that an attack is under way.
- Isolate compromised accounts to mitigate an attacker from moving laterally.
- Automate AD forest recovery in a dedicated environment, whether virtual or physical, to ensure backups aren't infected with the same malware that caused an attack.
- Back up, recover and restore Entra ID group, role, and user objects both individually and in bulk, ensuring access to Entra ID resources in addition to the Entra ID system.
- Conduct post-breach forensics quickly enough to make a follow-on attack impossible.

Continuous Improvements

- Conduct ongoing AD security assessments and use the results to improve security posture and influence security strategy development.
- Create and update custom rules that further automate detection and remediation, enabling security operations teams to shift from 'firefighting' to focus their attention on broader strategic initiatives.
- Dynamically create and distribute reports for common compliance standards to ensure AD protection strategies remain up to date and in compliance.

Building a Business Case for ITDR

The technical benefits of ITDR are clear, enabling organizations to identify vulnerabilities, detect and mitigate threats, recover from attacks, and bolster AD protection strategies without the need for additional IT or security operations personnel.

However, to build a strong business case for ITDR, it's important to look at the bigger picture. Minimizing the impact of cyberattacks, or preventing them altogether, is good for business. Operations are restored quickly, if they're interrupted at all. Customers and partners are shielded from the impact of a data breach. The organization avoids reputational and financial damages from of having its name in the headlines.

The business impacts of implementing ITDR were recently quantified in a Forrester report. In its 'total economic impact' study, Forrester extensively interviewed five enterprises across four industry sectors, concluding that users of comprehensive identity resilience platforms can achieve notable operational and financial benefits as shown in the accompanying table.

It's essential to remember that implementing ITDR is not a one-and-done exercise. Attackers are constantly changing their tactics, and organizations must adjust their AD security strategies accordingly. That's why it's crucial to conduct ongoing AD security assessments and to use the results to make meaningful changes. A 2023 survey of users of Purple Knight, a free AD security assessment tool, found organizations averaged a 40% improvement of their overall score after applying practical remediation guidance to close security gaps included in the results of their assessment. This further illustrates the value of investing in ITDR tools and strategies capable of evolving to meet organizations' most pressing needs.

Operational Benefits of ITDR

90% reduction in Active Directory Forest recovery time

90% reduction in time spent in day-to-day operational security management

40% reduction in time spent monitoring a hybrid on-premises / cloud AD environment

25% reduction in likelihood of successful AD attack

Financial Benefits of ITDR

(measured over three years)

$4.3 million in savings from granular object- and group-level remediation that quickly restores normal configurations

$3.9 million in savings from improved business continuity due to faster hybrid AD attack recovery

$1.2 million in improved business continuity through reducing likelihood of a successful hybrid AD attack

$109k in savings from hybrid AD event monitoring efficiencies such as real-time alerts and automation capabilities

Source: Forrester Total Economic Impact of Semperis

The Future of Active Directory Security

Cybersecurity threats are increasingly difficult for organizations to thwart. For example, a 2024 global survey of IT and security professionals found that 83% of responding organizations were victims of ransomware attacks.

These organizations found themselves in a difficult spot:

Impact of a Ransomware Attack

- ✔ 87% suffered business disruption
- ✔ 61% needed more than one day to restore minimal IT functionality
- ✔ 37% suffered data loss
- ✔ 33% had to take all systems offline
- ✔ 35% that paid the ransom were still unable to recover critical information

Source: 2024 Ransomware Risk Report

Tellingly, only 27% of respondents to the survey had dedicated, AD-specific backup systems in place. With 90% of cyberattacks hitting AD, this is clearly a gaping hole in cyber defenses — and a missed opportunity for organizations. Fortunately, the right ITDR tools and AD security best practices can speed up recovery time, automate incident detection and response, achieve significant financial savings, and help organizations protect their reputation as a business partner that takes security seriously.

Semperis is a leading supplier of cybersecurity solutions. We understand the link between identity-first security and operational resilience. Enterprises around the world in industries such as education, finance, healthcare, and telecommunications trust Semperis to protect AD and Entra ID from escalating cyberattacks. Contact us now to learn about our AD offerings or request a demo of our industry-leading solutions.

[1] https://www.semperis.com/active-directory-security/

[2] https://solutionsreview.com/identity-management/why-itdr-should-start-with-active-directory/

About Semperis

For security teams charged with defending hybrid and multi-cloud environments, Semperis ensures the integrity and availability of critical enterprise directory services at every step in the cyber kill chain and cuts recovery time by 90%. Purpose-built for securing hybrid identity environments—including Active Directory, Entra ID, and Okta—Semperis' patented technology protects over 100 million identities from cyberattacks, data breaches and operational errors. The world's leading organizations trust Semperis to spot directory vulnerabilities, intercept cyberattacks in progress and quickly recover from ransomware and other data integrity emergencies. Semperis is headquartered in Hoboken, New Jersey, and operates internationally, with its research and development team distributed throughout the United States, Canada and Israel.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

BANK INFO SECURITY® CAREERS INFO SECURITY® CU Just for Credit Unions INFO SECURITY

Data Breach TODAY HEALTHCARE INFO SECURITY® GOV INFO SECURITY® infoRisk TODAY

CyberEd.io FraudToday.io PaymentSecurity.io DeviceSecurity.io

CyberEdBoard OT.today AIToday.io CIO.inc

QG MEDIA ATHENA CYBER THEORY GREYHEAD AN ISMG COMPANY Xtra mile LIFECYCLE MARKETING

iSMG

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io