WHITE PAPER

Active Directory Recovery: Pivotal to Business Resiliency Planning

Go from breach to bounce-back—fast.

semperis

iSMG

Why Active Directory Recovery Is Essential

With ransomware threats rising, businesses must be better prepared to protect their core identity and access infrastructure. Active Directory (AD) serves as the linchpin of enterprise authentication and access control. When it falls, so do business operations.

The statistics are staggering. Nearly 74% of businesses that suffered ransomware attacks in the past year were attacked multiple times, with 87% of those attacked[1] experiencing operational disruption. Attackers increasingly target AD because it grants them keys to the kingdom — enabling lateral movement, privilege escalation, and the distribution of malware across critical systems. Once inside a corporate network, adversaries can access AD in as little as 16 hours[2], locking businesses out of mission-critical applications and grinding operations to a halt.

Yet, most organizations are still largely ill-prepared for AD recovery. Only 27% of businesses have dedicated recovery plans[3], and those that do often underestimate the complexity of restoring AD without reintroducing malware or disrupting compliance requirements. Without a tested, automated AD recovery strategy, enterprises risk prolonged downtime, financial losses, and reputational damage.

The question is not if AD will be compromised — but how quickly and effectively a business can recover when it is.

74% **of businesses that suffered ransomware attacks in the past year were attacked multiple times.**

87% **of those attacked experienced operational disruption.**

27% **of businesses have dedicated AD recovery plans.**

Falling Short on AD Recovery

Despite the severe consequences of an AD outage, many organizations remain unprepared for a swift and secure recovery.

While businesses recognize the importance of securing their identity infrastructure, few have a fully developed and tested AD recovery plan. As a result, when AD is compromised, recovery efforts are often slow, uncoordinated, and vulnerable to reinfection — leading to prolonged downtime and financial loss.

Several challenges contribute to this gap:

1. **Complexity of AD Forest Recovery** – AD recovery is not a simple restore operation. Microsoft's documentation alone spans over 150 pages[4], requiring highly customized recovery workflows tailored to each organization's unique AD environment. A one-size-fits-all approach does not work.
2. **Lack of Testing and Readiness** – Many organizations struggle to replicate AD forest recovery in a test environment, making it difficult to validate recovery procedures before an actual crisis.
3. **Resource Constraints** – AD recovery drills are often deprioritized due to their perceived complexity and the tedious process of provisioning hardware for recovery. IT teams already stretched thin often assume AD is stable — until a breach proves otherwise.

Without a dedicated and well-tested recovery strategy, organizations risk days or even weeks of disruption, regulatory penalties, and long-term reputational damage.

Backup Isn't the Same as AD Recovery

To compensate for the lack of a dedicated AD recovery plan, many organizations assume that routine backups will be enough to restore AD in the event of an attack. This is a critical misconception. Here's why backups alone don't ensure recovery:

- **Malware Contamination** – Attackers often embed malware weeks or months before launching an attack, meaning that most recent backups are already compromised.
- **Data Loss Risk** – AD undergoes thousands of changes per day. If an organization must revert to an older, malware-free backup, it risks losing critical security policies, configurations, and authentication data that may potentially violate compliance requirements.
- **Time-Consuming Restoration** – Provisioning new hardware and manually rebuilding AD is a lengthy process, giving attackers a window to further spread malware before a clean recovery is complete.

A true AD recovery plan goes beyond backups. It ensures malware-free recovery, minimizes downtime, and restores operations without compromising security. Without these essentials, businesses are left scrambling in the wake of an attack.

How Active Directory Recovery Improves Operational Resilience

Forrester research underscores the high financial cost of AD downtime, with large enterprises losing millions per hour when AD is offline. Without purpose-built recovery tools, organizations can face up to 21 days[5] of downtime, compounding operational and financial losses.

A prolonged recovery window also increases the risk of reinfection, data loss, and regulatory non-compliance. To prevent business disruption, organizations need an automated recovery solution that:

- ✔ Restores multiple AD forests simultaneously to minimize downtime
- ✔ Ensures malware-free recovery, preventing reinfection from compromised backups
- ✔ Recovers AD even if domain controllers have been infected, maintaining operational continuity
- ✔ Rapidly provisions physical or virtual hardware for a clean, non-compromised recovery environment

Automation is key to reducing downtime. Forrester estimates that organizations using automated recovery tools can cut downtime by up to 90% — from 21 days to as little as 5 hours[6].

However, AD recovery must go beyond incident response. A resilient approach should not only restore AD but also prevent future attacks through a proactive, end-to-end strategy.

The three core pillars of effective AD recovery include:

1. **Proactive, Automated Backups** – Regularly scheduled, AD-specific backups ensure that organizations can restore AD quickly and with minimal data loss. Automated scanning and validation also help identify and eliminate hidden malware.
2. **Pre-Tested Recovery Plans** – Organizations must move beyond generic recovery guidance and develop customized, well-tested AD forest recovery plans tailored to their unique AD environments. The right automation tools ensure recovery teams can act immediately instead of manually navigating complex documentation.
3. **Identity Forensics & Incident Response (IFIR)** – Without a thorough identity forensic investigation, attackers may still have backdoors into AD, leaving the business vulnerable to repeat attacks. Identifying indicators of compromise (IOC) and indicators of exposure (IOE) ensures the environment is truly secure before restoring operations.

Semperis Active Directory Forest Recovery automates the entire recovery process with a 5-click restoration system, reducing downtime from weeks to hours. Unlike manual 28-step recovery processes that are prone to delays and misconfigurations, Semperis enables enterprises to restore AD efficiently, securely, and with minimal disruption to business operations.

To Secure Board-Level Support, Demonstrate AD's Bottom-Line Impact

Lack of support from the Board of Directors is a common obstacle to addressing cybersecurity issues such as Active Directory recovery. Despite the financial and reputational damage that ransomware has inflicted, only 30% of businesses plan to increase their security budgets.[7]

When it comes to AD, IT and security teams can overcome this obstacle by shifting the conversation to mission-critical applications. It could be the ecommerce site for a retailer, for example, or the electronic health record system for a hospital. A simple tabletop exercise can demonstrate what happens when AD goes down and, all of a sudden, no one can access these essential systems.

When C-level executives and board members see that key applications cannot be recovered without the vital authentication and login capabilities that AD provides — and that AD recovery can take weeks using outdated manual processes — they will be quick to see the value proposition for AD recovery.

How Active Directory Recovery Aids Regulatory Compliance

Due to unique industry needs, businesses in finance, healthcare, insurance, and other heavily regulated industries benefit from AD recovery solutions that go beyond uptime and operational continuity guarantees. These businesses need solutions capable of addressing two important elements of regulatory compliance.

First, strong procedures and controls are necessary to secure sensitive information, per government regulations. Compliance with the European Union's Digital Operational Resilience Act (DORA), for example, requires financial institutions to implement a well-documented risk management framework for IT and communication systems. When it comes to AD, that means proving a company has full visibility over its AD configuration, can control its AD environment, and can recover AD if anything goes wrong.[8] In the United States, meanwhile, new Securities and Exchange Commission cybersecurity incident response and disclosure rules put the onus on companies to assess, test, and strengthen their AD disaster recovery plans. Such requirements further point to the value of automated AD forest recovery.[9]

Second, robust AD security provides a real-time audit trail of any AD changes, inactive accounts, and modifications to privileged accounts. Audits are essential for compliance purposes, and they're equally vital for identifying and closing security gaps within an AD environment. This helps the business protect sensitive data, remediate potential threats, and maintain compliance even in a changing regulatory landscape.[10]

It's important for businesses in heavily regulated industries to evaluate their options. The ideal strategy not only accounts for data protection but also is tailored to AD security and recovery workflows and processes that meet compliance requirements, out of the box. The last thing a business wants to discover amid responding to an AD attack is that its partner isn't equipped with the tools and expertise necessary to recover in a manner that can ensure proper regulatory compliance.

Augment AD Recovery with Semperis and Cohesity

Semperis recently announced a partnership with Cohesity to further improve incident response and recovery and enable companies to benefit from the combination of data security and identity security.

"By helping our joint customers identify and close off attack paths leading to the organizational backup and recovery system, we can prevent data exfiltration and preserve the recovery option, removing one of the primary negotiating tactics threat actors have," Semperis CEO Mickey Bresman said in a statement.[11]

The combined Semperis-Cohesity backup and recovery solution includes four components:

1. AD backups are transferred to Semperis Active Directory Forest Recovery at regular intervals. This ensures backups are secure and malware-free.
2. Backups optimize network bandwidth use. This ensures rapid data transfer, which is critical when time is of the essence for AD recovery.
3. Verification checks ensure the validity of backup data. This ensures the most recent AD changes have been captured in a backup.
4. The backup copies are secured by Cohesity's hardened platform, which is immutable and provides recovery at high speed and scale.

In addition, the Semperis-Cohesity partnership provides file auditing and data management controls to support an organization's compliance efforts. The recovery process also includes post-breach forensics, with an emphasis on eliminating backdoors that intruders are likely to exploit.

Through the partnership between Semperis and Cohesity, businesses are empowered to minimize the impact of cyberattacks, avoid disruptions to operations, coordinate an end-to-end response, and strengthen their security defenses. This will make them less susceptible to an attack on AD and better equipped to bounce back should an attack occur.

The Future of AD Recovery and Resilience

Given its important roles in business operations, identity management, and administration, Active Directory is likely to remain a popular target for threat actors. Successful attackers have no shortage of options, either. They can leak sensitive information, sell it, or hold it ransom. They can launch denial-of-service attacks that cripple a network. They can install malware and launch additional attacks anywhere they choose.[12]

Cybersecurity leaders would therefore be wise to protect AD against such threats. Proactive steps include implementing extended detection and response (XDR), monitoring user behavior as well as network traffic, and prioritizing security information and event management (SIEM). These actions help alert businesses to signs of malicious or otherwise abnormal activity that require attention and remediation.[13] Strengthening access controls, authentication policies, and security baseline configurations can also harden the AD environment, making it more difficult for attackers to get in.

Preparing for AD recovery, and not just backing up the AD environment, is also essential for building stronger operational resilience. Solutions that automate workflows for threat containment, response, and forensic data collection — and refer to a well-defined recovery plan tailor-made for unique business and regulatory requirements — can shorten the AD recovery timeline by as much as 90%. That news should also help cybersecurity leaders make the case to executive leadership that AD security and recovery is a worth the investment.

Together, Semperis and Cohesity offer an industry-leading solution for automating AD security and recovery. Learn more about integration of Semperis Active Directory Forest Recovery and tools such as Cohesity FortKnox and Cohesity DataLock, or request a demo of Semperis offerings for AD security, recovery, and modernization.

[1] 2024 Ransomware Risk Report. Semperis. July 2024.
[2] Time keeps on slippin' slippin' slippin': The 2023 Active Adversary Report for Tech Leaders. Sophos. August 23, 2023.
[3] 2024 Ransomware Risk Report. Semperis. July 2024.
[4] Active Directory Forest Recovery Guide. Microsoft. November 2024.
[5] The Total Economic Impact of Semperis. Forrester. May 2024.
[6] The Total Economic Impact of Semperis. Forrester. May 2024.
[7] 2024 Ransomware Risk Report. Semperis. July 2024.
[8] The 5 Pillars for DORA Compliance in Active Directory. Semperis. October 2024.
[9] What You Need to Know about SEC Regulation S-P Requirements and Active Directory. Semperis. December 2024.
[10] Maintaining Information Security Compliance Through Active Directory Services. Semperis. June 2023.
[11] Semperis Partners with Cohesity to Help Automate Active Directory and Close Attack Paths Leading to Recovery Systems. Semperis. August 2024.
[12] The Weaponization of Active Directory: An Inside Look at Ransomware Attacks Ryuk, Maze, and SaveTheQueen. Semperis. June 2023.
[13] Active Directory Hardening Best Practices. Semperis. April 2024.

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 INFO SECURITY (Just for Credit Unions)

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