semperis

2021

Active Directory Security *Halftime Report*

Insights and resources for improving hybrid identity security

Active Directory is under attack.

Cyberattacks are escalating across every industry, and the prime target for cybercriminals is identity systems: Mandiant researchers reported that 90% of the incidents they investigate involve Active Directory in some way.

But organizations can take action to defend their hybrid identity systems from cyberattacks.

The **Active Directory Security Halftime Report** addresses the surge in identity-related attacks—from the Colonial Pipeline breach to the Windows Print Spooler vulnerability—with expert advice on hardening identity security postures that have eroded through years of neglected misconfigurations and lagging skillsets.

Written by Semperis identity experts—many of whom are multi-year Microsoft MVPs—this resource provides practical skill-building guidance for preventing and mitigating identity-related attacks.

"If there was ever a time to re-examine the security of your Active Directory, it's now," said Mickey Bresman, Semperis CEO in a recent Help Net Security article. "Many organizations appreciate the importance of Active Directory but are a step behind in securely managing it. Make it a priority to implement comprehensive threat monitoring, detection, and response capabilities both on-premises and in the cloud."

Table of Contents
Halftime Report | 2021

CEO PERSPECTIVE
WITH MICKEY BRESMAN

Fundamental identity security practices need serious attention to curb cyberattacks

After a half-year of escalating cyberattacks across every business sector and around the world, Semperis CEO Mickey Bresman reflects on cybersecurity trends that will define the near-term battle against malicious attacks that threaten business revenue, public safety, and national security.

Why are companies still struggling to implement fundamental Active Directory security practices?

First, Active Directory has been around for 20 years and in the beginning, security was not necessarily top of mind for the teams configuring AD. In fact, many of the assumptions that existed in the industry in the early days, turned out to be insecure. The reality is that for 20 years, AD been modified in most organizations multiple times, by different people, and it cares a heavy security debt. Combine that with the fact that AD is now serving a much more complicated digital enterprise: Every environment has many different levels of permissions and complexities.

AD remains the beating heart of identity management—the core of the identity platform for most organizations—but everything around it has changed rapidly. Basic AD hygiene was not as much of a concern 15 years ago, so a lot of the mistakes that were made then are the problems you now need to address. I would also call out the lack of skillsets: You have people that know AD extremely well, but their thinking is more operationally related. Or you have people that know red-teaming and security extremely well, but they are not AD experts. It's not that simple to find that combination of skills in a single person.

What can companies do in terms of skills-building or organizational structure to break down siloes between IT and security

Identity should definitely be part of the broader cyber security story in the company. Anyone in charge of identity should think cybersecurity first. Since we know that many organizations are dependent on Active Directory in order to run day-to-day operations and to continue those operations after a cyberattack, how do you make sure that in the worst-case scenario, you're able to restore that functionality as fast as possible? We are seeing some companies start to transition the responsibility for identity to the security side of the house. And even with organizations where identity remains with the operational side, we now see more security awareness at the IT professional level and higher collaboration between the security and IT teams—especially in managing identity and Active Directory.

This is an encouraging trend, in my view: If you are in charge of any function in the identity space, you need to be security-oriented.

What security challenges come with managing a hybrid identity environment?

We see a lot of different challenges with managing hybrid identity environments, starting with the basic fact that Active Directory and Azure Active Directory—outside of the name—have very few things in common. Azure AD provides a different stack of protocols, requiring a very different management approach—including protecting the identity system from cyberattacks. For example, in some configurations, when I make changes to identities in the cloud, that action affects my overall security posture in the data center and various cloud applications. With a hybrid scenario, the potential attack surface expands for an adversary. It's a relatively common scenario to see attacks start on-prem and move to the cloud, or move from cloud to on-prem. In one broadly discussed breach, the adversary accessed the organizational Azure AD on one side of the corporation, extended to the AD on-prem environment, latterly moved to another side of the organization, and moved from there to another Azure AD tenant. Organizations now need to think about what changes are made to identity systems in each environment, and how the connectivity between the two can create an entry point for adversaries.

Managing security in a hybrid environment also brings to the forefront the shared responsibility model: Microsoft's (or any other IDP's) responsibility is to make sure that the service continues to operate. Although they will provide you tools that can help with securing the environment, what you do with your environment—including securing it—is your responsibility.

How long will the hybrid environment be in play for most organizations?

Most of our customers will never leave their data centers completely behind. Potentially the hybrid model will be here forever. Companies will consider what makes sense to continue to run in the data center and what makes sense to use as a service provided by Microsoft, AWS, Google, or another provider. Companies can now mix and match the best solution for their scenarios and requirements. The cloud is not the answer to everything.

But regardless of the particular mix of on-premises and cloud systems and assets, you will need to protect the identity store. Identity is going to continue to play a huge role in the protection game that we are playing against the adversaries. You should also assume that as you continue the digitalization and cloud adoption process, protecting identity will become even more critical to your operational and security strategy.

UNLEASH PURPLE KNIGHT

Purple Knight Empowers IT and Security Teams to Uncover Active Directory Security Gaps

With thousands of downloads to date, the free AD security assessment tool helps organizations identify and address security gaps that adversaries frequently exploit in cyberattacks

The release of the Purple Knight security assessment tool in March 2021 tapped an unmet need to identify and address security gaps in Active Directory. Thousands of IT and security professionals have downloaded the free tool, built by Semperis identity experts, which scans the Active Directory environment for 60+ Indicators of Exposure (IOEs) and Indicators of Compromise (IOCs).

"None of us expected this level of acceptance of Purple Knight in the market," said Mickey Bresman, Semperis CEO. "But it's a good surprise, as organizations are now able to make a direct connection between attacks they see in the wild and the security weak spots in Active Directory. Organizations are requesting Purple Knight to make sure their AD environments are prepared for these types of attacks."

Bresman said customer feedback indicates that Purple Knight uncovers vulnerabilities that even consulting companies miss, a benefit that he attributes to the Semperis team's deep understanding of Active Directory—and how organizations use it.

"We saw that many companies don't have a good understanding of the Active Directory exposures that adversaries are able to use against them," said Bresman. "We wanted to give security teams that don't have deep AD expertise a way to understand their AD security posture—and then close any existing gaps so that adversaries won't use those against them."

Purple Knight scans the AD environment to identify security gaps from malicious activity or from misconfigurations that might have lurked in the system for years. Ran Harel, Semperis Senior Security Product Manager, says that many of the misconfigurations he sees in Active Directory deployments are the result of either a lack of understanding about the overall security model or the decision to implement quick fixes that cause security vulnerabilities down the line.

"Those are the scenarios that attackers love to take advantage of—especially faulty configurations with Kerberos and Group Policy," said Harel.

Some of the most common vulnerabilities uncovered by Purple Knight include:

- Passwords that have not been changed frequently, leaving the company open to brute force attacks
- Accounts with elevated privileges in place that haven't been adequately reviewed—for example, the Enterprise Key Admins group
- Exchange accounts with elevated AD permissions that have proliferated over time
- Kerberos delegation set up as "unconstrained," a scenario that is easy to abuse or to unintentionally expose to inappropriate users
- Weak group policy configuration, which creates security vulnerabilities when GPOs are linked to Active Directory at the domain level

> *"We wanted to give security teams that don't have deep AD expertise a way to understand their AD security posture—and then close any existing gaps so that adversaries won't use those against them."*
>
> Mickey Bresman, *Semperis* CEO

Purple Knight provides an overall AD security secure as well as individual scores in the categories of AD delegation, account security, AD infrastructure security, group policy security, and Kerberos security. In initial Purple Knight reports, organizations reported average scores of 61%—a barely passing grade. Kerberos security was the lowest scoring category:

Average Scores from Initial Assessments

OVERALL SCORE	61%
AD Delegation	**68%**
Account Security	**59%**
AD Infrastructure	**77%**
Group Policy Security	**58%**
Kerberos Security	**43%**

Cybercriminals see lax domain admin permissions as low-hanging fruit, said Darren Mar-Elia, Semperis VP of Products. "Attackers like to go for that because it makes their job easier. An attacker is going to find the shortest path to the domain admin account. Because once they have that, then it's game over."

Continuously guarding against AD security vulnerabilities requires good account hygiene, said Ran Harel.

"But it's notoriously difficult to do that," said Harel. "One user can belong to 20 different groups, which might have subgroups with delegated rights. It becomes like spaghetti: You have to sort through the account permissions on a regular basis. If you're not doing that, then account management starts to slip through the cracks, and the problem gets worse."

Results from Purple Knight reports highlight the irony that the largest organizations, often with the most resources, are particularly susceptible to falling behind in securing their critical identity systems because of the sheer size and complexity of their environments—leaving them at risk of a SolarWinds-like attack.

"Since Active Directory is a prime target for attackers attempting to steal credentials and deploy ransomware across the network, it's worth considering the repercussions of an Active Directory attack even if you're not directly responsible for its daily operation."

MICKEY BRESMAN
Semperis CEO

ACTIVE DIRECTORY IS THE ACHILLES' HEEL OF ENTERPRISE SECURITY

Semperis CEO Calls on Security Leaders to Defend Active Directory

It might seem like Active Directory is just another service that needs to be recovered in the wake of a cyberattack. But the reality is, AD is a keystone. If it's compromised, so is your entire environment.

Nearly half (47%) of organizations use Active Directory as their primary identity store. 51% use it to varying degrees of importance alongside other identity stores, but only 1% of organizations either don't use AD at all or are phasing it out.

Many organizations are taking a hybrid approach to identity and beginning to focus on the cloud interdependencies and complexities that result—but ignoring the fact that the entirety of their cloud identity is still syncing to on-premises Active Directory. AD is used as a source from which to sync other identity stores, so an AD compromise can cause a cascading effect as AD links with other cloud applications. This potentially problematic connection between cloud-based and on-premises assets becomes more pronounced as organizations scramble to support remote workers with mobile devices in the aftermath of the pandemic.

In "Rethinking Active Directory Security" on Help Net Security, Semperis CEO Mickey Bresman discusses the importance of organizations having a tested action plan for recovering Active Directory (AD) in the event of a cyberattack. Learn more from his article about steps companies can take to shore up defenses against AD-related cyberattacks, including ensuring that AD-specific monitoring is in place.

MORE RESOURCES

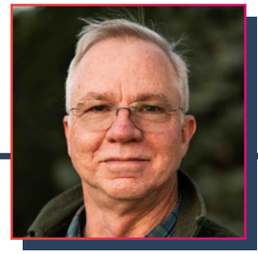
BLOGS

- Semperis Expert: SolarWinds Attack Highlights Need to Secure AD
- CISA's Ransomware Guidance Is Reminder to Include AD in Recovery Plan

WEBINAR

- What You Need to Know About Securing Active Directory

BUILDING A CYBER-RESILIENT ORGANIZATION



Active Directory Experts Have a Future in Security

BY **GIL KIRKPATRICK,** *Chief Architect at Semperis*

Between the growth of cloud applications and a changing threat landscape, the world of a Microsoft Active Directory (AD) professional has changed significantly over the last 20-plus years.

As in any other area of IT, the drive and curiosity to level up one's skills to keep pace with evolving technologies is one of the most critical attributes AD engineers and architects can have.

After two decades of focusing on on-premises systems, users, and applications, most AD professionals are now responsible for cloud integration and ensuring secure access for an environment where the traditional network perimeter no longer exists. AD pros must conduct this work while attackers continue to use increasingly sophisticated attacking tools to take advantage of AD configuration errors and Windows vulnerabilities, target user credentials, and try to maintain persistence in the on-premises systems.

In the face of this situation, technology leaders are recognizing the need to facilitate cooperation between security and identity teams to ensure secure user access in the age of cloud computing and an increasingly remote workforce.

Moving into the future, AD experts should expect to take a more active role in security discussions. This practice is not yet common, but as AD continues to be a go-to attack surface for cybercriminals, AD pros can seize this moment to contribute their expertise to the company's security efforts. As organizations make identity the focal point for their security strategy and AD admins become more involved in security conversations, administrators who can broaden their knowledge and skillsets will demonstrate deeper value to the enterprise.

Changes in threat landscape bring opportunity for Active Directory professionals

In many respects, AD was not designed with today's security challenges in mind—and it's not just vulnerabilities like the issue exploited by the Zerologon attacks last year. Modern attackers also take advantage of built-in protocols in the Windows operating system and AD itself in their attacks.

Then there is the problem of ransomware. In recent years, ransomware attacks have been observed using Advanced Persistent Threat (APT) techniques, such as those provided by tools like BloodHound and Mimikatz, to perform reconnaissance and credential theft. In one case from 2020, a piece of ransomware used the SYSVOL share on AD domain controllers to spread malware throughout the target environment.

In the past, AD recovery planning focused primarily on events such as natural disasters, power failures, or administrative errors. Now, with the prospect of ransomware disrupting their entire IT operation, businesses need to prepare for a much more likely situation—a cyberattack that forces them to recover their AD from scratch.

Putting identity first

Mobile users and cloud computing have eroded the traditional network perimeter: The only control point among users, applications, and network assets is user identity. Digital identity touches all aspects of the modern enterprise. Every user needs access to the appropriate systems and applications to do their jobs. However, controlling access securely is far more than a productivity issue. Excessive permissions, weak passwords, and numerous other potential problems lead to data breaches, malware infections, substantial financial damage—and long nights for IT and business leaders.

As the ecosystem of cloud applications used by workers grows, handling the necessary integrations to AD is a challenge not just for the identity team. Extending security and access policies from on-premises AD into the cloud is a security issue as well. For those AD experts accustomed to their on-premises environment's permission model, the mindset shift in integrating on-premises AD with Azure Active Directory (AAD) might be jarring. (For a more in-depth discussion about the implications of managing both on-premises AD and AAD in a hybrid environment, read "Top Risks to Watch for in Shifting to Hybrid Identity Management" by Doug Davis, Semperis Senior Product Manager.)

As always, however, with change comes opportunity. Understanding the new risks an organization faces and where AD fits in the security puzzle is a critical asset to digital transformation efforts. Identity professionals who can offer their expertise in conversations with the security team or C-level business executives will be in the best position to contribute to the company's security plan and expand their own career prospects.

Level up identity and security knowledge

For Active Directory and other identity services professionals who want to contribute to the company security strategy, the key is to stay current—always one of the most challenging (and rewarding) aspects of an IT career. Think about all the technologies IT pros have used in their careers that are no longer relevant. How many technologies have reached their end of life and are no longer supported? Education is the key to adjusting to the ever-changing realities of IT security and operations.

The good news is that you can find abundant resources for IT professionals on the internet. Channel 9, for example, is a great resource for instructional videos about Microsoft products. Microsoft also provides preparation guides for Microsoft certification exams. Some security certifications identity pros should consider include "Security, Compliance, and Identity Fundamentals" and "Security Fundamentals." These and other certifications, besides being good resume proof points, will give identity pros a strong foundation in the security concepts they'll need to bring to the discussions with technology leaders.

Still, nothing beats experience. Having hands-on experience in a lab environment—not only with on-premises AD but also with hybrid environments that use Azure, AWS, and Google Cloud Platform—is the only way to truly gain skill in managing it effectively and securely.

Always be a student of identity and security

As with all career paths in IT, change is the only constant. Pursuing mastery of any aspect of the industry, from security to app development, requires a commitment to keeping pace with different technologies and trends. With identity-related security risks increasing and cloud adoption growing, AD professionals need to understand—and strive to lead the discussion—in how identity management fits into their organization's security strategy.

MORE RESOURCES

BLOG

- Leading CISOs Discuss Shifting Priorities Amidst Increased Security Threats

WEBINAR

- The Changing Role of Active Directory Engineers in a Cyber-Resilient Organization

Three Steps to Harden Your Active Directory in Light of Recent Attacks

BY **BRIAN DESMOND,** *Principal at Ravenswood Technology Group*

In a recent webinar I co-hosted with Semperis (the folks behind the Purple Knight security assessment tool), we focused on a key common denominator across recent high-profile attacks—Active Directory. In the session "How Attackers Exploit Active Directory: Lessons Learned from High-Profile Breaches," Sean Deuby and Ran Harel from Semperis joined me as we discussed four recent attacks that created headlines—SolarWinds, the Hafnium Exchange 0-day attacks, the Colonial Pipeline attack, and the attack on Ireland Health Service. Although every breach was different in terms of tactics, and was executed by different bad actors, they all had devastating consequences. In our discussion, we covered three of the most important preventative measures that organizations can take to protect themselves against cyberattacks.

1 Protect email from advanced threats

One of the most common entry points for attackers is email. Advanced phishing campaigns are extremely convincing to end users, and they provide an avenue for attackers to obtain valid credentials and/or deliver malware to endpoints. It is crucially important that organizations take a multi-faceted approach to protecting themselves from these threats. Security awareness training and phishing simulations are important to educate and measure risk. No matter how much training you do, attackers will still succeed. To combat this, an advanced email threat protection solution—one that raises the bar beyond anti-spam and anti-virus tools—must be part of your defense strategy. A service that uses machine learning algorithms and other advanced detections to detect and block phishing messages and suspicious attachments must be in place in today's threat landscape.

"You'd have to be living under a rock for the past year in order to have missed the significant cyber security events that have happened on a week-to week-basis. We spend a lot of time talking about the novel ways bad guys attack, but in reality, the threat actors are not in it to find novel ways; they just want to get in—and the superhighway for threat actors is Active Directory ."

— SEAN DEUBY, *Director of Services at Semperis*

2 Prevent lateral movement

Once an attacker compromises a client computer or member server, they will look to move laterally across the network and escalate privilege. Preventing lateral movement makes the attacker's job dramatically harder. You can put in place some technically simple—but sometimes operationally challenging—controls to block lateral movement. First, the local administrator password on each endpoint must be different. Microsoft offers a free solution called the Local Administrator Password Solution (LAPS) to achieve this. Second, you cannot nest domain accounts in the local administrators group to enable easy IT support. IT personnel must use LAPS to retrieve administrative credentials for specific endpoints.

3 Secure access to privileged credentials

Preventing adversaries from obtaining privileged access—especially Domain Admin—is a critical defense. If an adversary can escalate their privileges, they can achieve higher or even complete control of the entire network. Implementing effective controls that isolate and protect privileged credentials is extremely important. Two of the most common control sets we implement at Ravenswood Technology Group are the concepts of tiered security controls and privileged access workstations (PAWs). Tiered security controls prevent high-privilege credentials from being exposed to higher-risk assets such as client computers where the credentials might be stolen. PAWs isolate the tasks an administrator performs from their day-to-day workstation to a highly secured workstation, protecting the credential and the administrator's session from threat vectors such as email, Internet access, and some types of malware.

MORE RESOURCES

VIDEO

- Active Directory security pro tip: Staying ahead of ransomware attacks that exploit AD

BLOG

- How to Defend Against Ransomware-as-a-Service Groups That Attack Active Directory

DOWNLOAD PURPLE KNIGHT

- Identify and address AD security gaps and gain confidence in the security of your AD environment

Is your AD ready for today's threat landscape?

The attacks we discussed in the on-demand webinar are just four of the countless breaches that are making daily headlines. Hardening your organization's IT environment is critical and for any enterprise, and Active Directory must be a core component of your hardening strategy. Between Ravenswood and Semperis, there are probably no two organizations (outside of Microsoft itself) with more combined AD security expertise. We have an extremely powerful partnership that helps organizations worldwide raise the bar on hybrid identity security.

To get more advice on how to protect your organization, check out the on-demand web seminar. And, of course, you can download Purple Knight for free to identify and address AD security gaps and gain confidence in the security of your AD environment—no matter how complex, convoluted, or neglected it is.

The Practical ROI of a Quick Active Directory Recovery

BY **SEAN DEUBY,** *Director of Services at Semperis*

While every IT manager or administrator knows that a solid Active Directory recovery plan is an essential component of any business continuity strategy, calculating the practical return on investment (ROI) of an optimized AD recovery plan is notoriously tricky. Too many variables are at play to generate a defensible, exact calculation. And to set expectations up front: I won't offer any sort of interactive ROI calculator here.

Instead, I want to take a look at a few practical ways to see a return on your investment in ensuring a proper AD recovery—allowing you to do your own calculations and come to your own conclusions. Losing one domain controller is a problem in itself, but let's look at another increasingly common scenario that has catastrophic consequences: a ransomware attack that takes out every domain controller across all company sites. In that situation, recovering AD can be a white-knuckle, under-the-gun challenge.

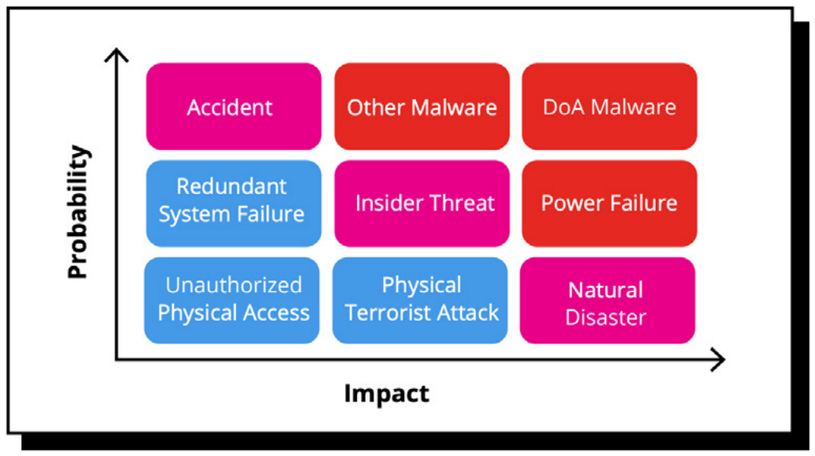
In the last year, we've discussed scores of ransomware attacks where cybercriminals modified AD in one way or another—far beyond the basic changes to user accounts or passwords—to gain entry into information systems and move laterally to propagate malware. Ransomware architects now have engineers on staff who are dissecting AD and its security updates looking for opportunities to elevate permissions and quickly distribute malware across the entire organization. Post-attack forensics from previous ransomware attacks involving AD have revealed that threat actors primarily focus on changes to group accounts, user accounts, Group Policy objects, the SYSVOL, and domain controllers.

With these cybercriminal tactics in mind, consider the following factors in calculating your own AD recovery ROI:

Cost of operational losses

It's likely that a material part of your operations relies on AD being up and running to authenticate users as the basis for providing access to applications, systems, and data. For every hour that AD cannot operate, how much revenue or productivity would your business lose? How many hours, days, or weeks would it take before the business passes a point of no return and cannot financially recover? Remember the ransomware attack on the City of Baltimore? Their recovery of operations took months and cost over $18 million.

Cyber-First Disaster Recovery Risk Matrix



Lack of a business continuity plan that includes AD

If your organization is mature enough, you have a BC/DR plan in place defining the work needed to restore business operations after an outage. Most plans account for loss of infrastructure or loss of a location after a natural disaster. But few companies have a plan specifically for restoring business after a cyberattack—and especially one as unpredictable as a ransomware attack. The way you recover AD in a scenario like this depends on what changes cybercriminals made within AD. You might plan to recover AD back to a previous version, but how do you determine how far back you need to go to find a known secure version? What AD-dependent systems, services, and applications will be affected or won't function at all because of a broad-stroke recovery to an earlier AD state? Are you confident that you can even locate a recent, malware-free backup from which to restore? Without a plan or an ability to understand what was changed in AD before recovering, your organization will spend incalculable time fixing all the problems the recovery caused.

Recovery might not be the answer

If all the changes being made by the bad guys during an attack boil down to, let's say, adding an account to the Domain Admins group, then recovering AD to a few days ago or last month might not be the right answer. Instead, perhaps the less costly method is to monitor changes in AD and have an ability to either disallow changes to "protected" accounts (like the Domain Admins group) or to automatically revert a change to a sanctioned configuration.

The considerations above summarize to three risks: the risk of a slow recovery, the risk of a recovery that creates more remediation work, and the risk of a recovery that might be considered overkill for the nature of the changes made to AD.

A different approach to calculating the ROI of AD Recovery

Instead of looking at the ROI of AD recovery using some calculator you found online, the better choice is to work through several real-world scenarios and evaluate how your current means of AD recovery would fare by answering the following questions based on the factors outlined above:

- What critical parts of the operation depend on AD to function? What is the estimated cost of their downtime?
- How long will it take to recover AD based on the changes made during an attack?
- Do you have visibility into what malicious changes were made in AD and, if not, how far back will you need to investigate and how long will that take you?
- Will the recovery impact any other parts of operations that you will need to fix and, if so, how long will that take? (Remember that some number of both user and computer account passwords will not match, impeding the ability to log on to the domain. Plus, earlier versions might be missing accounts, group memberships, DNS records, etc.)
- Are you confident that recovery will put you into a known-secure state? Beware of the difference between resuming business operations and recovering business operations: If you don't have a clean, malware-free backup from which to recover, you run the risk of reintroducing the same vulnerabilities that left you open to attack in the first place.

In short, the ROI of AD recovery has much more to do with your current ability to recover to a known-productive and known-secure state post-attack than it does with an online ROI calculator that doesn't account for the myriad variables involved in a ransomware attack. By walking through some scenarios and thinking specifically about what your current recovery abilities are, you will expose costs that can be eliminated by having a proper AD recovery solution in place—one that is designed to protect against, prevent, and recover from malicious changes to AD.

QUICK STORIES FROM THE FIELD

Semperis provides top-rated cyber-first disaster recovery for Active Directory. Some of the results our customers have reported after deploying Semperis Active Directory Forest Recovery:

- Israeli airline El Al deployed Semperis ADFR and reduced complete AD forest recovery time from 24 hours to two hours.
- A global retailer with 2.2 million users and 500 DCs switched to Semperis ADFR from their existing solution and reduced the time to recover an AD forest from 6 days to 6 hours.
- A healthcare company with a 65GB DIT reduced time to recover the AD forest from 1.5 days with their existing solution to under 4 hours with Semperis ADFR.

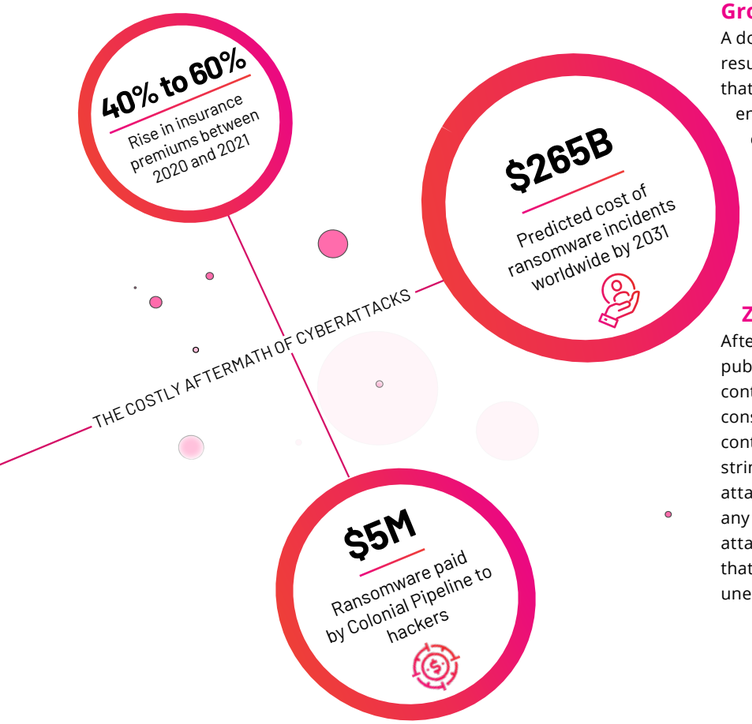
How to Defend Against Active Directory Attacks That Leave No Trace

BY **GUIDO GRILLENMEIER,** *Chief Technologist at Semperis*

Cybercriminals are using new tactics and techniques to gain access to Active Directory in novel ways, making their attacks even more dangerous—and more necessary to detect.

One of the most important parts of any cybersecurity strategy is detection. Having an ability to spot the bad guy entering, moving about, or worse—administering—your network is key to a swift response. And with the median number of days an attacker sits undetected on your network at 146, according to Microsoft, it's evident that the bad guys are very good at working in stealth.

When it comes to detecting potentially malicious actions within Active Directory (AD), most organizations rely on Domain Controller event log consolidation and SIEM solutions to spot abnormal logons and changes. This all works—as long as the attack technique leaves a log trail.



A few types of attacks have been seen in the wild that leave no discernable trail or, at least, any evidence of malicious activity. Some examples include:

DCShadow attack

Using the DCShadow functionality within the hacker tool Mimikatz, this attack first takes the path of registering a rogue domain controller (DC) by modifying the Configuration partition of AD. Then the threat actor makes malicious fake changes (e.g., changes to group memberships of Domain Admins, or even less obvious changes such as adding the SID of the Domain Admins group to the sidHistory attribute of a compromised normal user). This attack technique bypasses traditional SIEM-based logging, as the rogue DC doesn't report the changes. Instead, changes are injected directly into the replication stream of the production domain controllers.

Group Policy changes

A documented attack involving Ryuk ransomware resulted in changes being made to a Group Policy object that propagated the installation of Ryuk to remote endpoints within the victim organization. By default, event logs don't include details on what was changed within a Group Policy. So, if an attacker makes a malicious change (as in the case of Ryuk), all that's seen is that an account with access to the Group Policy made a change, which probably won't set off any alarms.

Zerologon attack

After a proof–of–concept exploit code was released in public, an attacker with network access to a domain controller was able to send special Netlogon messages consisting of strings of zeros, forcing the domain controller computer password to be changed to an empty string. So, without any logon—i.e., with zero logon—the attacker now owns the domain controller, can perform any changes in AD, and can further use this path to attack other systems in your infrastructure. It is unlikely that your monitoring tools today are watching out for unexpected password changes on your DCs.

It isn't by chance that these attacks don't leave a trace; it's by design. The bad guys are spending massive amounts of time inspecting exactly how their target environments function and looking for ways to bypass, obfuscate, and circumvent any form of detection—which includes logging.

Because these kinds of attacks exist, the question becomes what should you do about it—both proactively and reactively?

Protecting against malicious Active Directory changes

There are three ways to protect your organization against malicious AD changes:

- **Monitor AD for malicious changes:** This goes beyond SIEM and involves a third-party solution designed to see every change made within AD—regardless of who makes it, on which DC, using what solution, etc.—ideally by reading and understanding the replication traffic of the DCs themselves. This monitoring needs to include changes within Group Policy as well. In many cases, solutions designed to monitor changes in AD can define specific protected objects to be monitored for any change—for example, changes in membership to Domain Admins—so that any time those protected objects are modified, alarms do go off. The solution should cover both changes to Group Policies as well as visibility into replication.

- **Look for DCShadow:** Mimikatz leaves some artifacts behind and there are some telltale signs that DCShadow has been used on your network. Reviewing AD for these signs needs to be part of a regular review of AD security. Note that once you find a trace of Mimikatz DCShadow in your environment, you must act quickly as you'll already be a victim of an attack. At that point, you will wish you also had a solution that would show you what changes were performed at the replication level, which you could then analyze and ideally revert.

- **Be able to recover AD:** Your organization needs the proactive ability to recover any and all of AD should you determine that AD has been compromised. In some cases, you can be thinking in terms of backups and a DR strategy to recover AD in a cyberattack scenario. Should you indeed need to recover your complete AD service, potentially as the next victim of a malware attack, beware that a good domain controller backup does not equate to a seamless and fast AD service recovery. You'll want to have practiced the whole recovery process periodically, following the copious Microsoft AD Forest Recovery Guide. But it's equally valuable to look for solutions that can revert changes down to the attribute level or even automatically revert changes to protect objects when detected.

Targeting Active Directory and modifying it to suit the attacker is a common tactic taken by today's cybercriminal—so much so that the old model of watching AD audit events for changes might no longer be viable. Organizations that are serious about the security and integrity of their AD need to be looking for additional ways to gain visibility into every AD change and have the ability to revert or recover when necessary.

WEBINAR

HOW ATTACKERS EXPLOIT ACTIVE DIRECTORY: LESSONS LEARNED FROM HIGH-PROFILE BREACHES

MORE RESOURCES

WEBINAR

- Would Your Organization Fail the Active Directory Security Assessment?

BLOGS

- Timeline of a Hafnium Attack
- Active Directory Security: Abusing Display Specifiers

Do You Know Your Active Directory Security Vulnerabilities?

BY **SEAN DEUBY,** *Director of Services at Semperis*

Securing Microsoft Active Directory (AD) involves dealing with a mixed bag of risks, ranging from management mistakes to unpatched vulnerabilities. We often write about the fact that cyber-attackers are targeting AD to elevate privileges and gain persistence in the organization. Investigate a typical data breach, and you'll find that stolen credentials likely were used—sometimes for initial entry, sometimes for accessing critical systems, but always to the detriment of the targeted organization.

Hardening AD begins with getting a handle on the vulnerabilities and common configuration and management mishaps that pave the road to compromises. To defend AD, administrators need to know how attackers are targeting their environment. How many, however, can pass a pop quiz about the types of security holes threat actors are sneaking through as they move through the steps of the breach?

Authentication fail

It seems ironic, but some of the most prevalent and damaging configuration errors impacting Active Directory are related to the authentication process. Consider a scenario where an organization wants to allow a third-party or home-grown application that doesn't integrate with AD, but wants to query AD for active users. The easiest route is to simply enable anonymous access to Active Directory. While this action might make sense from a productivity standpoint for busy administrators, it also allows unauthenticated users to query AD. If that capability is enabled without mitigating controls, the risk profile of that organization is going to increase substantially.

The Zerologon vulnerability reported in 2020 was quickly exploited by attackers because it allowed them to change or remove the password for a service account on a domain controller. The results of a successful exploit could be catastrophic. Weak passwords, non-expiring passwords, no passwords—all these are warning signs that an organization's AD environment is not secure.

Secure password policies should be the order of the day throughout the Active Directory infrastructure. Any account with the PASSWD_NOTREQD flag set should automatically draw additional scrutiny and have a justifiable reason for its configuration. Additionally, passwords—especially service account passwords—should be periodically rotated. Leaving passwords unchanged for lengthy amounts of time increases the likelihood of a successful brute force attack, as attackers will have more time to take swipes at them.

Authentication issues to watch for include

- Computers and Group Managed Service Accounts (gMSA) objects with passwords set over 90 days ago
- Reversible passwords found in Group Policy Objects (GPOs)
- Anonymous access to Active Directory enabled
- Zerologon vulnerability (CVE-2020-1472) if the patch is not applied.

Permitting excessive permissions

As most AD environments have been in production for many years, their attack surfaces have grown. Many of a forest's accumulated vulnerabilities can be traced back to the pattern that someone needs something done, usually in a hurry, and the least–privilege path to get that done is too time consuming, not easily available, or simply not known. As a result, the user or group or permission is over-privileged just to ensure the request will be satisfied and the ticket closed. And of course, that entitlement is never ever removed, so the attack surface simply grows and grows.

In reality, it's not uncommon for AD environments to have unnecessarily high numbers of domain administrators—a fact that can be even more troubling if those accounts are orphaned and are simply waiting to be leveraged in an attack. Service accounts with excess permissions also pose a high risk because their passwords are usually set to not expire, and many of them will have weak passwords (which makes them a good kerberoasting target). As the number of users with administrative privileges grows, so does the attack surface that needs to be protected. Membership to these groups should be tightly controlled.

Mistakes happen, of course. As an AD environment grows larger and more complex, for example, someone might fail to properly account for inherited permissions and inadvertently grant an account too many privileges. But even properly managing privilege delegation is not enough with attackers taking the offensive.

As an example, consider the impact of an AdminSDHolder attack. Just as a refresher, the AdminSDHolder container stores the Security Descriptor applied to privileged groups. By default, every 60 minutes, the Security Description Propagation (SDPROP) process compares the permissions on protected objects and reverses any discrepancies according to what is defined in AdminSDHolder.

In an AdminSDHolder attack, threat actors exploit SDPROP to maintain persistence by replacing the permissions of an object with the attacker's unauthorized modifications. If the permission changes are identified and undone, but the unauthorized changes to AdminSDHolder are undetected, the attacker's changes will be reinstated.

Auditing permissions and monitoring for suspicious activity is the best defense against the abuse of privileges.

Permission issues to watch for include:

- Privileged objects with unprivileged owners
- Permission changes on the AdminSDHolder object
- Unprivileged users with DC Sync rights on the domain
- Default security descriptor schema changes in the last 90 days

> *To defend AD, administrators **need to know** how attackers are targeting their environment.*

READ MORE

BLOGS

- Good Riddance, Red Forest: Understanding Microsoft's New Privileged Access Management Strategy
- DnsAdmins Revisited

SECURING AZURE ACTIVE DIRECTORY

Top Security Risks to Watch for in Shifting to Hybrid Identity Management

BY **DOUG DAVIS,** *Senior Product Manager at Semperis*

It's easy to see why enterprises are gravitating toward a hybrid identity management model that promises the best of both worlds—a little bit in the cloud, and a little bit on-premises. In an Active Directory-centric environment, leveraging the cloud means integrating with Azure Active Directory.

Azure Active Directory (AAD), after all, is designed with an eye toward SaaS applications, providing single sign-on and access control. As cloud adoption increases, the ability to manage both on-premises and cloud access is becoming a business necessity. Leveraging AAD alongside Active Directory (AD) helps make hybrid identity management a reality.

As with anything in IT, however, the adage of look-before-you-leap still applies.

Monumental change with moving to the cloud

Moving any part of an IT operation to the cloud requires an adjustment. User authentication is no different. From a conceptual standpoint, organizations need to consider three critical issues.

1. A new authentication model

After 20 years of managing identity one way, adding AAD to the mix will be a critical adjustment. Going from using only on-premises AD to extending to cloud authentication requires a different mindset and approach. In AAD, there are no organizational units or forests, and no group policy objects. Concepts (and battle scars) about how to secure the identities in AD no longer apply in AAD.

Many administrators start out believing that securing AAD is similar to securing AD, which is not the case. And you might already be using AAD without thinking much about it. If your organization is leveraging any Microsoft cloud services, such as Office 365, then AAD is already being used in the background. AAD is also leveraged heavily to connect to other non-Microsoft SaaS applications, such as Salesforce. All these factors introduce new considerations and choices. For example, should you keep AD and AAD separate or merge them using Azure AD Connect? Many new concepts need to be understood so you can make these decisions while keeping information systems secure.

2. The extension of the perimeter

Once an organization embraces the cloud, the notion of the traditional network perimeter ceases to exist. For IT administrators who have spent the last two decades running AD on-premises, this notion is a tremendous adjustment. In a hybrid identity environment, organizations now must be prepared to guard against an endless array of possible entry points.

3. Radical changes to the permission model

Moving to AAD also drastically changes the permissions model organizations need to secure. On-premises, it is fairly easy to control who has physical access to domain controllers, and overall management entry points are well-defined and documented. In a hybrid AD environment, identities are also now stored in the cloud, vulnerable to exploitation by anyone who has access to the internet. Suddenly, administrators are dealing with an inherently open model for initial access connections, which—when coupled with the larger number of services, roles, and permissions required—has a significant impact on risk.

Microsoft has actively tried to provide educational materials to prepare businesses for the changes caused by AAD adoption. However, many IT organizations are still failing to fully appreciate the implications of hybrid identity management. As more companies take a hybrid approach, attackers have expanded their modus operandi accordingly.

SECURING AZURE ACTIVE DIRECTORY

In September 2020, researchers at Mandiant (FireEye) noted they had seen an increase of incidents involving Microsoft 365 and Azure Active Directory, mostly tied to phishing emails attempting to entice victims into entering their Office 365 credentials into a phishing site. Mandiant researchers also observed attackers using a PowerShell module called AADInternals, which enables attackers to move from the on-premises environment to AAD, create backdoors, steal passwords, and take other malicious actions. These threats will continue to grow with the exponential growth of interest in Azure and Office 365.

Permissions, permissions, permissions

By far, of the three subjects mentioned above, the biggest security risk is caused by the changes to the permissions model. There are a huge number of services that are available when organizations move to a hybrid identity environment. Instead of a well-defined set of administrative groups in Active Directory, you now have roles in Azure AD, which will be unfamiliar. You can see this list of roles here. Each role has a lengthy list of assigned permissions. It is hard to understand the permissions assigned to each role just from the description, but many have a high level of access that isn't apparent.

Also, linking any SaaS service to AAD, which is probably why you added AAD to the mix, adds permission models that need to be managed. Microsoft Teams, for example, uses SharePoint integration at the back end. With the wrong configurations, adding a guest to Teams might create a situation where this new user now has access to files stored on SharePoint for Teams. Folks might not be aware that these files are now available to guest users who were added to their channel only for a quick chat. In addition, the ability to add Apps in Teams effectively extends the permission model to these third-party tools. This is just one example of the matrix of complex issues for each service managed via AAD.

In fact, keeping track of the permissions of third-party apps is critical and is an area that is undermanaged in most AAD implementations. These permission requests will trigger a one-time-only pop-up that lists the permissions the app needs. These lists can be lengthy and should be reviewed carefully before acceptance, but rarely are.

Organizations also might face these two new scenarios related to permissions that need to be understood in a security context:

- **Third-party tools that pull data from Azure AD and store it in their own database.** For example, an application registered in Azure AD that allows for a CRM system to read user profiles or has other read permissions effectively has the ability to retrieve and store data for itself. Once the data is taken from Azure AD, it sits in an external database, leaving the organization to rely on the security framework of the third-party tool.

- **Third-party tools with write access that can make changes within their tool.** In this case, the required authentication to make changes in the tenant is moved from Azure AD to whatever controls the third-party tool has. A user might be able to log into the tool without multifactor authentication because it does not support single sign-on (SSO), operating instead with the application acting as the permission proxy that does the action on their behalf without some of the checks that would normally be required.

IT organizations should strongly consider restricting who can approve applications or, at the very least, have clear guidance on what permissions should be considered appropriate. Taking a hybrid identity approach requires dealing with a much broader permission model. To do so effectively, organizations must establish strong governance of what apps are going to be turned on and what access rights they will get.

Understand the risk of hybrid identity management

Whether authentication is handled in the cloud, on-premises, or both, putting security first is always a must. While managing identity in a hybrid environment might seem as simple as joining a Windows device to AAD, failing to account for changes to the risk landscape opens the door to issues that can cause headaches in the future. Knowledge is always your first line of defense, but the amount of documentation needed to fully understand security in AAD is daunting. Native or third-party tools that automate that understanding and reduce the complexity of security will help lower security risk during and after the rollout of your hybrid environment.

IDENTITY ATTACK WATCH IN REVIEW

JUNE 2021

- Colonial Pipeline attack traced to inactive account
- FujiFilm network breached in ransomware attack
- JBS meat producer paid $11 million to REvil ransomware group after attack
- REvil targets U.S. nuclear weapons contractor Sol Oriens
- UK National Cyber Security Centre calls for increased cyberattack defenses in education sector
- U.S. House engagement vendor iConstitutent compromised in ransomware attack

No backup = no choice

Although fewer companies are paying ransom to unlock their data, some victims without cyber-safe backups often see no other choice.

MAY 2021

- Microsoft reports that Russian cybercriminals behind SolarWinds attack are escalating efforts
- FBI: APT cybercriminals exploited Fortinet bugs to attack U.S. local government
- Colonial Pipeline attackers targeted Windows vulnerabilities, including AD
- Conti attack on Ireland's Health Services leveraged access to Windows domain credentials
- CISA calls for review of permissions to combat FiveHands ransomware variant
- Northern California county ransomware attack remediation required AD recovery
- Analyst presents findings that faulty permissions led to breach of veterans' med records
- Report: Risky Exchange operations top Azure Active Directory threat detection list
- Bose post-attack preventative measures included password resets and enhanced monitoring for account changes

More persistent threats

After penetrating an organization, persistent threats like the SolarWinds breach can repeatedly wreak havoc.

Governments are cracking down

Government entities like the U.S. Cybersecurity and Infrastructure Security Agency (CISA) are stepping up prescriptive guidance in the wake of relentless cyberattacks especially on organizations that deliver services important to public safety and national security.

Victims go back to basics

Companies like Bose that suffered an identity-related breach are now implementing tighter processes for ensuring fundamental identity security.

APRIL 2021

- Ransomware attack shuts down UK-based education charity Harris Federation
- Conti group attacks Broward County schools in Florida
- New ransomware Cring compromises authentication credentials
- 'Supply chain' attack on password manager exposes users' passwords

MARCH 2021

- Microsoft Exchange breach involved stolen copies of AD databases
- SolarWinds attackers targeted Mimecast's AD systems to access source code
- Attackers used admin credentials to breach Verdaka video network
- Attack group advises victim FatFace to review AD policies

Expanding threat landscape

Accelerating supply-chain attacks, made infamous by the SolarWinds breach, require that security leaders re-examine security practices of all third-party vendors.

Attackers exploit lax security

Many cyberattacks succeed because of lax Active Directory security practices, as this guidance from an attack group to its victim illustrates (with supreme irony).

Identity attacks are common thread

The SolarWinds hearings highlighted the significant role identity security plays in many high-profile breaches.

Proven attack paths still rule

Attackers love to exploit tried-and-true vulnerabilities, such as "ghost accounts" with elevated permissions, often associated with former employees or short-term projects.

FEBRUARY 2021

- SolarWinds hearings highlighted gaps in identity security
- Brazilian electric utility company attack compromised AD
- Active Directory targeted in malware attack on New York schools

JANUARY 2021

- Hackers exploit the "Active Directory of SAP"
- Ghost attacks target Active Directory
- Dairy Farm suffers REvil ransomware attack

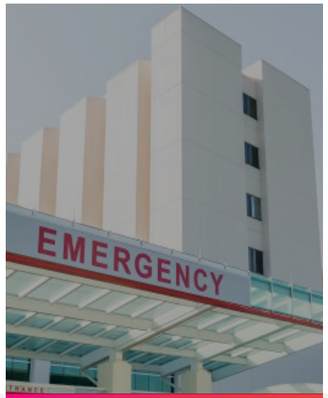
VERTICAL-MARKET CYBERATTACKS IN FOCUS

CRITICAL INFRASTRUCTURE

56%
of global gas, wind, water, and solar utilities reported at least one cyberattack in the last year

54%
of global utilities expect an attack on critical infrastructure in the next 12 months

25%
of global utilities have experienced mega attacks, with expertise developed by nation-state actors

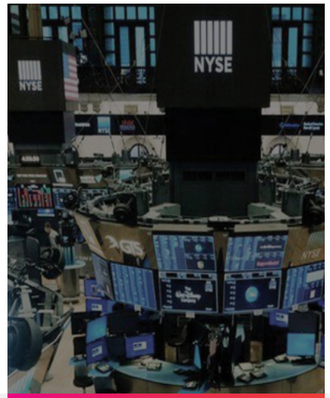


HEALTHCARE

55%
Increase in healthcare breaches in 2020

26
Million patient records compromised in 2020

61%
Of cyberattacks against healthcare organizations in 2020 were caused by outside threat actors



FINANCIAL SERVICES

62%
Of data exposed in breaches comes from the financial services industry

300x
That's the likelihood of financial services companies experiencing a cyberattack compared with other sectors

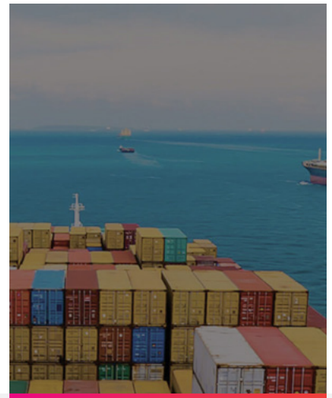
238%
The spike in cyberattacks against banks between February and April 2020

RETAIL

$85B
Estimated economic cost (on the low side) of ransomware attacks on retailers in 2020

3,126
The number of online shops that were actively under attack at one time by a 2019 Magecart skimming operation

72%
Cybersecurity workload increase since 2020 for IT teams in retail



TRANSPORTATION

$200M – $300M
Estimated revenue loss by Maersk, the world's largest shipping company, following the NotPetya cyberattack

200,000
Russian Railways computers in 150 countries were infected within one day by the WannaCry ransomware

146M
Records—including email addresses and personal contact information—were exposed online in the 2020 Network Rail/C3UK breach increase since 2020 for IT teams in retail

INSURANCE

$115M
Amount Anthem Healthcare paid to 2015 cyberattack victims for breach of data privacy

132,000
GEICO customer driver's licenses compromised by malicious actors in early 2021

$40M
Ransom paid by CNA Financial in March 2021 to regain control of its network

NEW PERSPECTIVES ON PROTECTING HYBRID IDENTITY SYSTEMS

From identity security experts presenting at #HIPEurope2021

"When an attacker has gained AD access, everything is time-sensitive. We have to ensure that the attacker can't spread to all the Active Directory forests. We need to analyze the breach, see the potential impact, and implement a safety net. We need to recover AD in hours instead of days."

Ben Cauwel
Security Delivery Manager for Accenture

"One of the big problems with cloud security today is some people don't understand the shared responsibility model yet."

Jan de Clercq
Senior Security Architect at HPE

Join us for HIP Global 2021

OCTOBER 20 - 21

REGISTER →

Pamela Dingle
Director of Identity Standards at Microsoft

"To everyone out there who has not implemented MFA, you all need to get your priorities in order. Attackers are finding ways to get into your on-premises infrastructure and then leveraging the fact that some of you have this crazy idea that just because users are on-premises that they are trusted. Getting breached is complicated, expensive, and damaging. I'm not saying that implementing MFA is not difficult, but the alternative is massively problematic."

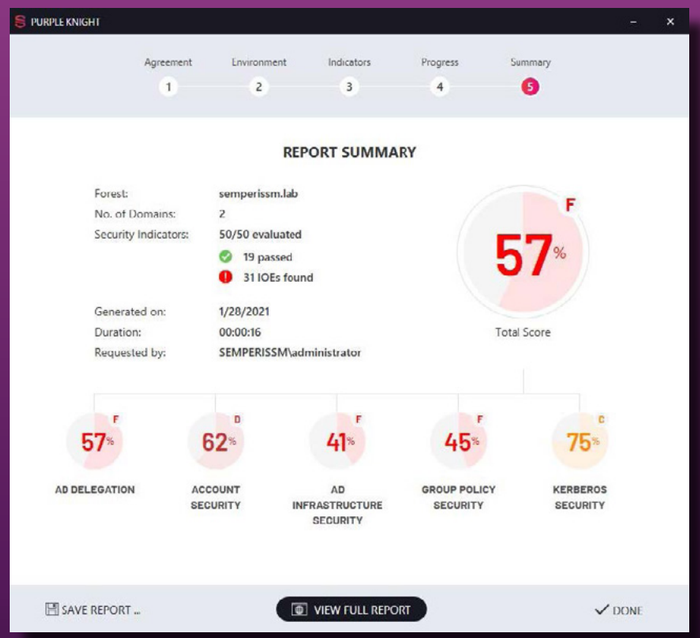
PURPLE KNIGHT

Unleash Purple Knight: Fix Active Directory Vulnerabilities

→ AD Security Report Card

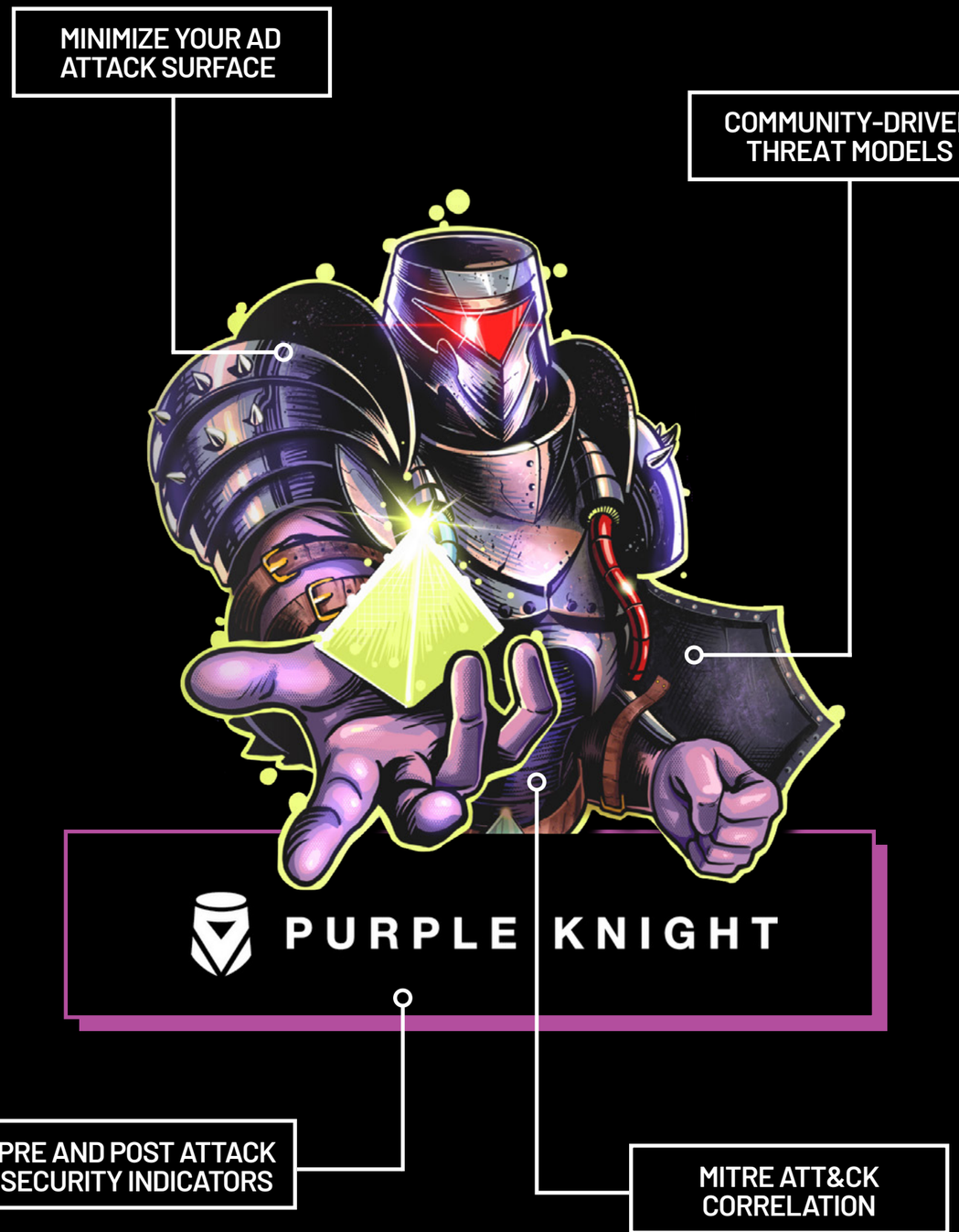
→ Pre- and Post Attack Security Indicators

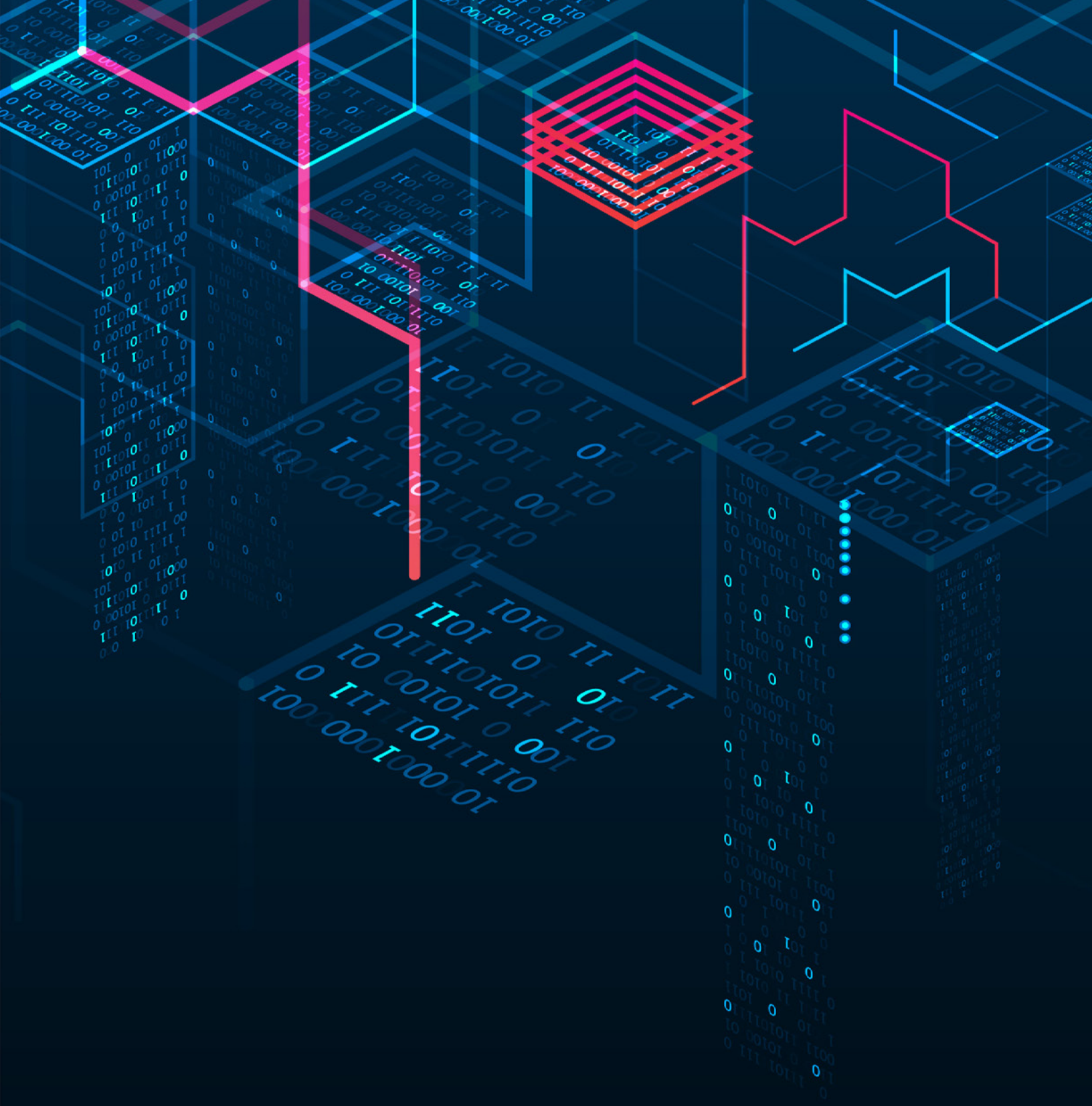
→ Prioritized, Actionable Guidance



Free Purple Knight Download →

Powered by semperis





Thank you for your interest in this resource for improving hybrid identity security. Please send any questions or comments to feedback@semperis.com.

semperis

semperis.com