The state of hybrid Active Directory cyber resilience

A report based on a recent survey of 430 Quest customers and Active Directory (AD) users to discover where organizations struggle with AD security today

Quest

How do organizations today handle Active Directory security, and where do they struggle the most?

To answer this question, the State of Hybrid Active Directory Cyber Resilience survey was conducted in September 2023 via The Experts Conference (TEC), with more than 430 responses from IT professionals and IT executives.

The main take-away is eye-opening:

IT pros overwhelmingly know where they should be focusing and how they can better secure their organizations — they just don't always have the resources and support to do it.

Our top three findings:

1. IT teams say their top struggle is identifying and limiting security risks, including improper configurations.
2. IT teams know that a security model that prioritizes Tier Zero assets (the control plane) is effective for protecting their organization's most critical IT assets, but this model is largely unutilized.
3. IT organizations aren't sufficiently staffed to support all their AD security needs, and shrinking budgets are not the only reason.

Key Finding #1: The top struggle for IT pros is assessing risk exposure.

By far, the area where IT pros struggle the most is identifying misconfigurations and other exposures. Pinpointing these weaknesses is critical to Active Directory security because they open the door to both external attacks and insider threats.

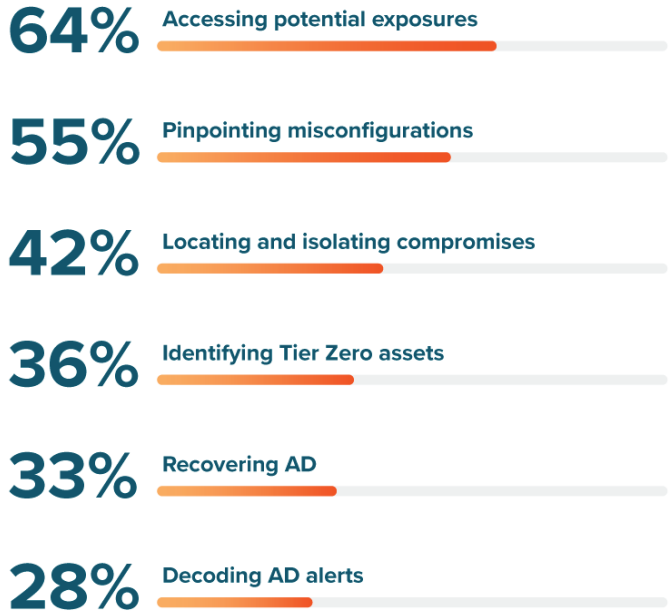
In your role, what AD security-related concerns keep you up at night?

> Security posture and cyber security weakness of the platform, Threat Detection and attack path patterns, potential Cyber Security incident, the ability to track applications and infrastructure that consume the platform, Hybrid Integration with Entra ID (Azure AD) platform, AD platform recovery and post recovery processes.

Sr. Infrastructure Engineer – Identity Services – ETS – Technology and Innovation, Large Enterprise Professional Services Company

uevi.co/7780VLXB

The top AD security-related struggles in organizations today are:



uevi.co/6201DFAN

Key Finding #1: Other top challenges for IT pros are threat detection and AD recovery.

IT practitioners also say it's difficult to detect security compromises and make sense of alerts. These tasks are vital to shutting down threats promptly to limit their impact.

In addition, IT pros struggle to restore Active Directory after a disaster, a task that is vital to cyber resilience. Indeed, without the right tools, recovering AD can take days or weeks — during which time the business is dead in the water.

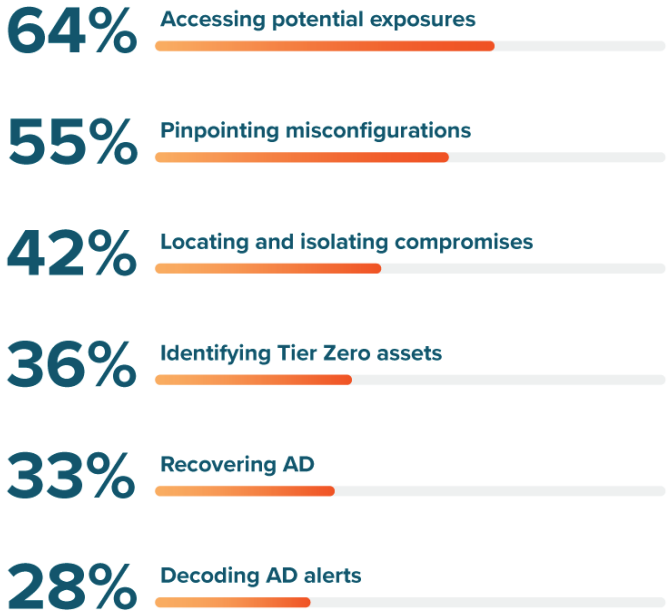
In your role, what AD security-related concerns keep you up at night?

> "Identifying externally sourced unauthorized intrusion quickly, and recoverability after detection."

Large Enterprise Professional Services Company

uevi.co/4949XYWI

The top AD security-related struggles in organizations today are:



uevi.co/6201DFAN

Key Finding #1: IT executives cite the same issues but are more concerned about risk.

IT pros and IT executives have different areas of focus, so they aren't always aligned about priorities. But when it comes to AD security struggles, they are in lockstep — both groups rank the key issues in exactly the same order.

The striking difference is the intensity of the response. Nearly 8 in 10 IT execs say that assessing exposures is a key struggle, compared to 64% of IT pros.

That's not surprising, however: IT execs are keenly aware that failure to address AD risks can lead to serious and lasting damage to the company brand. No one wants to be the next name in the news as a victim of a devastating cyberattack.

uevi.co/1457CVQW

Key Finding #1: Why do IT teams worry so much about AD security risks?

Why are entire IT teams, from hands-on practitioners to executives, so concerned about AD security exposure?

The answer is simple: Active Directory has been around for more than 20 years, and over time, AD deployments have exploded in both size and complexity. As a result, it's not easy to locate indicators of exposure (IoEs) in AD, prioritize them, and understand how to fix them to limit your attack surface.

Meanwhile, adversaries have had decades to uncover the platform's weaknesses and hone their exploits.

It's really no wonder that the State of Cyber Resilience survey found that assessing exposure was the top concern cited by both IT practitioners and IT executives, regardless of organization size or sector.

In your role, what AD security-related concerns keep you up at night?

> **AD is 20+ years old, its well understood by attackers and very difficult to properly secure.**
>
> *VP Identity & Collaboration, Large Enterprise Media Company*

uevi.co/6668BKWD

Key Finding #1: What AD concerns worry your peers?

In your role, what AD security-related concerns keep you up at night?

> Incorrectly administered changes, improper access. Essentially human error problems.

Senior Technology Officer,
Medium Enterprise Diversified Financial Services Company

uevi.co/6712HKTU

> Internal threats, disgruntled employees or end users that let Malware lose.

Sr. Mgr Cyber Defense
Large Enterprise Aerospace & Defense Company

uevi.co/6008BWMF

> Privileged accounts — both number and escalation of — and too much access through trusts.

Principal Engineer, Large Enterprise Professional Services Company

uevi.co/5976HYGO

Key Finding #2: IT pros know full well that prioritizing Tier Zero is vital...

For a decade, Microsoft has been pushing organizations to adopt an AD security model centered around Tier Zero. Tier Zero comprises all of the organization's most critical IT assets, including privileged accounts like Domain Admins and crucial servers like domain controllers (DCs).

This message has been received loud and clear: 84% of survey respondents say they understand the importance of Tier Zero for ensuring cybersecurity and cyber resilience.

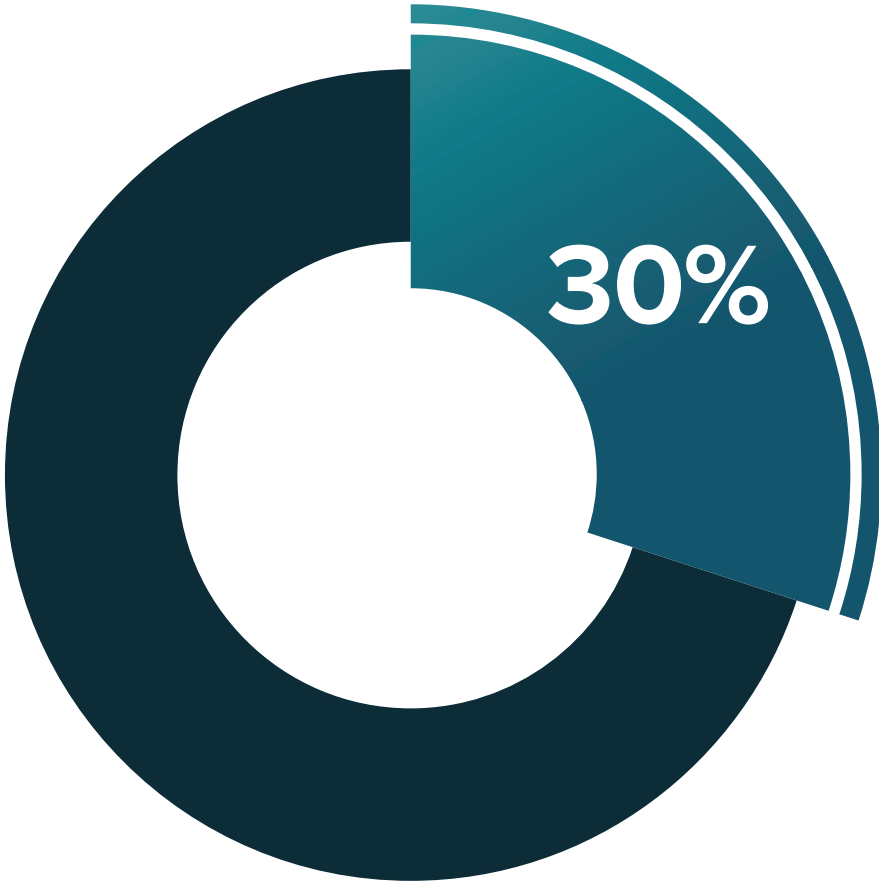
84% understand the importance of an AD Tier Zero structure, or Control Plane, in prioritizing and securing the most critical IT assets.

uevi.co/3915HSMV

Key Finding #2: ...but just 30% are using a Tier Zero security model.

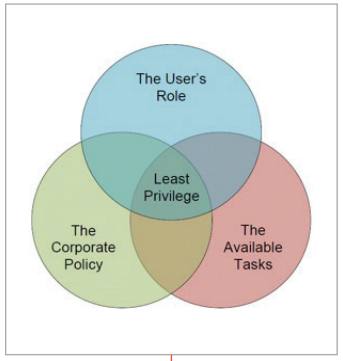
Shockingly, only **3 in 10** survey respondents say they're actively using a Tier Zero structure to keep their AD environments secure.

uevi.co/9945VLXB

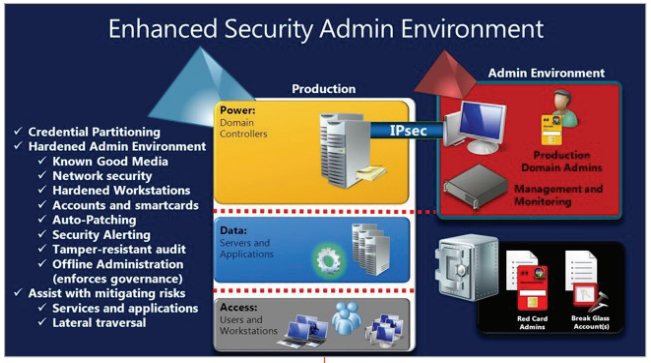


Key Finding #2: The evolution of secure directory management

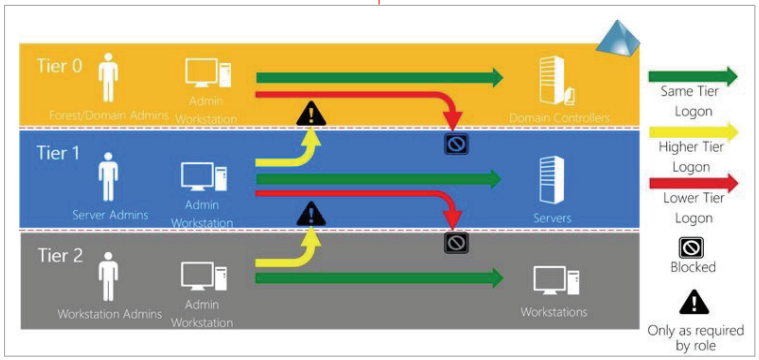
1999: Least Privilege



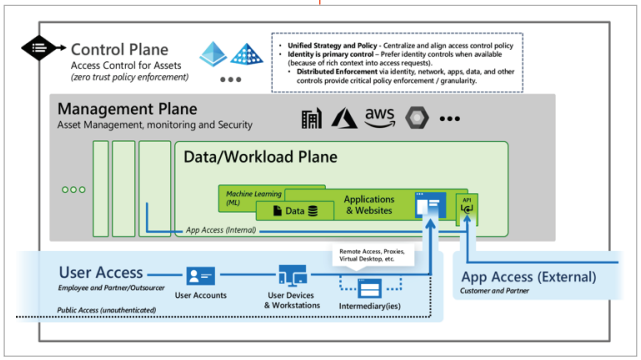
2014: ESAE/Red Forest



TODAY



2012: Least Privilege



2020: Enterprise Access Model

Key Finding #2: How has directory security changed over the years?

The first AD security model was rooted in the principle of least privilege, which mandates granting each account exactly the access rights that it requires, no more, no less. This principle remains a cornerstone of IT security, of course, but the fact is, not all IT assets require the same level of protection. Trying to lock down everything equally failed to scale as AD environments grew in size and complexity.

Tier Zero appeared in 2012 as part of a new model in which IT assets were sorted into tiers based on their protection requirements. Microsoft soon refined this approach into the ESEA (Red Forest) model, which offered more clarity about exactly what Tier Zero should comprise and how it should be protected.

Then IT environments began changing even more dramatically, particularly due to the rapid adoption of cloud technologies. To address the resulting security requirements, in 2020, Microsoft introduced the Enterprise Access model, which is the AD security model it recommends for most customers today.

Tier Zero has been an essential element of Microsoft's recommended security model since 2012.

Key Finding #3: IT organizations aren't staffed to support all their AD security needs.

Now let's address the million-dollar question:

Why are organizations struggling with vital AD security tasks like assessing vulnerabilities, spotting active threats and prioritizing their Tier Zero assets?

The core reason is that just half of IT organizations are adequately staffed to handle AD security.

Tight IT budgets are clearly one factor in this staffing shortfall — but the full explanation is far more nuanced.

50% short staffed

Half of IT organizations today can't handle their AD security needs with current staffing.

uevi.co/3729DZGY

Key Finding #3: Factor A — IT pros are overwhelmed.

More than half of IT pros surveyed say their highest priority is just finding enough time in their day to get everything done.

When you're already strapped for time, you may not be looking to revise priorities and rework processes. As a result, there's little opportunity to advance from a simple least privilege model to understanding and protecting Tier Zero as part of a modern Enterprise Access model.

53%

say their highest priority is finding time in their day to complete all of the necessary AD security-related management tasks.

uevi.co/2446KRCF

Key Finding #3: Factor B — Expertise in Active Directory is evaporating.

Another critical aspect of the IT staffing issue is a growing shortage of IT professionals with deep expertise in Active Directory. There are two complementary trends at work here:

- Many of the people trained on AD security — and those with specific institutional knowledge — have started to move on or retire.
- But often there's no one to replace them because new hires simply aren't being trained on AD security requirements and practices like they once were. Indeed, Microsoft has eliminated some important AD training courses and certifications, and more are on the chopping block in the coming years.

Key Finding #3: Factor C — It's often unclear who's responsible for AD security.

When it comes to identity threat detection and response (ITDR), just 4 in 10 organizations say there's alignment between their AD and SecOps teams. As a result, it's often unclear exactly who is responsible for what.

Moreover, 17% of respondents say ITDR decisions are left to IT leadership. In those organizations, it's even less likely for IT pros in the trenches to be championing initiatives like adopting a modern AD security model.

Only 41%

of organizations have agreement between AD and SecOps Teams on AD identity threat detection and response (ITDR).

uevi.co/2271IWKF

17%

of organizations leave ITDR decisions to IT leadership/CISO.

uevi.co/9320CFKX

Additional notable survey insights

Two additional survey results are worth noting:

- Less than 6 in 10 organizations have fully implemented the NIST Cybersecurity Framework (CSF), which provides a valuable and flexible framework for strengthening the security of an IT ecosystem, including the vital AD identity infrastructure.
- Many organizations are now paying close attention to supply chain risk management, likely because of devastating cyberattacks like the one that breached SolarWinds and rippled through to thousands of customers, from tech giants like Microsoft, Intel and Cisco to the U.S. departments of Homeland Security, State and Treasury.

Only 58%

of organizations have fully implemented the NIST Cybersecurity Framework.

uevi.co/1945OEXU

Nearly 2/3 assess supply chain security

64% of organizations assess the security practices and potential risk associated with the vendors in their supply chain.

uevi.co/1897KEWM

Recommendations

If your organization is facing the same AD security challenges reported in the Quest survey, here are reliable strategies for addressing them:

Prepare to adopt a modern security model by understanding your Tier Zero assets.

Don't let lack of insight into your Tier Zero assets keep you from adopting a modern Enterprise Access model. With third-party solutions, you can get a comprehensive inventory of your most valuable IT assets, including all privileged accounts, Group Policy objects, domain controllers, and other crucial servers such as those that host Azure AD Connect.

Uncover and mitigate the vulnerabilities that put your Tier Zero at risk.

If you haven't conducted an AD security assessment recently, get one scheduled. It's vital to understand where your environment is most vulnerable. That includes not just misconfigurations and other issues that could let an attacker gain a foothold in your environment, but also any weaknesses they could exploit once they are inside to escalate their privileges and move laterally to reach your Tier Zero assets. Make sure to test all fixes thoroughly before pushing them live to avoid unintended consequences.

Mitigate IT staffing woes by partnering with experts and choosing effective tools.

Cyber criminals are sophisticated and relentless, so security incidents are all but inevitable. Don't leave it up to chance whether you're ready. By working with a trusted partner and investing in a comprehensive AD security solution that covers all the functions detailed in the NIST CSF, you can empower your limited IT team to handle the full spectrum of AD security tasks, from vulnerability mitigation to threat detection & response to disaster recovery.