purple knight

powered by semperis

2025 PURPLE KNIGHT REPORT

The Ongoing Struggle to Secure Hybrid AD and Entra ID Environments

Users of Purple Knight, a community identity security assessment tool for Active Directory, Entra ID, and Okta, report on their security scores, ongoing challenges, and remediation plans.

KEY FINDINGS

- Average initial Purple Knight score reported was 61%, a failing grade, and 11 points lower than the average score reported in 2023.
- Survey respondents reported the worst scores in the category of AD infrastructure security. This result points to increased complications managing AD Certificate Services, which were targeted in the APT29 attack (also known as Midnight Blizzard).
- Government agencies reported the lowest scores among industry sectors, highlighting a lack of resources for addressing identity security.
- Teams responsible for AD and Entra ID reported lack of familiarity with Entra ID security best practices.
- By applying remediation guidance provided in the Purple Knight report, organizations were able to improve their scores by an average of 21 points up to a top improvement of 61 points.

Executive **Summary**

Identity systems—Active Directory (AD) and Entra ID in particular—continue to be a prime cyberattack target. The Five Eyes Alliance, a consortium of international security agencies, including CISA and NSA in the US, issued a warning in a joint paper, Detecting and Mitigating Active Directory Compromises: "Active Directory's pivotal role in authentication and authorisation makes it a valuable target for malicious actors. It is routinely targeted as part of malicious activity on enterprise IT networks."

Despite increased awareness of AD and Entra ID as an attack target, organizations continue to struggle to adequately secure their hybrid AD environments. Purple Knight users who responded to an online survey conducted by Semperis reported an average initial security assessment score of 61%, a failing grade, and down 11 points since the survey was last conducted in 2023.

The survey findings, in addition to in-person interviews with IT and security team members, point to continued challenges in adequately securing hybrid AD, Entra ID, and Okta identity systems for organizations across every industry sector.

However, IT and security teams are using the Purple Knight assessment results to make positive changes in their identity system posture. Respondents reported that using Purple Knight's remediation guidance has helped them close security gaps, raising scores by an average of 21 points and by as much as 61 points, and providing a framework for systematically addressing misconfigurations that can open doors for threat actors.

purple knight
powered by semperis

Table of **Contents**

WHAT IS PURPLE KNIGHT?

Purple Knight is a free Active Directory, Entra ID, and Okta security assessment tool developed by Semperis identity security experts that has been downloaded by 45,000+ users since its first release in spring 2021. Purple Knight scans the hybrid identity environment for 185+ security indicators of exposure or compromise. Users receive a graphical report with an overall score, 7 category scores, and guidance on how to remediate security risks.

Each security indicator is mapped to security frameworks such as MITRE ATT&CK, MITRE D3FEND, and the French National Agency for the Security of Information Systems (ANSSI). The report provides an explanation of what aspects of the indicator were evaluated and the likelihood that the exposure will compromise AD, Entra ID, and Okta.

Purple Knight has been cited in the Five Eyes Alliance report Detecting and Mitigating Active Directory Compromises, which offers guidance from on mitigating the 17 most common techniques used by adversaries and malicious actors to compromise AD, Entra ID, and Okta environments. Spearheaded by the Australian Cyber Security Centre in partnership with international agencies, including the U.S. Cybersecurity and Infrastructure Security Agencies (CISA) and the National Security Agency (NSA), the report called out Purple Knight as a community tool that helps organizations better understand their Active Directory security. For more information, visit semperis.com/purple-knight.

Why Organizations Download Purple Knight

As awareness grows of hybrid AD systems' vulnerability as an attack target, IT and security teams are motivated to find out how secure their own systems are. Purple Knight users cited three primary objectives in running Purple Knight.

1

Benchmarking

IT teams use Purple Knight on a regular schedule to set security score benchmarks and track progress over time.

"I'm a big fan of benchmarks," said Mike S., director of IT security and compliance for a dental insurance company. "And I'm always interested in tools that tell us how to do things. Purple Knight helps our network operations folks secure things better. I'm in favor of that."

2

Post-attack Assessment

In the aftermath of an AD-related attack, a Purple Knight scan can uncover overlooked vulnerabilities that still need to be addressed.

"We suffered an attack that compromised some of our systems, and we thought we were pretty secure in terms of Active Directory," said Jose G., a global admin at an IT services company. "We learned a lot from that event. Out of curiosity, I ran Purple Knight on the environment, and I found a new world of stuff to fix."

3

Preparation for Consolidation Projects

For organizations with legacy AD environments, consolidating AD systems is complicated by security concerns when configurations are changed.

Bob G., infrastructure team lead at a global shipping company, said his company has launched a multi-year project to reorganize the environment, which currently consists of about 30 AD forests. "Using Purple Knight to scan those environments helps us understand what might break in our permissions structure or what open security vulnerabilities we need to fix."

What Surprises **Purple Knight Users**

Purple Knight users who consider their organizations to be security-conscious were often surprised by their initial low scores.

"My pride took a little bit of a hit, for sure," said Eric M., senior identity engineer at a printing company. "I think I do a pretty good job. And we haven't been breached. But then you see the D-minus on your report card and it's like, wow. There are some things we could do better."

Eric said while it was painful to confront the score, he appreciated that he could use the results to "look under the hood" of his AD system and prioritize the highest risk factors for remediation.

Identifying permissions that were based on templates was an eye-opener, said Jose G. "There are a few objects in Active Directory where certain permissions are set, and new objects check on those permissions based on those templates. Those templates contained a lot of non-default settings that an admin thought were good, when in fact they weren't."

"I think I do a pretty good job. And we haven't been breached. But then you see the D-minus on your report card and it's like, wow. There are some things we could do better."

– Eric M.
Senior Identity Engineer, printing company

Which Categories Scored the Lowest in Initial Scans

Respondents scored an average of 61%—a failing grade—on their initial Purple Knight scans. Among the six categories of vulnerabilities included in Purple Knight, scores were lowest in the AD infrastructure category, followed by account security.

The AD infrastructure category includes several indicators focused on AD Certificate Services (ADCS), which was the target of the notorious APT29 (Midnight Blizzard) attack. ADCS security has historically been a challenging area for IT and security teams, said Jake Hildreth, Semperis Principal Security Consultant.

"Certificate Services is an island shrouded in mystery for most AD admins," he said. "It seems like it's either working, or it's broken, and you don't know why it's not working right."

Certificate Services are used for authentication to AD, so a misconfiguration could open access to high-value assets with one checkbox, Hildreth said.

"And it's wild how often that happens," he said. "In the Active Directory environments I've reviewed, using Purple Knight to scan the environment, there's always a finding about certificates."

The category with the second-lowest average score was account security, which includes commonly exploited vulnerabilities related to specific user accounts such as faulty password settings and overprivileged accounts.

WHICH VULNERABILITY CATEGORIES SCORED THE LOWEST?

1. AD delegation
2. Account security
3. Kerberos
4. Group Policy
5. Entra ID
6. Okta

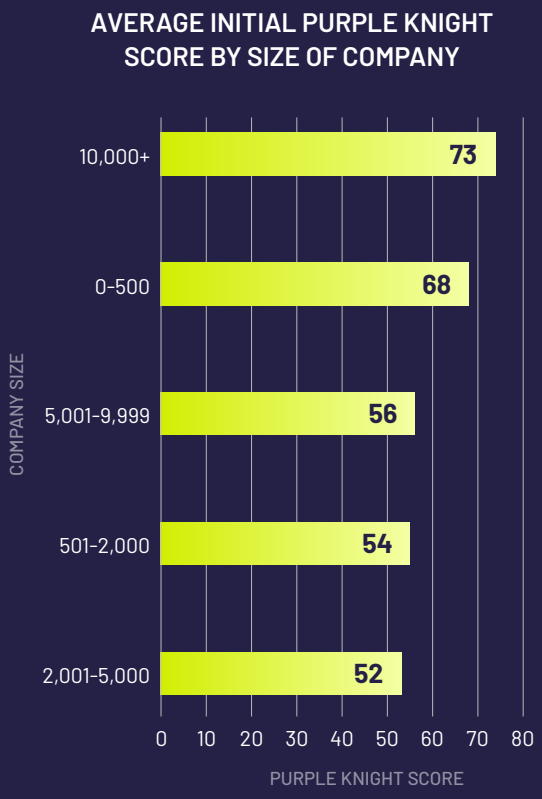
Midsized Companies and Government Entities Scored Lowest

Purple Knight score averages were highest among the largest organizations surveyed (10,000+ employees) and the smallest organizations (0-500). The worst average scores were reported by respondents in the middle three size tiers.

"The largest organizations have more resources, and the smallest organizations often have less complicated environments to secure," said Sean Deuby, Semperis Chief Technologist, Americas. "But the midsized companies are where the IT pros have to do everything. You don't have full-time AD specialists. So AD just runs until something breaks, then they patch it. But they don't have someone whose job it is to make sure AD is as healthy as possible."

That perspective was confirmed by Purple Knight user Raphael K., an IT admin in a manufacturing company with about 600 employees.

"Our security assessment is ongoing because our Active Directory is what we call a historical building," he said. "We just have to clean it up step by step."



"Our security assessment is ongoing because our Active Directory is what we call a historical building. We just have to clean it up step by step."

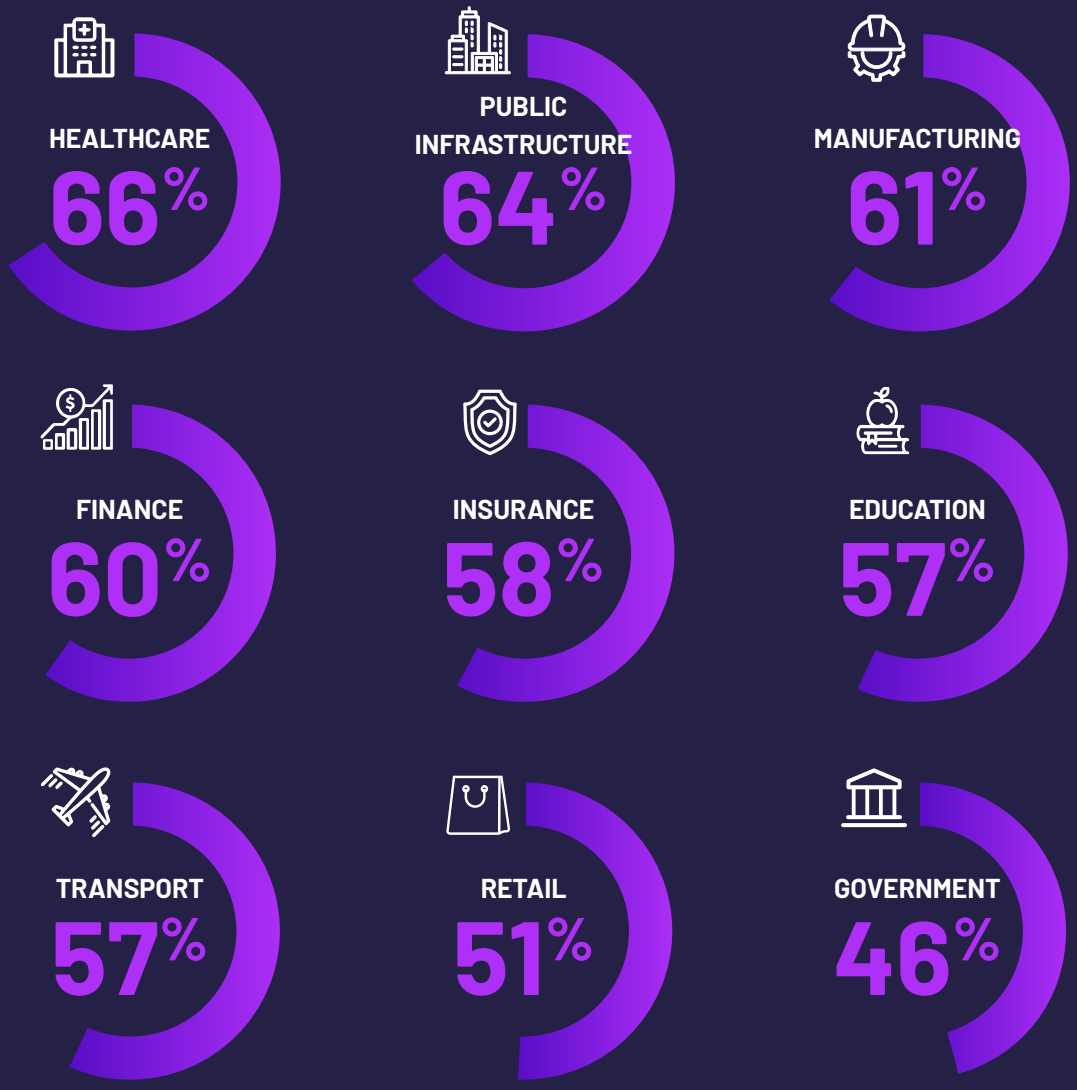
– Raphael K.
IT Administrator, manufacturing company

Midsized Companies and Government Entities Scored Lowest

The industry sector with the lowest average initial Purple Knight scores was government at 46%, a score that Deuby said likely reflected a lack of budget resources. The healthcare segment scored highest with 66%—still a poor score.

"The fact that the healthcare industry turned in the highest average scores doesn't surprise me because these organizations are so compliance-bound," he said. "But the initial score is still failing, which speaks to the overwhelmingly complex environments that IT and security teams in this field have to secure."

AVERAGE INITIAL PURPLE KNIGHT SCORES BY INDUSTRY SECTOR



How Users Apply
Purple Knight Findings

Respondents reported using the

PURPLE KNIGHT REPORT SCORES

and remediation guidance to systematically improve their AD environment security.

Prioritizing Remediation

"We are doing at least one Purple Knight scan a quarter to make sure things are staying how they should be," said Eric M. "In my role, I'm heavily involved in the strategy and mitigation of security-related items and misconfigurations. I use the Purple Knight report to understand everything that's going on. Based on what we know about our environment, maybe there are some really quick wins. I say let's just get those done. Then we use change management processes to tackle the critical findings."

"We run those results through risk analysis," said Mike S. "The high-risk things are the ones we make the network operations group fix. In 2024, this process resulted in 13 tickets for the critical and warning indicators of exposure."

Evaluating Security Before a Migration

"We moved from Microsoft Exchange and wound up needing an Entra ID environment," said Mike S. "That made everybody in my organization very nervous. There are so many checkboxes. I realized that I could use Purple Knight to test the Entra ID."

Learning About AD and Entra ID Security Best Practices

Many organizations lack AD and Entra ID skillsets on staff, particularly in securing hybrid AD environments. In the Purple Knight survey, 57% of respondents reported they were only "somewhat familiar" and 22% reported they were "not at all familiar" with Entra ID security best practices.

"I have definitely grown as a subject matter expert over Active Directory and Entra ID very quickly from using Purple Knight," said Eric M. "The tool uncovers these problems, then I research how attackers were abusing AD and how to mitigate the problems. It's opened my eyes and my mind to how Active Directory comes together."

Jose G. said Purple Knight exposed the state of his AD environment. "It offers a lot of knowledge in such an easy way to get it. If you contract an external consultant to perform an audit on your Active Directory, it will cost a lot of money, will take a long time, and maybe the results will be the same as you get with Purple Knight. Best case is to go run this check."

Another respondent commented: "There are so many ways to mess up configuration in Entra and Active Directory. It's helpful to have a second set of eyes reviewing the choices you've made."

Communicating Identity Security Posture to Leaders

The Purple Knight report includes visual graphs that capture the key points about the identity environment security posture, which saves time for IT and security teams.

"I can just directly hand off the full Purple Knight PDF to upper management and our security status is very clear to them," said Eric M. "I don't have to spend extra cycles digesting the information and building a summary. And you know management, they like charts. Seeing the security posture score go up is very, very valuable."

"I have definitely grown as a subject matter expert over Active Directory and Entra ID very quickly from using Purple Knight."

– Eric M.
Senior Identity Engineer, printing company

Taking Steps to Improve Identity Security Posture

Although average

initial scores were alarmingly low

among respondents, they reported using the remediation guidance to significantly improve their security posture.

Respondents reported an **average improvement of 21 points** from the first scan to their top score. **The best improvement cited was 61 points.**

Using Purple Knight to shed light on their organizations' security posture was the first step in closing security gaps and reducing risk of an identity-related cyberattack.

"Purple Knight helps discover a lot about an environment, and helps me fix issues quickly to lower the security risk," said a respondent.

BEST IMPROVEMENT → **61 POINTS**

METHODOLOGY

We invited nearly 100 verified Purple Knight power users to complete an online survey about their experience with Purple Knight and the results of their Active Directory, Entra ID, and Okta security environment assessments. We also conducted one-on-one follow-up interviews with users to gather more in-depth information about their Purple Knight scores, specific challenges in securing their identity systems, and how they have used the Purple Knight remediation guidance to improve their overall security posture.

Respondents included IT practitioners, CTOs/CIOs, SOC engineers, and CISOs from a cross-section of industries, including healthcare, public infrastructure, financial services, government, and manufacturing. About 70% of respondents worked in organizations of 2,000 or fewer employees. Each of the respondents who completed the survey received a $50 gift card for their time.

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.

Semperis hosts the award-winning Hybrid Identity Protection conference and podcast series and built the community hybrid Active Directory cyber defender tools Purple Knight and Forest Druid. The company has received the highest level of industry accolades, recently named an Inc. Best Workplace for 2025 and ranked the fastest-growing cybersecurity company in America by the Financial Times. Semperis is a Microsoft Enterprise Cloud Alliance and Co-Sell partner and is a member of the Microsoft Intelligent Security Association (MISA).

To learn more about Purple Knight, built by Semperis, go to semperis.com/purple-knight.

semperis

+1-703-918-4884 | info@semperis.com | www.semperis.com
5 Marine View Plaza, Suite 102, Hoboken, NJ 07030