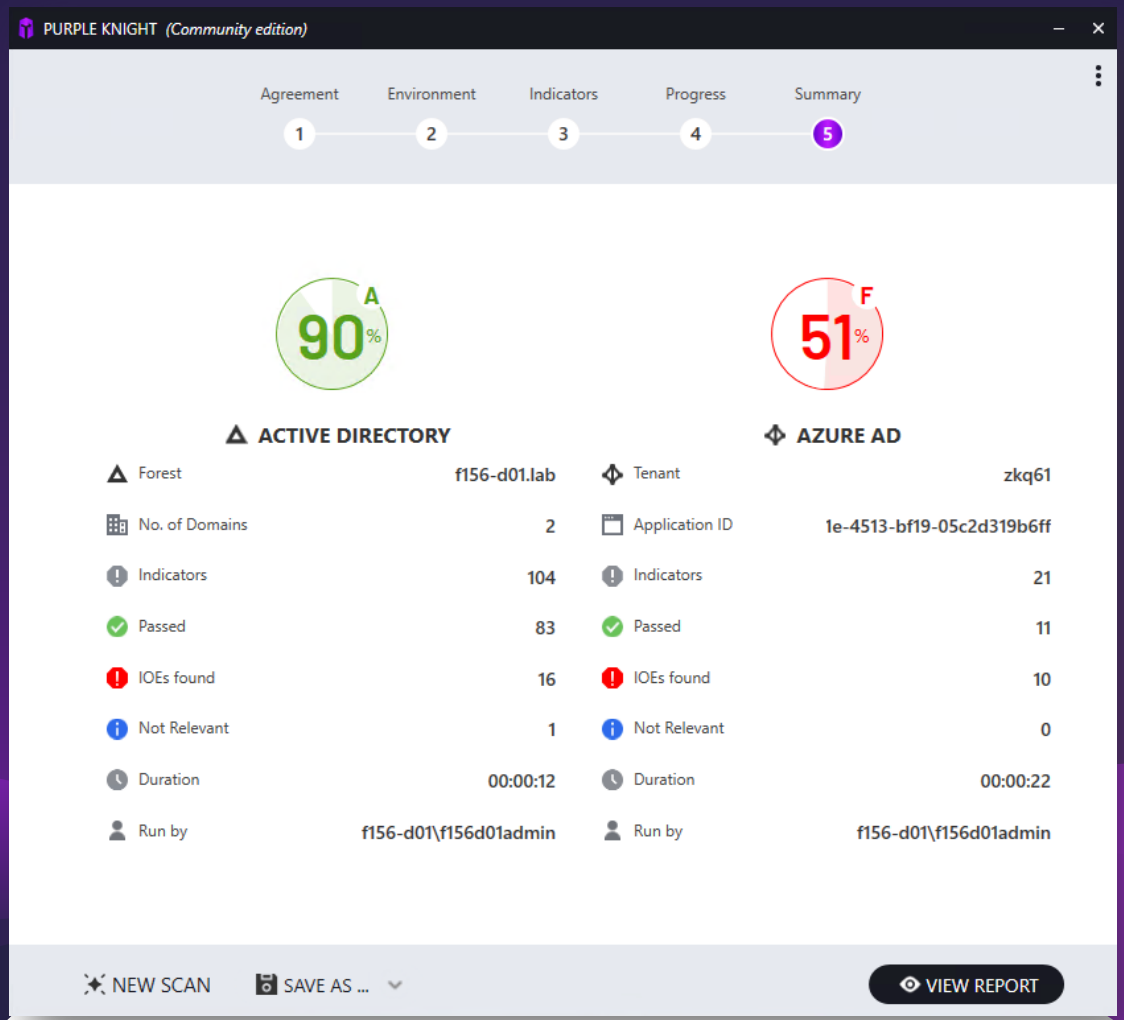
semperis

2023 Purple Knight Report

A survey of 150+ users of Purple Knight, the Active Directory security assessment tool downloaded by 20,000+ organizations

- Overview
- Challenges
- Findings
- Actions
- Methodology
- FAQs



Purple Knight scans the Active Directory environment for 150+ security vulnerabilities and provides a total average security posture score, individual category scores, and detailed remediation guidance that IT and security teams can use to close security gaps.

Organizations continue to report low scores on Purple Knight Active Directory security assessment

But users report improvements as high as 64% after using expert guidance to remediate

Users of Purple Knight, the community Active Directory (AD) security vulnerability assessment tool built by Semperis experts, reported an average score of 72 out of 100 on their initial reports—a low C grade—in a 2023 survey of 150+ organizations.

While the average overall score is better this year when compared with the average score of 61% reported in the 2022 survey, the results indicate that organizations are still struggling to identify and address security vulnerabilities that leave their identity environments open to cyberattacks. These results corroborate findings from Microsoft: According to the 2022 Digital Defense Report, **88% of Microsoft customers impacted by cyber incidents had "insecure AD configuration."**

One bright spot in this year's report: Organizations reported **score improvements averaging 40% and up to 64%** following remediation efforts using expert guidance provided by Semperis' AD security experts in the Purple Knight security assessments.

What is Purple Knight?

Purple Knight is a community (free) Active Directory security assessment tool developed by Semperis directory services experts that has been downloaded by 20,000+ users since its first release in spring 2021.

Purple Knight scans the Active Directory environment for **150+ security indicators** of exposure (IOEs) or compromise (IOCs). Users receive a graphical report with an overall score, 7 category scores, and expert guidance on how to remediate security risks.

Key findings from the 2023 survey

- Organizations scored an average of 72 on their initial AD security assessments—better than last year's average score of 61, but still a low C grade.
- Organizations reported an average score of 61 in the account security category, the lowest score among the seven AD categories assessed by the Purple Knight tool; 55% of organizations reported 5+ vulnerabilities in the Azure AD category
- 13% of organizations also reported 5+ security indicators in the new Azure AD category, which focuses on vulnerabilities such as inactive guest accounts and misconfigured conditional access policies
- Users reported an average of 40% improvement—and as much as 64% improvement—on subsequent assessment scores after applying the remediation guidance included in their assessments.
- Beyond using the Purple Knight results for remediation, organizations use the tool to uncover unknown vulnerabilities, communicate security posture to leaders and other teams, compensate for lack of in-house AD skills, prepare for other assessments including pen tests, and garner more resources for AD security improvements.
- Despite multiple warnings from analysts, coverage of ongoing AD attacks, and urgent calls for action from their own IT teams, many organizational leaders are not prioritizing AD-specific security and recovery, leaving them vulnerable to proliferating AD-based attacks.

Why did Semperis release a free Active Directory security assessment tool?

"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 Mickey Bresman, Semperis CEO. "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."

Top challenges in fixing AD security vulnerabilities

1. Lack of visibility into AD vulnerabilities
2. Lack of time and resources to address proliferating vulnerabilities
3. Lack of attention to AD security problems from business leaders and other teams
4. Complications from inherited or legacy AD infrastructures
5. Failure of third-party audits to identify security vulnerabilities

"I'd like to think I'm doing a better job, but tools like this douse me with cold water."

"It's a matter of us all being overworked and not being able to find the time to fix everything."

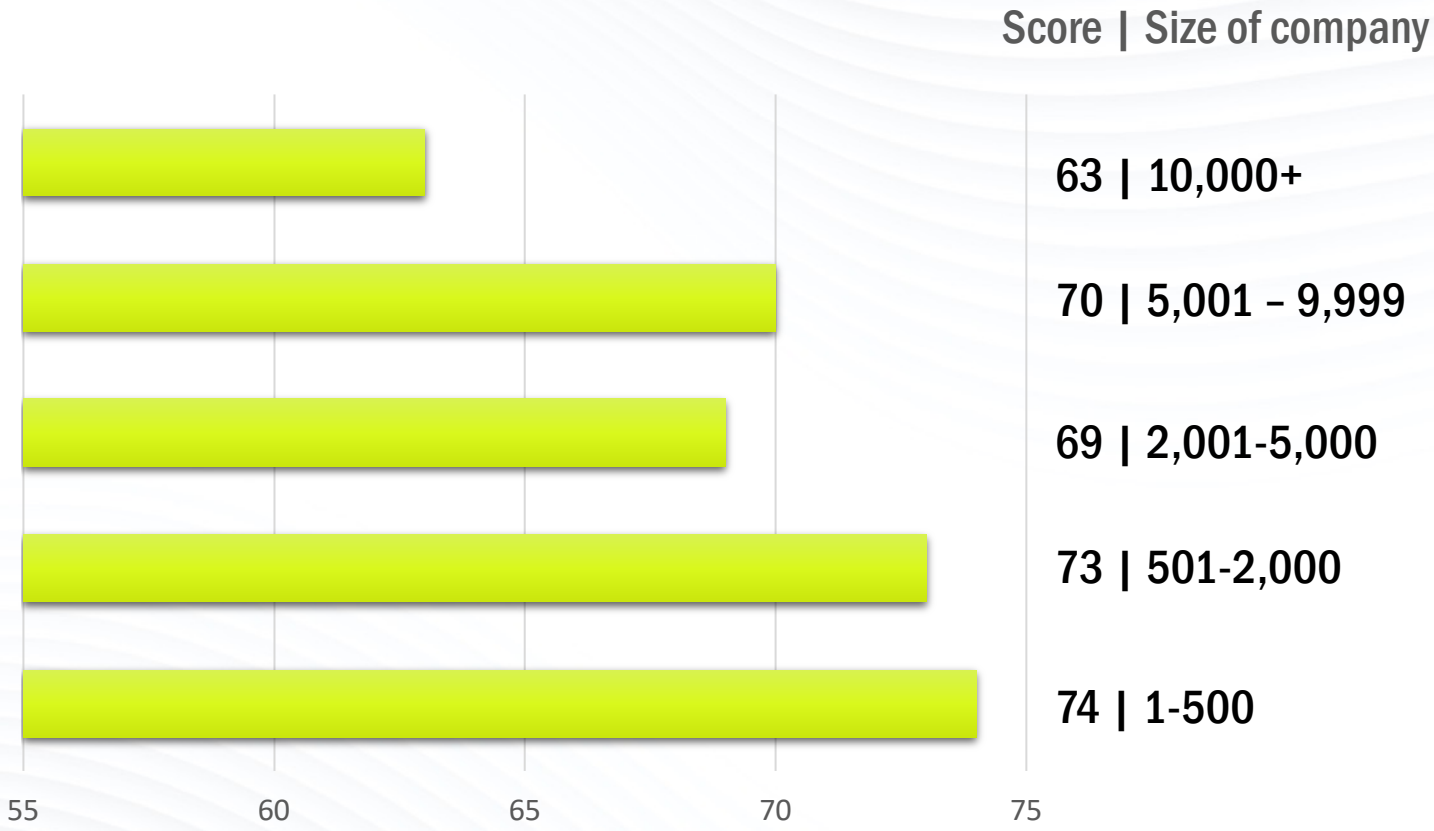
"There's a lot of 'planned activity,' but we are frankly ignorant of remediation at the executive level. Pretty frustrating."

"We've grown through acquisitions. Some of the companies haven't adhered to security standards. It's kind of the Wild West."

"We had a walkthrough with AD and Azure AD pros, and they missed some of the things this tool revealed."

SURVEY RESULTS: 2023 Purple Knight Report

Large organizations reported lowest average security scores

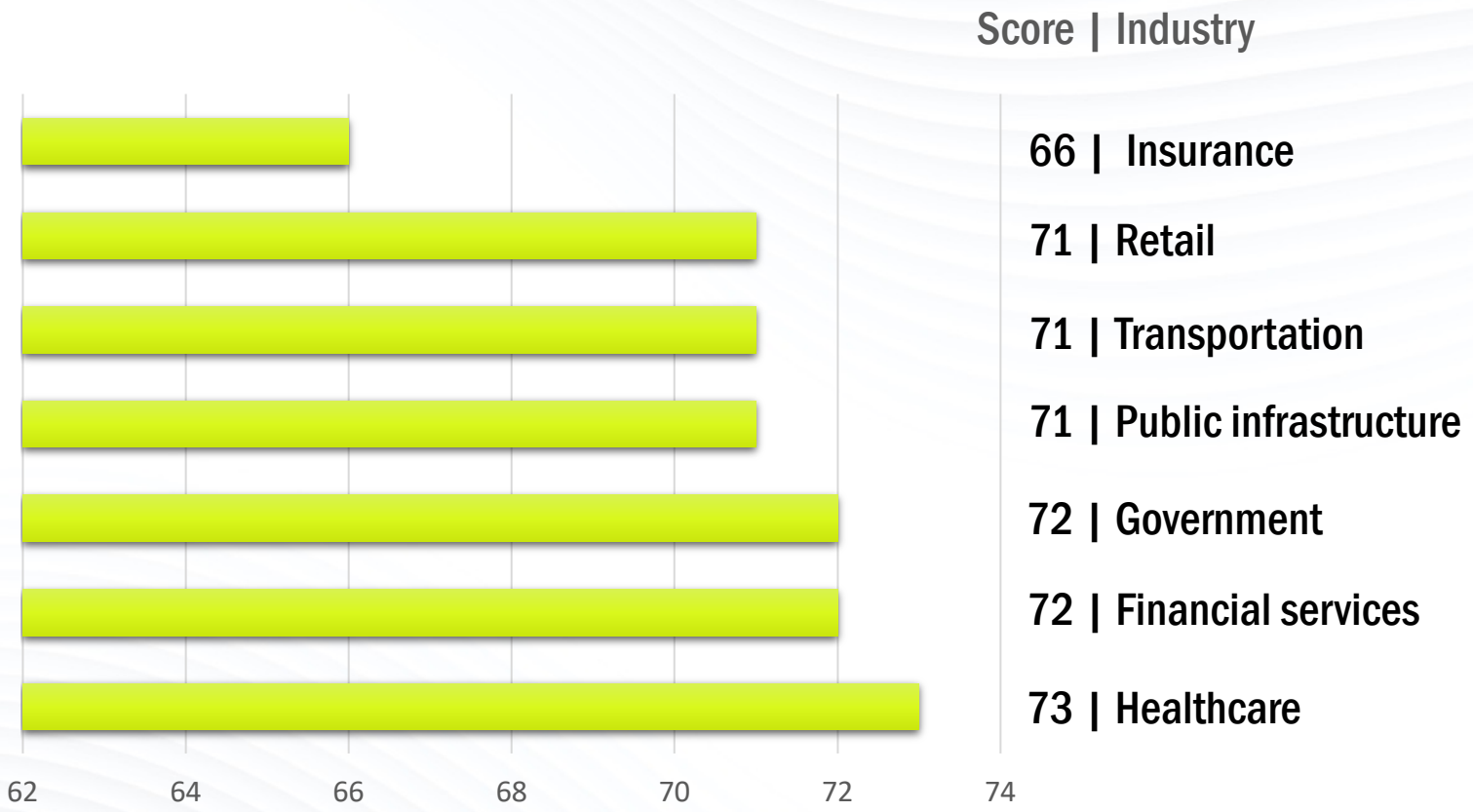


Legacy AD misconfigurations confound large organizations

Respondents from the largest organizations with 10,000+ employees reported the lowest average security score—63, which is nearly 10 points lower than the average score of all organizations combined.

The biggest factor contributing to lower scores in large organizations is legacy AD environments with accumulated misconfigurations, particularly for companies that have inherited disparate AD infrastructures through frequent merger-and-acquisition activity.

Insurance companies reported the lowest security scores

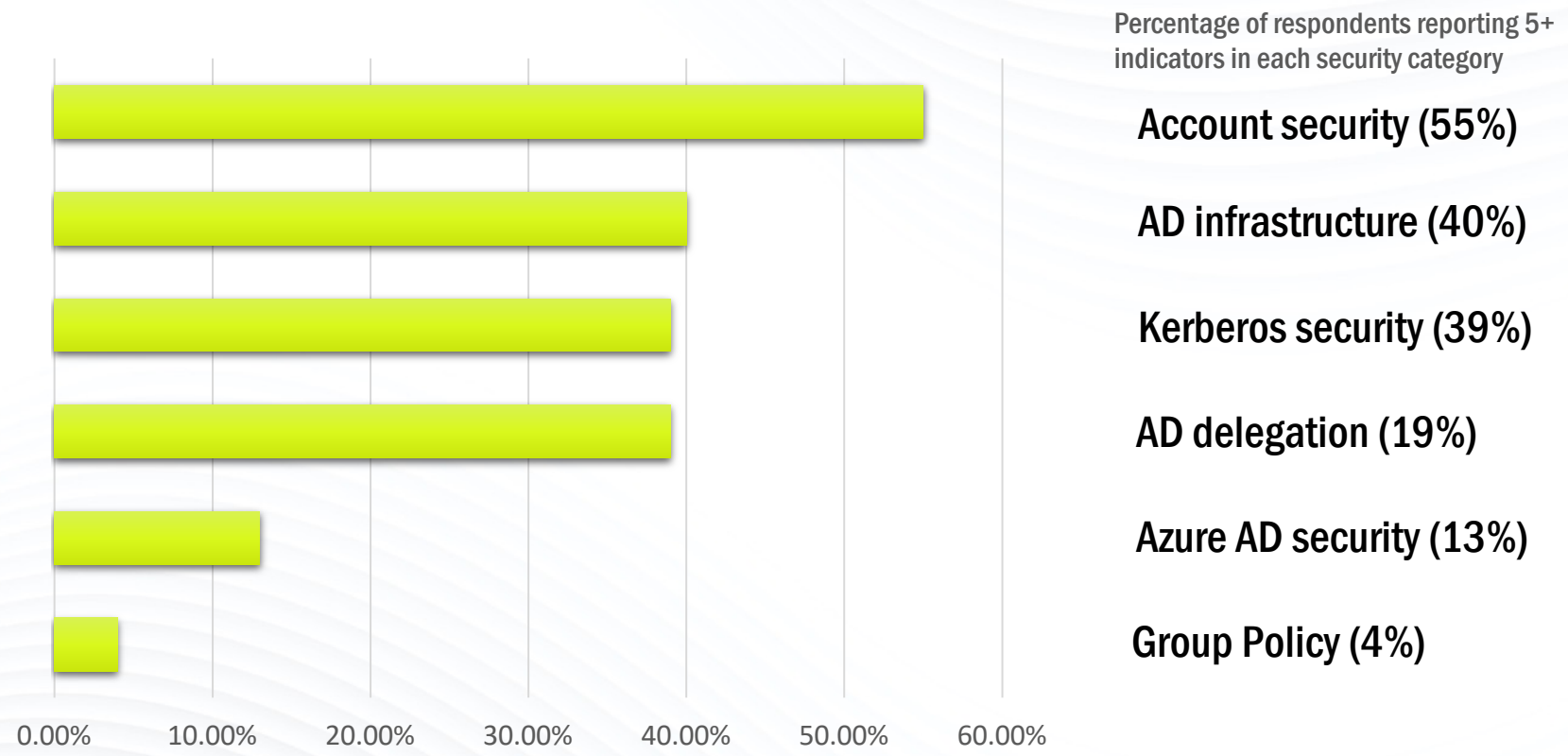


Cyberattacks target AD environments across industries

With the notable exception of the insurance vertical market, most organizations reported similar overall average security scores, ranging from 71 to 73.

Organizations across every vertical market are being targeted by sophisticated ransomware groups. Organizations with security scores in the low 70s have significant work to do in closing off security gaps that are frequently targeted by ransomware groups such as Vice Society, LockBit, BlackCat, Clop, and more.

Organizations score lowest in account security: 55% of respondents reported 5+ indicators in this category



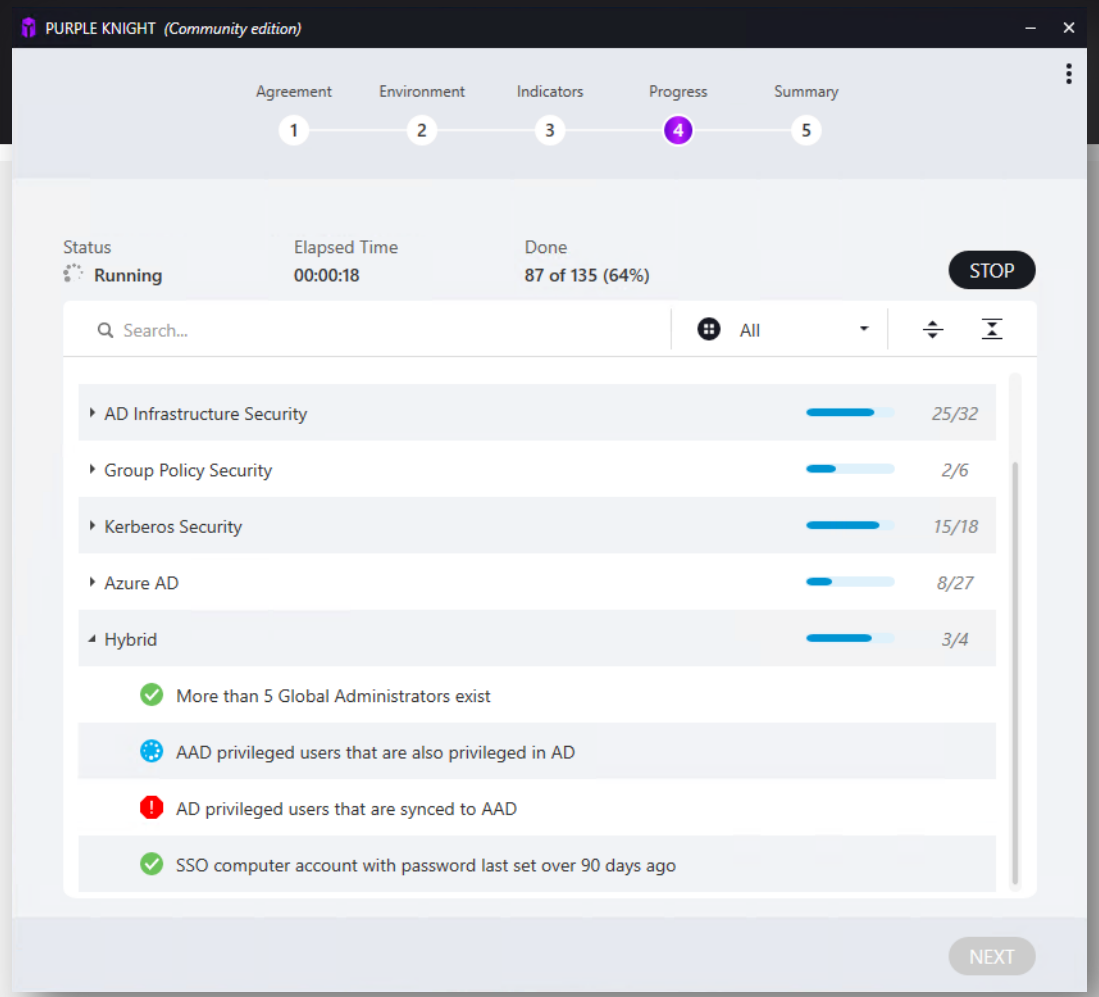
Account security remains the lowest-scoring category

Of the 7 Active Directory security categories included in the Purple Knight assessment, organizations scored lowest—61 on average—in account security, which pertains to the security of individual accounts in AD.

In last year's report, the average account security score was 57.

Common vulnerabilities uncovered by Purple Knight

- Non-default principals with DC Sync rights on the domain
- Privileged users with weak passwords
- Anonymous access to Active Directory enabled
- Unprotected accounts with admin rights
- User accounts with old passwords
- Admin accounts with old passwords
- Azure AD privileged users that are also privileged in AD

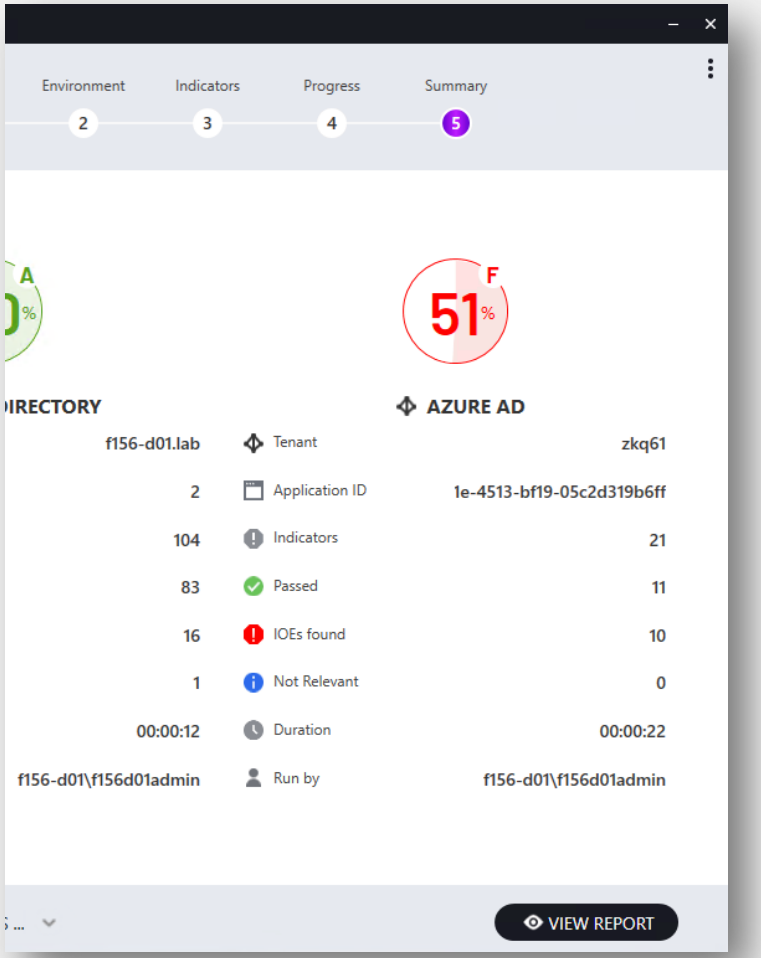


Purple Knight scores the AD environment in 7 security categories, which are classified as informational, warning, or critical

Azure AD emerges as security category organizations are tracking

Most organizations have embraced a hybrid identity infrastructure with both on-premises Active Directory and Azure AD (now Microsoft Entra ID). Purple Knight added Entra ID security indicators in 2022.

- 13% of survey respondents reported 5+ security indicators in the Azure AD (Entra ID) category
- Azure AD (Entra ID) category vulnerabilities include:
  - Inactive guest accounts, which leave an open gate to the Azure AD tenant
  - Azure AD users that are eligible for a privileged role, which could result in privilege escalation
  - Numbering matching enabled in MFA, which could make the account vulnerable to MFA bombing



ACTION ITEM:

Use prescriptive guidance in the report to accelerate remediation

- The top action Purple Knight users take after running an initial scan is applying the expert remediation guidance provided in the report to systematically address security vulnerabilities.
- Users reported an average of 40% improvement—and as much as 64% improvement—on subsequent assessment scores after applying the remediation guidance included in their assessments to close existing security gaps.
- Respondents are adding periodic Purple Knight scans to their ongoing AD security evaluation process, using the scores to set future improvement goals.

"We improved our AD and Azure AD security posture by solving the indicators of exposure (IOEs) Purple Knight showed us."

"We've added the critical fixes to our monthly project list and are working to score above 70% in the next 3 months."

"We have monthly remediation review meetings to track progress."

ACTION ITEM:

Identify unknown AD vulnerabilities

- Because many organizations have legacy AD environments with misconfigurations that have accumulated over time, many current IT teams (and business leaders) are unaware of the number and severity of AD vulnerabilities in their environments.
- Even seasoned AD administrators were surprised at the vulnerabilities in their AD infrastructure that Purple Knight uncovered, especially if they are security-minded.
- By regularly re-scanning the environments, respondents aspire to stay ahead of emerging threats.

"Purple Knight looks at things I've never thought of looking at, and I've been working with AD since the beginning."

"Purple Knight helped highlight many of the things that we were unaware of as a company."

"Some IOEs were known to our organization, others will be addressed ASAP."

ACTION ITEM:

Compensate for lack of in-house AD skills

- Because AD is a nearly quarter-century-old technology, many organizations lack IT professionals with AD experience, so they rely on outside consultants or tools to fill the gap.
- AD misconfigurations can have a big impact on the environment, so many IT teams are reluctant to change settings that were implemented years ago by previous administrators.
- Without current knowledge of how cyberattackers are targeting AD, IT teams often don't know where to look for signs of compromise in the AD environment.

"I will use this as a guide to mitigate efforts and also learn best practices."

"Purple Knight gives good advice for remediation for those that may not be as familiar with AD."

"Due to our current team not being the one that originally implemented our AD environment, this report has been very helpful in determining where we lacked visibility for a lot of these accounts and settings."

ACTION ITEM:

Collaborate with other teams to improve security

- Improving AD security often falls through the cracks at many organizations because IT and security professionals are on different teams, so having a clear report on AD vulnerabilities helps foster communication and collaboration.
- The Purple Knight report provides a clear roadmap for improving security that both IT and security teams can incorporate into their security and operational KPIs.
- Collaboration on improving overall security posture lays the groundwork for IT and security teams to work together in the event of a cyber disaster that targets the identity environment.

"We meet weekly with our corresponding technology team to create action items that correct issues found and improve our scan result scores."

"I, the cybersecurity engineer, have extensive plans to have the team managing AD address these issues."

"When we acquire companies, we can send this report to the new company's IT team so we can all knock out the top items."

ACTION ITEM:

Convey AD security problems to business leaders

- Although AD is well known as a common target in cyberattacks, organizational leaders fail to allocate sufficient resources to address the problem, often because of budget concerns or a misplaced conviction that the problem is already being addressed.
- Because AD administration is part of the IT operations structure in most organizations, it's not viewed as an essential part of the overall security strategy.
- Using clear reports and actionable remediation guidance, IT and security teams can convince leaders to allocate resources to fixing business-critical AD security vulnerabilities.

"We are trying to get management to remove the delegation and other configs that are causing us to fail."

"We've made recommendations to management based on the outcome of the assessment and plan to run it quarterly to gauge progress."

"I presented the results to the IT Director in an effort to get more resources assigned to correcting the critical issues.."

ACTION ITEM:

Prepare for other security audits

- IT and security teams often used a variety of cybersecurity tools to identify vulnerabilities in their organizations, including free tools, and compare the results to eliminate blind spots.
- Some security pros used the Purple Knight assessment to close gaps before a planned pen testing project.
- IT pros reported that third-party audits and consultants often did not uncover the same vulnerabilities that the Purple Knight assessment revealed, making it a valuable cross-check to current security efforts.

"If we had run Purple Knight before our last pen test it would have saved us some negative findings."

"I ran Purple Knight to compare its output with the Microsoft AD assessment, our homegrown tool, and other tools for comparison in features and further usage."

RECOMMENDATIONS:

Don’t delay reducing the AD attack surface

Organizations can take meaningful action to improve security posture and reduce the AD attack surface to avoid incidents that can disrupt business operations for weeks or months.

- Download Purple Knight to assess the current security posture of your AD environment. As one Purple Knight user said, “Knowledge is power!”
- Use the results to remediate security vulnerabilities, starting with critical indicators.
- Develop a plan for systematically finding and fixing security gaps, in collaboration with other teams.
- Use the Purple Knight scorecard to convey the risk and consequences of inaction to organizational leaders.

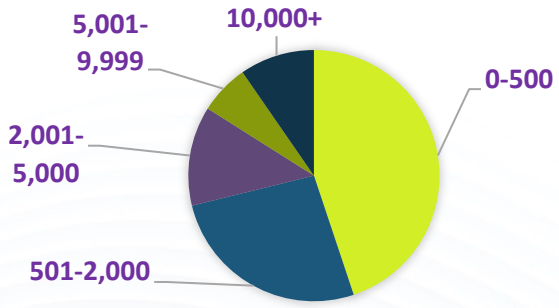
Resources

- Purple-Knight.com
- Purple Knight security indicators
- Purple Knight FAQ
- Purple Knight videos
- Download Purple Knight

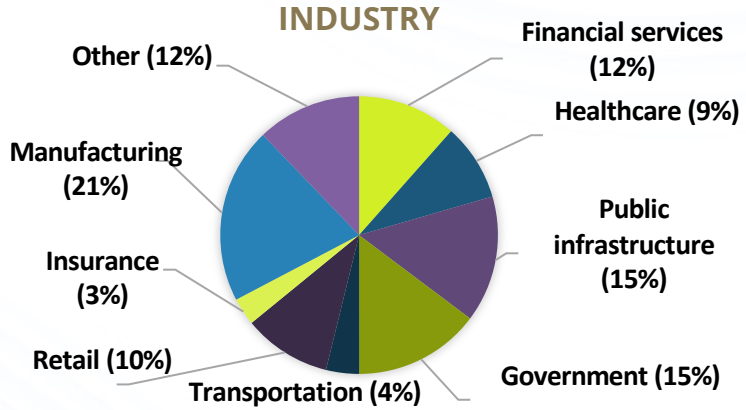
Methodology

We invited verified Purple Knight users to complete a survey about their experience with using Purple Knight and the results of their Active Directory security environment assessments. The 156 respondents included IT and AD infrastructure administrators, CTOs/CIOs, SOC engineers, and security leaders from a cross-section of industries. Respondents represented organizations of all sizes. Each respondent who completed the survey received a $100 gift card for their time. We also conducted follow-on interviews with respondents who expressed interest in providing additional feedback about Purple Knight.

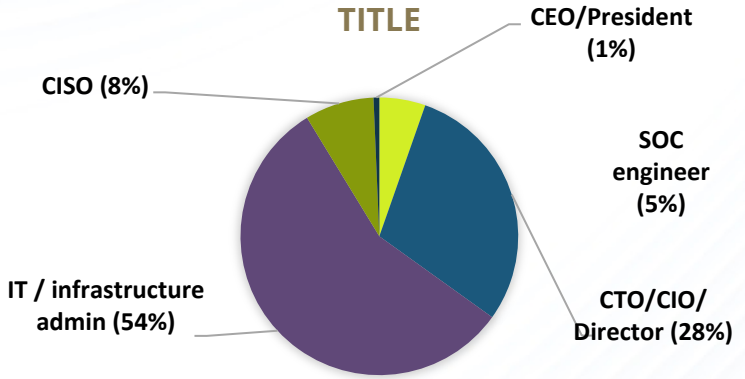
COMPANY SIZE (# OF EMPLOYEES)



INDUSTRY



TITLE



What is Purple Knight?

Purple Knight is an Active Directory and Azure AD security assessment tool used by thousands of organizations to quickly identify vulnerabilities in hybrid AD environments and receive prioritized, expert remediation guidance.

What does Purple Knight cost?

Purple Knight is free community tool.

Why should I use Purple Knight?

To lock down your hybrid Active Directory environment, you must think like an attacker. Purple Knight maps pre- and post-attack security indicators to the MITRE ATT&CK and ANSSI frameworks, offering an overall risk score along with the likelihood of compromise and specific remediation steps. Purple Knight also provides new security framework tags for the MITRE D3FEND model, a beta framework for network defense. You can use Purple Knight to proactively harden AD and Azure AD against new adversary tactics and techniques with built-in threat modeling that is constantly updated by a team of security experts.

Does running Purple Knight make changes to my Active Directory?

No, Purple Knight does not make changes to Active Directory. The tool requires the ability to run PowerShell scripts and uses LDAP queries over RPC for specific vulnerability scans.

Which Active Directory permissions are required to run Purple Knight?

Purple Knight is designed to give a quick snapshot of your AD and Azure AD environment as an attacker would see it. Therefore, Purple Knight does not require any elevated or administrator permissions..

What does Semperis do with the information Purple Knight generates about my environment?

Nothing! Purple Knight has no phone-home capabilities. The data and information that the tool generates are exclusively available to the organization running the tool and never available to Semperis.

How many security indicators does Purple Knight track?

The Semperis Research Team continuously studies the ways cyber criminals are plotting to compromise organizations' information systems—particularly by exploiting vulnerabilities in AD and Azure AD. Semperis uses this threat intelligence to constantly update the list of security indicators that Purple Knight tracks. For a complete list of indicators, review the Purple Knight Security Indicators.

Does Purple Knight look at anything beyond AD?

Purple Knight covers on-premises AD, Azure AD, and Okta (as of August 2023).

How long does a Purple Knight scan take?

The time needed to run a Purple Knight scan varies depending on the size and complexity of your Active Directory environment and the scans being run. Typically, a scan of one forest takes minutes, with additional time required for a Zerologon scan, which runs RPC to scan against all domain controllers.

How does Purple Knight adjust to emerging threats, new weaknesses, and new attack tactics?

The Semperis Research Team continuously studies the ways cyber criminals are plotting to compromise organizations' information systems—particularly by exploiting vulnerabilities in Active Directory. Semperis uses this threat intelligence to constantly update the list of security indicators that Purple Knight tracks.

How do I use the results of my assessment?

Purple Knight generates a detailed report that includes all scanned indicators, the pass/fail status of each indicator, its mapping to the MITRE ATT&CK and other frameworks, and remediation recommendations. Purple Knight users have applied the results to initiatives that improve overall security of their identity environments, including:

- Using the remediation guidance to close security gaps
- Sharing the reports with other teams and business leaders to foster collaboration
- Preparing for other security audits and pen testing
- Learning more about AD and Azure AD security vulnerabilities
- Gaining support for more resources to address security gaps

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 Active Directory environments, Semperis' patented technology protects over 50 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 (www.hipconf.com) and built the free Active Directory security assessment tools Purple Knight (www.purple-knight.com) and Forest Druid. The company has received the highest level of industry accolades, named to Inc. Magazine's list of best workplaces for 2023 and 2022, 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 member of the Microsoft Intelligent Security Association (MISA).

+1-703-908-4884
info@semperis.com
www.semperis.com

221 River Street
9th Floor
Hoboken, NJ 07030