Cayosoft

The State of Free Microsoft Identity Tools

Research conducted by Petri sponsored by Cayosoft measuring the effectiveness of Microsoft identity threat detection and change monitoring tools.

Sponsored by Cayosoft

PETRI
WE GET IT

Survey reveals free tools lack real-time detection and comprehensive Microsoft platform visibility

The State of Free Microsoft Identity Tools Survey, conducted by Petri, highlights an important reality in today's hybrid enterprise landscape: many organizations rely on tools that provide periodic snapshots of their security posture and lack the real-time detection and continuous coverage needed to keep pace with modern identity-based threats.

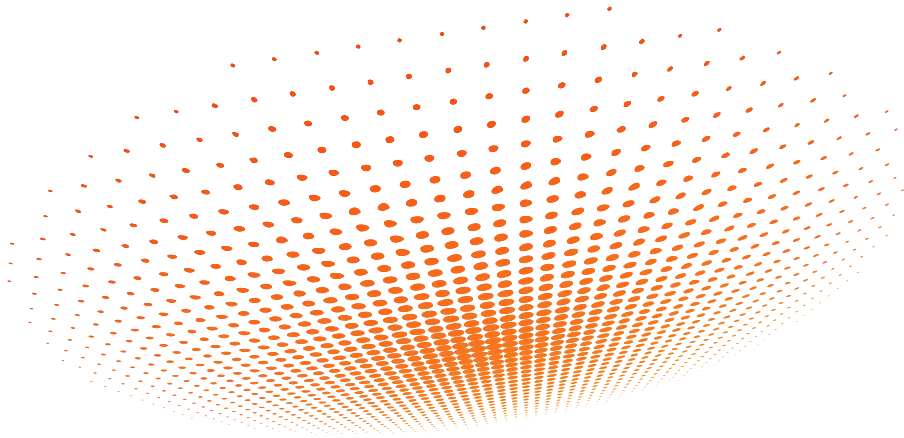
More than 90% of respondents report managing hybrid Microsoft environments that span Active Directory, Entra ID, Teams, Exchange Online, and Intune. These platforms collectively represent the core of most organizations' identity infrastructure and are the most frequent target for threat actors.

The survey reveals that nearly half of participants lack real-time alerting, continuous monitoring, and automated threat intelligence updates across their Microsoft platforms.

This gap in visibility leaves administrators and security teams exposed to blind spots that can lead to undetected identity risks and delayed response.

Over 91% of respondents have AD, Entra ID, Teams, Exchange Online, and Intune and report the following challenges with threat monitoring across platforms:

- **40% said AD is hard to monitor for threats**
- **37% said Entra ID is hard to monitor for threats**
- **31% said Teams is hard to monitor for threats 32% said Exchange is hard to monitor for threats**



The survey paints a picture of widespread fragmentation and fatigue in identity security operations.

- Many teams rely on a patchwork of scripts, logs, and standalone scanners that require manual effort to maintain.
- Tools often overlap or leave coverage gaps between on-premises and cloud systems.
- Budget pressures and tool sprawl compound the issue, forcing teams to prioritize cost and simplicity over depth and automation.

The expanding attack surface requires more coverage

Hybrid attack surfaces are expanding rapidly for organizations of all sizes. Misconfigurations, dormant accounts, and privilege escalations within Active Directory and Entra ID continue to rank among the top exploit vectors for ransomware and insider threats. Collaboration tools such as Teams and Exchange Online introduce additional layers of complexity, where changes to permissions or ownership can quietly open doors to sensitive data.

The findings indicate a fundamental shift in what IT and security leaders now consider essential: continuous, automated, and context-rich visibility across every layer of their identity ecosystem. Rather than relying on periodic scans or post-incident reviews, organizations are seeking real-time monitoring and alerting to reduce detection time, close compliance gaps, and strengthen operational resilience.

This latest research highlights a growing industry consensus: snapshot security is no longer sufficient. To protect modern hybrid environments, enterprises require continuous monitoring, instant alerting, and adaptive intelligence that keeps pace with every change in the identity landscape.

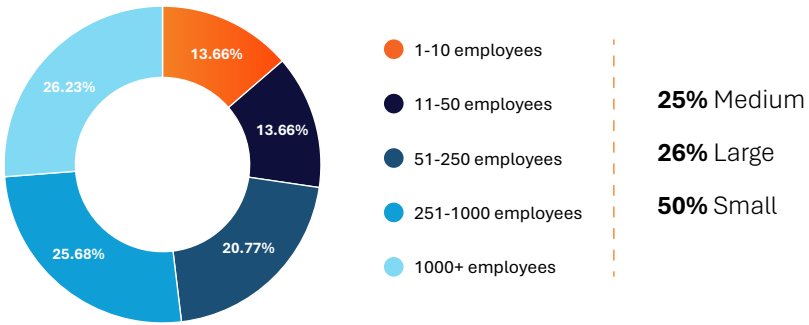
Survey methodology and demographics

Petri's The State of Free Microsoft Identity Tools Survey Petri's gathered insights from 183 respondents, including hands-on administrators, IT managers, security engineers, and compliance leaders responsible for managing Microsoft identity infrastructure. The survey explored how organizations handle visibility, threat detection, and change monitoring across hybrid Microsoft identity environments.

Relationship to Microsoft identity infrastructure

- **51.9%** Manage Microsoft identity systems
- **14.2%** Oversee management teams
- **21.3%** work in security/compliance
- **87%** have direct responsibility for protecting Microsoft identity infrastructure

Organization Size

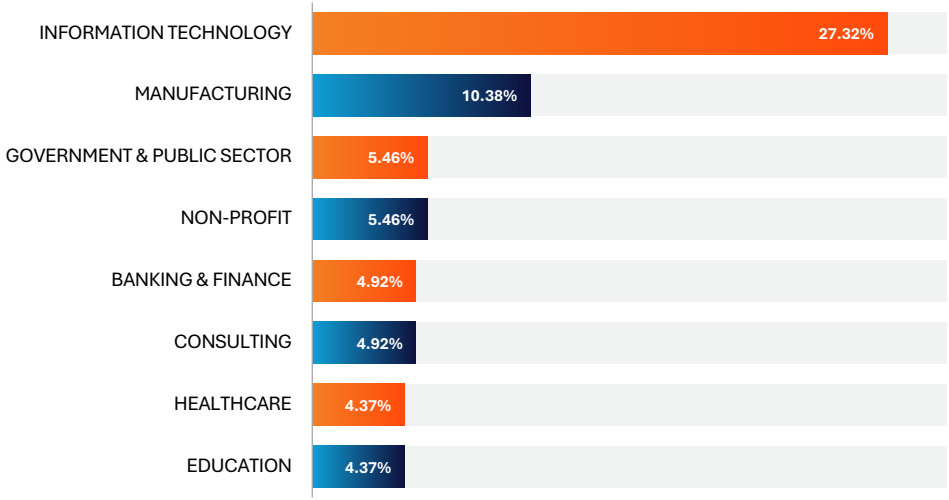


25% Medium

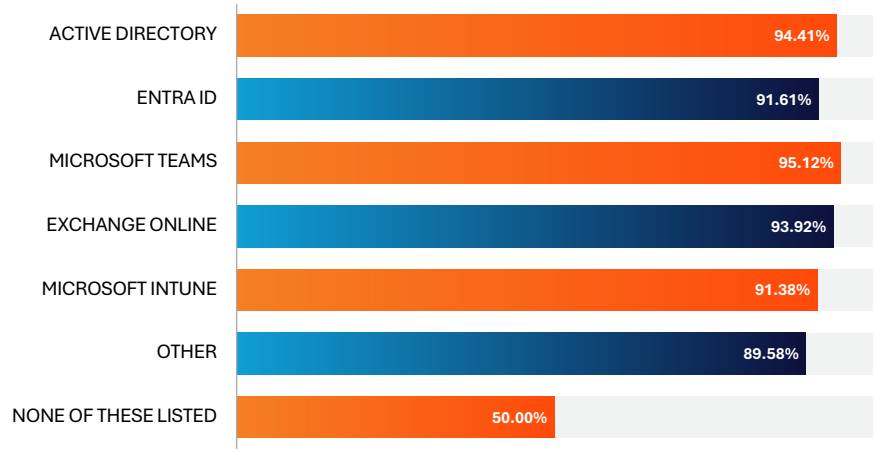
26% Large

50% Small

Industry



Identity Systems



Key Findings: Visibility and threat detection gaps

1. Hybrid environments lack platform visibility

Over 90% of organizations use five or more Microsoft platforms:

94% Active Directory

92% Entra ID

95% Microsoft Teams

94% Exchange Online

91% Intune

Takeaway: *Despite widespread hybrid adoption, point-in-time scanners leave gaps in Microsoft's identity stack. Continuous visibility and full platform coverage is now a baseline requirement.*

2. Top concerns with identity monitoring

When asked about their biggest monitoring concerns:

60.66% cited tracking the latest vulnerabilities and threats

53.55% fear missing real-time alerts

36.61% struggle with incomplete visibility

33.88% face budget constraints

31.15% say tools are too complex to deploy or maintain

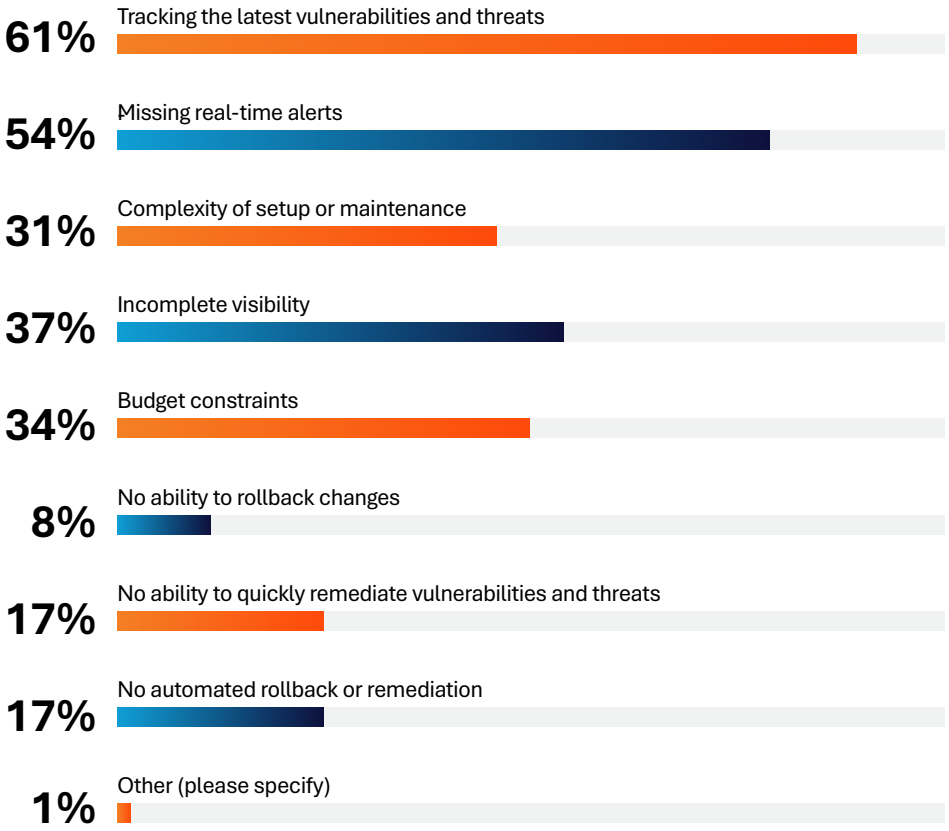
Takeaway: *Organizations face critical gaps in real-time alerting and visibility, compounded by tools that are often too complex and costly to deploy and maintain.*

3. The most challenging platforms to monitor for threats

When asked which platforms were the most challenging to monitor:

Takeaway: *Monitoring identity risks remains a challenge across core Microsoft platforms, with Active Directory and Entra ID leading the list, followed closely by Teams, Exchange Online, and Intune, highlighting the complexity of securing hybrid environments.*

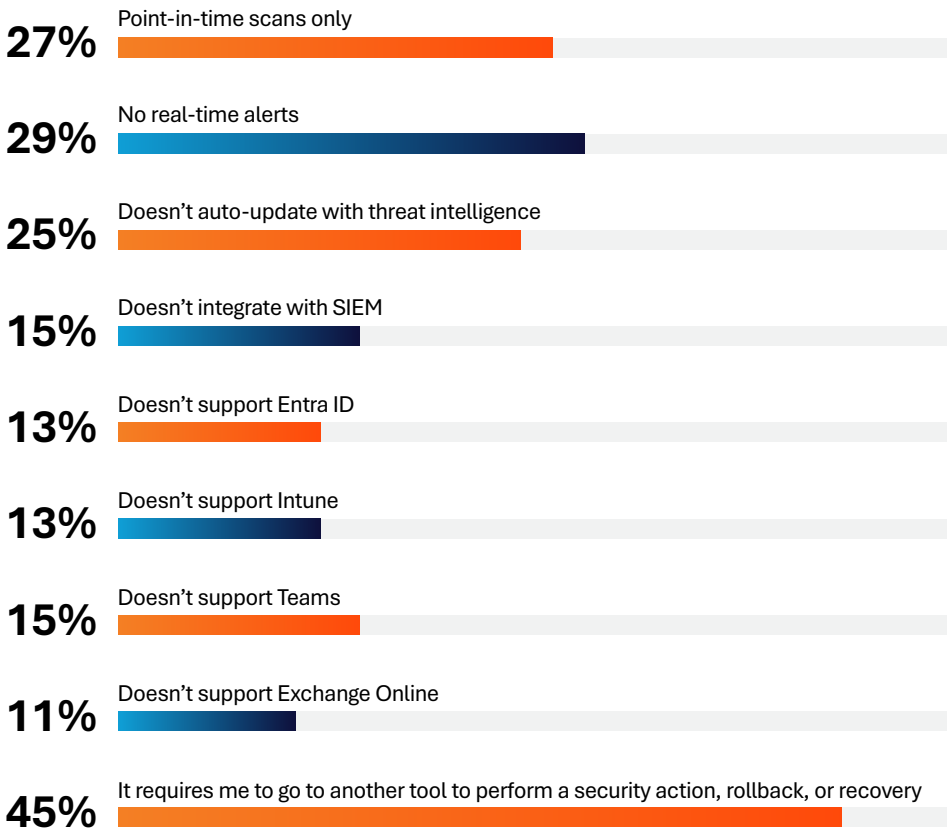
4. Top areas of concern when monitoring changes in their environment



Takeaway: *The biggest gaps in monitoring changes are tracking new vulnerabilities (60.66%) and missing real-time alerts (53.55%). Incomplete visibility (36.61%) and complexity of setup or maintenance (31.15%) add to the challenge, while budget constraints (33.88%) remain a significant barrier.*

Additional insights

What are the limitations within your current identity security infrastructure tool set?



Top limitations reported:

- **45.36%** must use other tools to remediate or roll back changes
- **28.96%** have no real-time alerts
- **27.32%** rely on point-in-time scans only
- **25.14%** lack automated threat intelligence updates
- **15%+** say their tools don't support Entra ID, Intune, or Teams

Takeaway: *These findings suggest that many organizations continue to manage hybrid identity environments with fragmented or reactive solutions. The data underscores the need for unified tools that deliver real-time visibility, automated intelligence updates, and built-in remediation capabilities across the entire Microsoft identity ecosystem.*

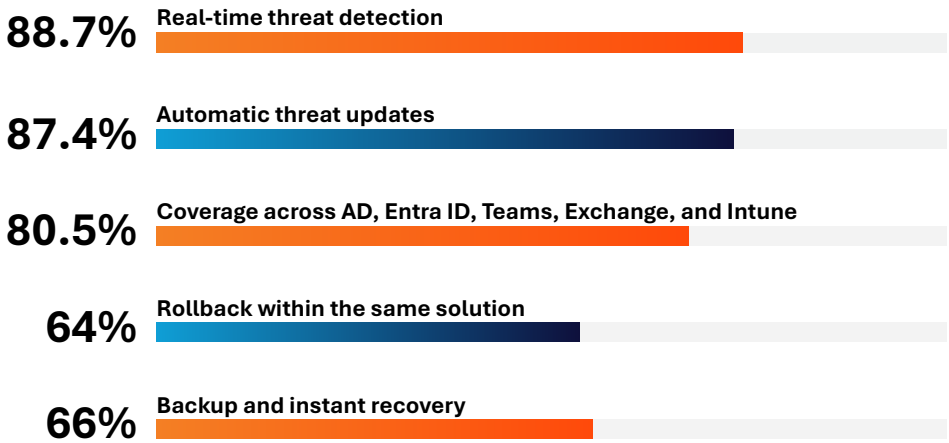
What tools are in use and what's missing

Tool Type	In Use	Real-Time Alerts	Auto Updates w/ Threat Intel
Microsoft Native Tools	90%	25%	14%
Purple Knight	53%	26%	35%
PingCastle	48%	42%	29%
SIEM (e.g., Sentinel, Splunk)	76%	65%	37%
Commercial Identity Security Tools	68%	56%	38%

Takeaway: *Most respondents use Microsoft native tools, but only a fraction provide real-time alerts or threat intel updates. Even advanced tools show gaps, and free scanners offer reports, not protection—highlighting the need for continuous, automated monitoring.*

The importance of capabilities within Microsoft identity tools

Survey respondents ranked the following capabilities as *"very important":*



Takeaway: *Respondents ranked real-time threat detection (88.7%) and automatic updates (87.4%) highest, but also placed strong importance on coverage across AD, Entra ID, Teams, Exchange, and Intune (80.5%). This signals a need for unified solutions that protect the entire Microsoft ecosystem, combining detection, automation, and resilience in one platform.*

Analysis: Where free scanners are falling short

As the respondents shared, most organizations rely on free tools to gauge posture, but these tools fall short when it comes to active protection. Point-in-time scanners produce static scorecards, but lack:

- Continuous detection
- Real-time alerting
- Coss-platform visibility

As hybrid identity environments grow in complexity, these limitations leave teams exposed between scans. Modern IT and security operations require always-on visibility, automated intelligence, and rapid remediation capabilities beyond what static assessment tools are providing.

Conclusion: A call for continuous protection

The Petri survey exposes widespread monitoring and detection deficits across hybrid Microsoft environments.

Administrators and security leaders understand the risks but often lack solutions that go beyond scanning and provide real-time threat detection and continuous monitoring to protect modern identity systems.

The way forward: Always on. Always ready.

Effective hybrid identity protection requires

- **Real-Time Threat Detection:** Immediate identification of privilege escalations, policy tampering, and risky account activity.
- **Continuous Change Monitoring:** Full context for every change—who made it, where, and when.
- **Comprehensive Coverage:** Visibility across AD, Entra ID, and Microsoft 365 services.
- **Automatic Threat Intelligence Updates:** Up-to-date detection without manual intervention.

Modern identity defense isn't about periodic scans—it's about continuous protection, complete visibility, and immediate response.

Introducing
Cayosoft Guardian Protector

Recognizing the gaps and challenges IT teams face when relying on free identity monitoring tools, Cayosoft developed Guardian Protector, an always-on solution designed for the IT community.

The tool delivers real-time threat detection and monitoring across hybrid Microsoft environments, empowering organizations with continuous protection and complete visibility without added cost. IT teams can download it free here: Cayosoft Guardian Protector.