RAPIDFIRE TOOLS
A Kaseya COMPANY

NAVIGATING THE FUTURE:

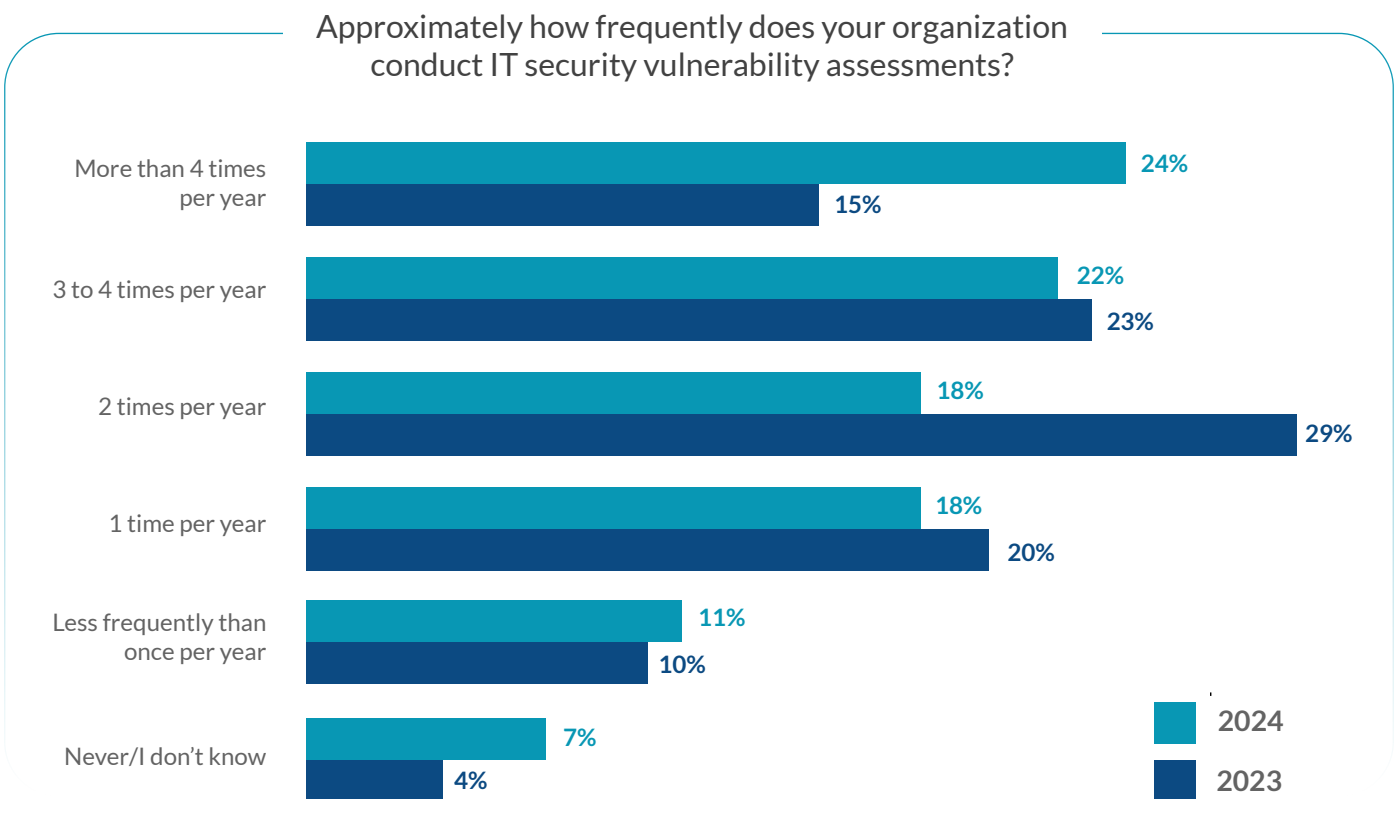
Key IT Vulnerability Management Trends

As the cybersecurity landscape continues to evolve, staying proactive about vulnerabilities has become a critical priority for managed service providers (MSPs) and IT teams. Recent trends show that organizations are increasingly prioritizing more frequent IT security vulnerability assessments to identify and address potential security flaws.

Staying informed on these trends can help MSPs and IT teams remain one step ahead of potential cyber-risks. **The Kaseya Cybersecurity Survey Report 2024** navigates this new frontier of cyber challenges. The data is clear: Organizations are becoming increasingly reliant on vulnerability assessments and plan to prioritize these investments in 2025.

Companies are increasing the frequency of vulnerability assessments

In 2024, 24% of respondents said they conduct vulnerability assessments more than four times per year, up from 15% in 2023. This shift highlights a growing recognition of the need for continuous monitoring and quick response to emerging threats. Meanwhile, biannual assessments are becoming less common, with the percentage of organizations conducting them dropping from 29% to 18%. The trend toward more frequent vulnerability assessments signals a collective move toward a stronger, more resilient security posture.



One-quarter of respondents conduct vulnerability assessments more than four times per year.

How often you should run vulnerability scans depends on a number of factors, including the risk level of your environment and compliance requirements:

- High-risk areas, such as public-facing applications and critical infrastructure, may need daily or weekly scans. Less critical systems can be scanned monthly or quarterly.
- Some compliance regulations, like the Payment Card Industry (PCI DSS), require vulnerability scans to be performed at least once every three months.
- Major changes to infrastructure, such as new cloud accounts, network changes or large structural changes to web applications, may require more frequent scans.

Continuous scanning is becoming more popular because it provides 24/7 monitoring of your IT environment. It can also help reduce the time to find and fix vulnerabilities.

When choosing a vulnerability scanning frequency, it's important to consider the pace of technology and the need to close cybersecurity gaps before attackers exploit them.

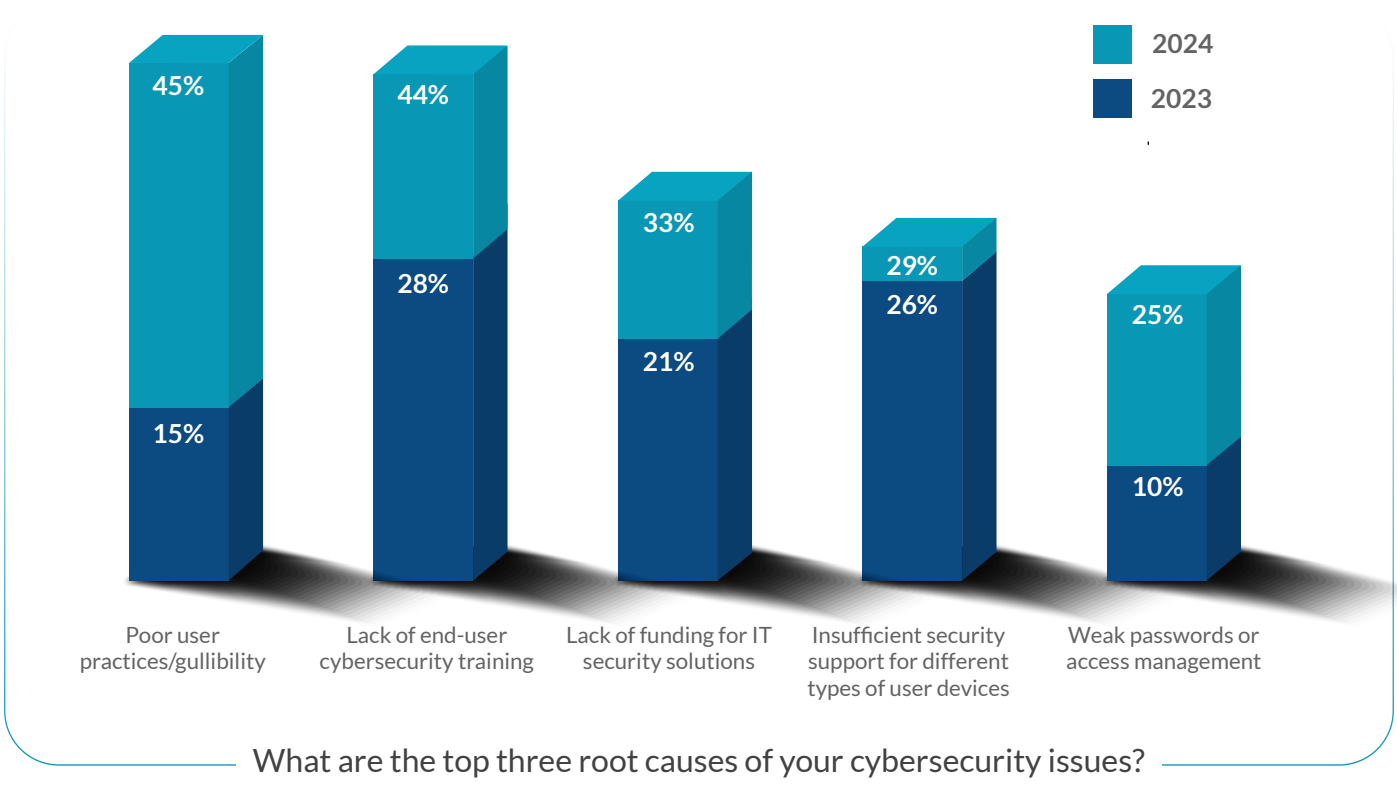
The top cause of cybersecurity issues is people

User-related security issues are a significant concern for IT professionals. Organizations citing a lack of end-user or cybersecurity training as a root cause increased from 28% in 2023 to 44% in 2024. Additionally, nearly half of respondents identified poor user practices or gullibility as a major problem, tripling from 15% to 45%.

Poor user behavior can lead to cybersecurity vulnerabilities in many ways. After compromising a user's login credentials, cybercriminals can gain unauthorized access to an organization's network.

This contributes to anywhere from 60% to almost 80% of cybersecurity breaches.

IT professionals clearly view users as a key factor in cybersecurity challenges, making it even more important for organizations to take proactive measures, like vulnerability assessments and training, to close security gaps and reduce risks to minimize human-centered trouble.

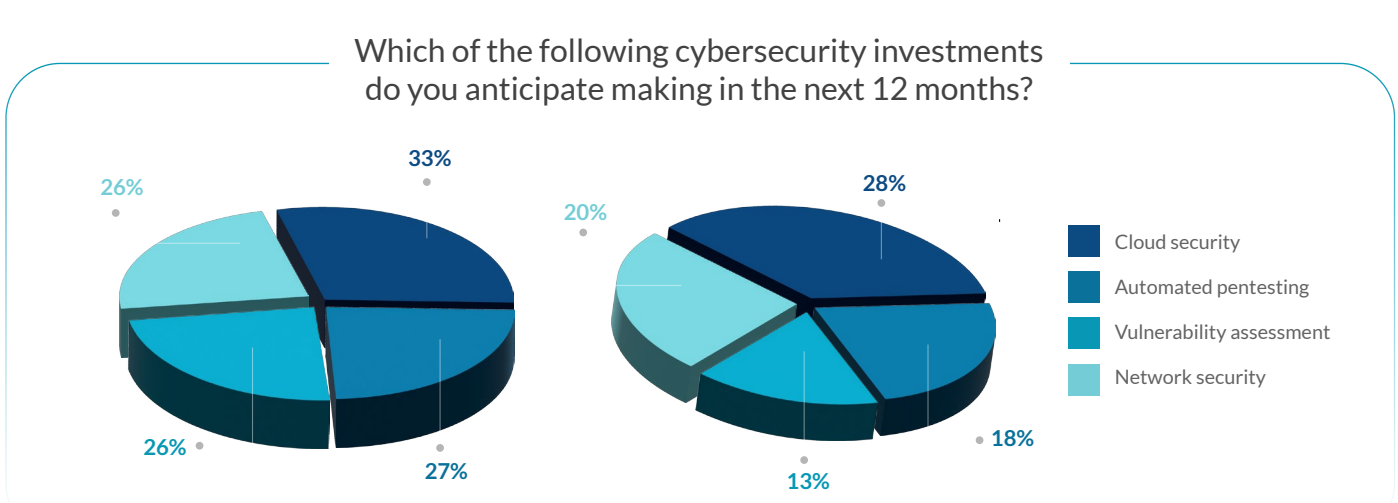


What are the top three root causes of your cybersecurity issues?

Nearly 9 in 10 respondents named a lack of training or bad user behavior as one of the biggest causes of cybersecurity challenges.

Vulnerability management is a high priority for cybersecurity investment

As security maturity levels off for many businesses, there's an increased focus on proactive cybersecurity measures. Interest in investment in vulnerability assessment **doubled from 13% in 2023 to 26% in 2024**. This trend coincides with growing investments in cloud security (33%), automated pentesting (27%) and network security (26%), highlighting the critical need to identify and address vulnerabilities quickly in a fast-moving threat landscape.



Vulnerability assessment is on the cybersecurity investment shortlist for 2025.

Vulnerability assessments are key to minimizing incident costs

Businesses are seeing that their security investments are paying off, with a trend toward lower-cost cybersecurity incidents in 2024. Proactive measures like vulnerability assessments can significantly reduce incident costs and enhance cybersecurity resilience.

Fast and Effective Vulnerability Management with VulScan

VulScan is a comprehensive solution that identifies and prioritizes internal and external vulnerabilities in the networks you manage. It simplifies scheduling scans and filtering results for effective vulnerability management. Intuitive dashboards and reports facilitate quick identification of critical vulnerabilities to address before they can be exploited. Additionally, setting up unlimited network scanners and accessing scan results through the web management portal is quick and easy.

VULSCAN FEATURES

- Local and remote internal vulnerability management
- Local and hosted external vulnerability scanning
- Multi-tenant management dashboard
- Vulnerability noise management
- Automatic service ticket creation
- Ability to scan by IP address, domain name or hostname

Schedule a demo today