Cybersecurity
INSIDERS

2023

State of Vulnerability Management

KEY INSIGHTS & STRATEGIES

SYXSENSE®

Introduction

Managing cybersecurity vulnerabilities is a significant challenge for most organizations. Unaddressed vulnerabilities open doors to cyber threats, while the sheer volume of potential risks can make it difficult to prioritize remediation tasks effectively. Rapid technology advancements and ever increasing attack surfaces often outpace organizations' abilities to stay ahead of emerging threats.

This survey was designed to shed light on current practices, obstacles, and perspectives in vulnerability management. Through understanding how organizations are tackling these challenges, the "2023 State of Vulnerability Management" report offers strategic insights and industry benchmarks.

KEY FINDINGS FROM THE SURVEY INCLUDE:

- **Real-World Impact:** Nearly a quarter of the organizations surveyed (24%) reported experiencing a breach due to unaddressed vulnerabilities, revealing the real-world implications of neglected vulnerabilities.
- **Preventive Measures:** Though the majority of organizations (85%) use network vulnerability scans, the application of other preventive measures varies. Only 65% prioritize vulnerabilities based on risk.
- **Visibility and Detection:** Half of organizations (51%) have, at best, only a moderate level of visibility into vulnerabilities and 26% detect more than 100 new vulnerabilities every month. This underlines the sheer volume of potential risks organizations contend with, necessitating efficient vulnerability management strategies.
- **Vulnerability Scanning and Patching Speed:** While continuous vulnerability scanning is employed by 35% of respondents, there remains a considerable lag in patch deployment. Surprisingly, only 11% manage to deploy patches on the same day they become available, with a significant 47% taking more than a week. This gap creates a significant risk window, during which organizations remain susceptible to exploited vulnerabilities.
- **Scope of Vulnerability Scanning:** The survey results show a contrast between what organizations currently scan and where they perceive the need for more comprehensive vulnerability management. Servers (91%) and desktops/laptops/endpoints (80%) are the most scanned assets. However, respondents expressed a need for improved vulnerability management in areas like IoT/OT devices (49%) and cloud assets (44%).
- **Maturity of Approach:** It's worth noting that only 19% of organizations have achieved a high-level maturity in their vulnerability management program, suggesting substantial room for industry-wide improvement.
- **Barriers to Improvement:** The majority of organizations identified budget constraints (56%) and skill shortages (46%) as the most substantial barriers to improved vulnerability management, revealing the increasing demand for innovative solutions and automation to help existing staff do more with less.
- **Solution Priorities:** When evaluating vulnerability management solutions, the survey participants placed the highest importance on the accuracy of vulnerability detection (79%), followed closely by reporting and analytics capabilities (63%) and the cost of ownership (61%).

We'd like to extend our gratitude to Syxsense for the support in conducting this important research. Syxsense is a leading provider of unified security and endpoint management solutions, bridging the gap between patch and vulnerability scanning and automated remediation, and their expertise has been invaluable in our analysis.

The insights derived from this survey will serve as a guidepost for organizations striving to bolster their cybersecurity posture through more robust vulnerability management. We hope you find this new report not only informative, but also an effective tool in your mission to protecting your organization's IT environment.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

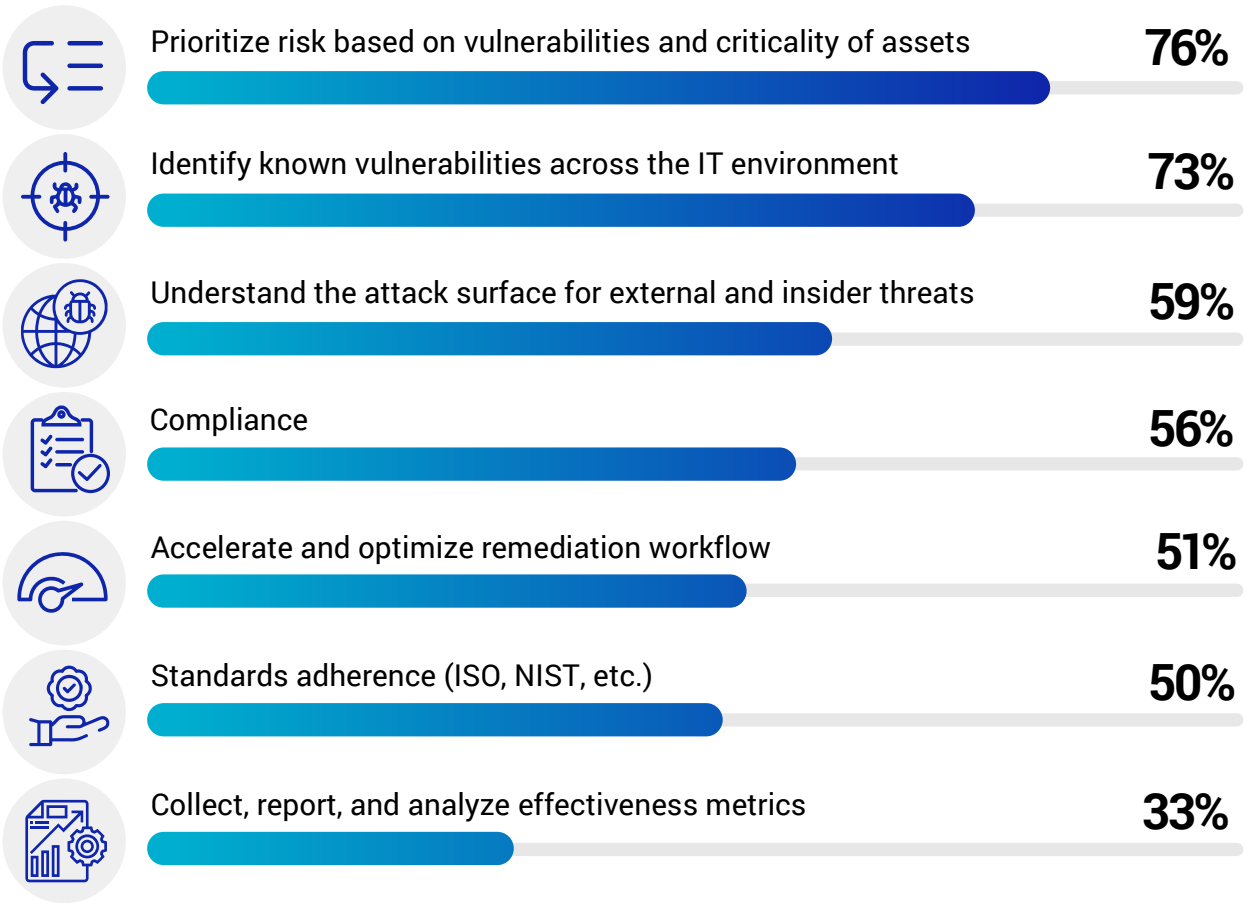
Key Objectives

Understanding the objectives of an organization's vulnerability management program is essential, as it helps in shaping the cybersecurity posture and strategy.

The survey results highlight that most organizations (76%) prioritize risk based on vulnerabilities and the criticality of assets, while nearly as many (73%) aim to identify known vulnerabilities across their IT environment. More than half the organizations (59%) focus on understanding the attack surface for both external and insider threats, and work on optimizing the remediation workflow to minimize the risk of a breach (51%). Compliance is also a key objective for 56% of organizations, along with standards adherence for 50% of the survey participants.

Organizations should consider aligning their objectives with risk-based vulnerability management, a technique that assesses vulnerabilities in the context of their breadth across the enterprise and evaluates their potential impact. With risk-based vulnerability management, organizations can understand what their environment looks like in real time. Automation solutions can assist with this, offering features that help prioritize vulnerabilities based on risk and optimize the remediation workflow. This approach will ensure the most critical threats are addressed promptly, thereby minimizing potential breaches and enhancing security.

What are the key objectives for your organization's vulnerability management program?

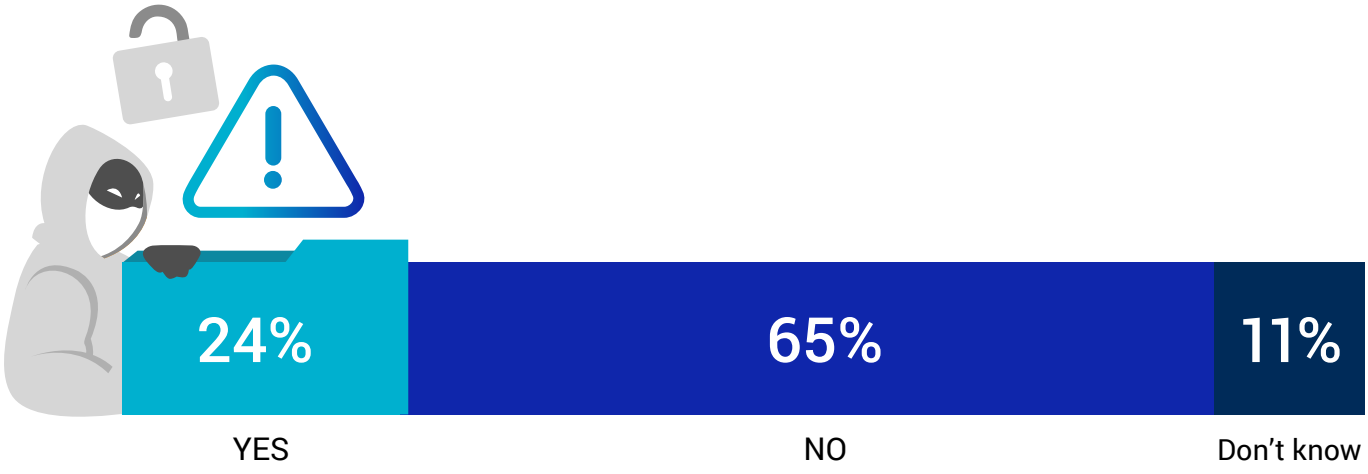


Breaches Due to Unaddressed Vulnerabilities

Recognizing and addressing vulnerabilities is critical to an organization's cybersecurity stance. Past breaches due to unaddressed vulnerabilities signify gaps in the vulnerability management process. Nearly a quarter of organizations (24%) reported that they have suffered a breach due to an unaddressed vulnerability. This highlights a significant oversight in the industry, particularly considering that many of these vulnerabilities could have been preemptively identified and remediated. Further, the 11% who don't know if this has occurred suggests a lack of transparency and visibility in their breach history.

Organizations should take this as a wake-up call to strengthen their vulnerability management efforts. Continuous and automated monitoring and patch management are essential to prevent such breaches. This proactive approach allows teams to remediate vulnerabilities before they can be exploited, dramatically reducing the risk of a breach.

Has your organization been breached in the past as a result of a vulnerability that was not addressed?

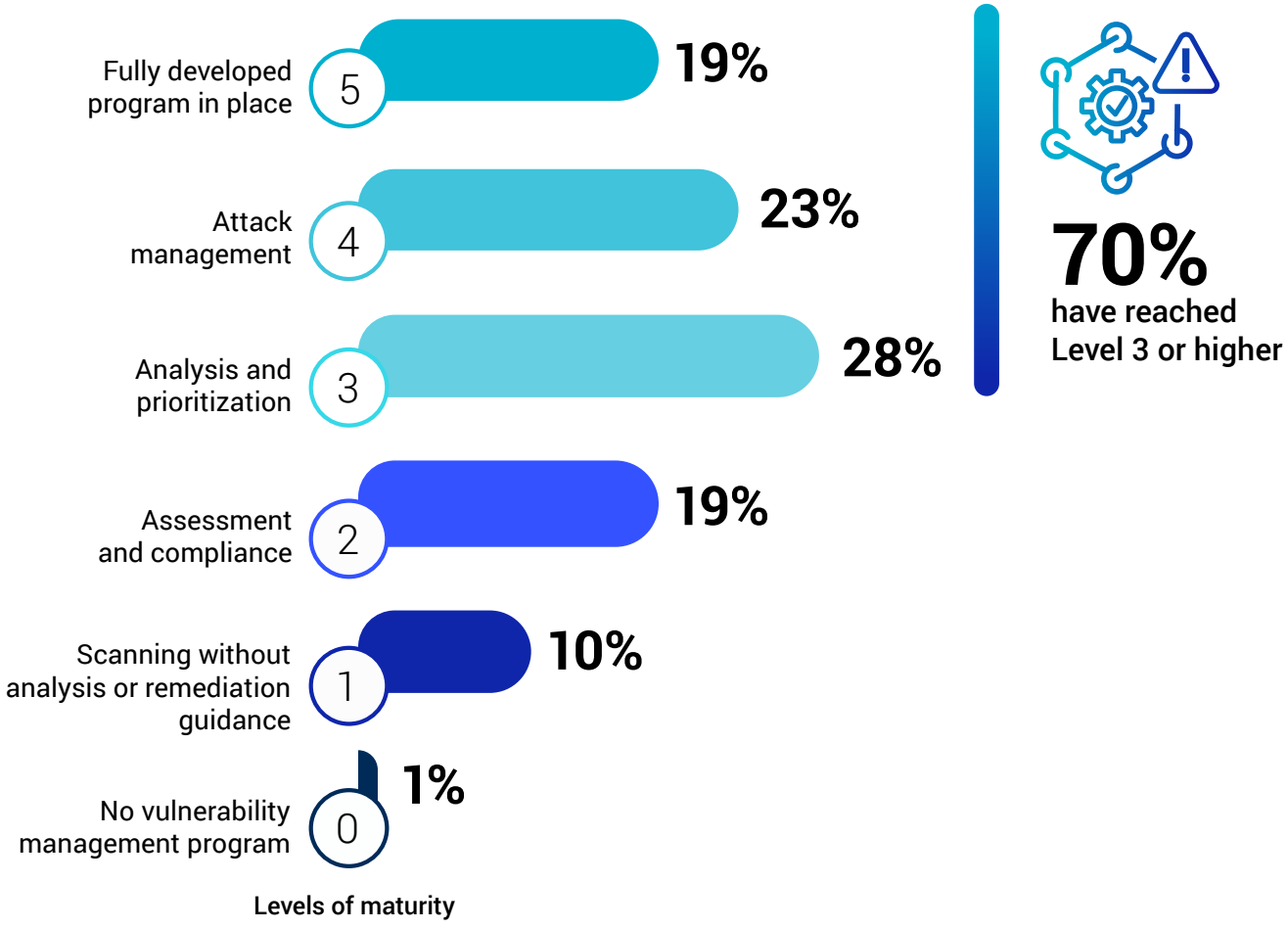


Vulnerability Management Maturity

Understanding the maturity of an organization's vulnerability management program is critical, as it provides a benchmark on how well the organization is equipped to identify, assess, and address vulnerabilities in its systems. Most respondents (70%) self-categorized their vulnerability management program as being at Level 3 or higher. This reflects an ability to analyze and prioritize vulnerabilities based on the specific risk to their IT environments (Level 3: 28%), perform scan and penetration testing (Level 4: 23%), and fully develop vulnerability management programs (Level 5: 19%). Very few organizations in our survey reported having no program in place (1%).

Based on these findings, organizations should prioritize advancing their vulnerability management maturity. Those at lower levels should aim for a structured strategy with regular assessments (Level 2) as a minimum. This process could be supported with the integration of advanced vulnerability management solutions to provide comprehensive scanning, analysis, and remediation guidance for vulnerabilities. Those at higher levels should continue refining their strategies to better identify vulnerability trends and utilize enhanced remediation techniques (Level 5).

How would you characterize the level of maturity your vulnerability management program has reached? (Select one, from 0 = none to 5 = high level)



Vulnerability Management Components

The use of advanced techniques in vulnerability management enables organizations to adopt a holistic approach to detecting and managing vulnerabilities, thereby securing their systems more effectively.

Network Vulnerability Scans (85%) and Penetration Testing (76%) are the most widely employed components, reflecting the essential role these techniques play in the identification of vulnerabilities. Despite the high uptake of these methods, it's concerning that more advanced and targeted measures like Adversary Simulation (21%) and Breach and Attack Simulation (34%) are less used.

To enhance their security posture, organizations should look to employ a wider array of techniques in their vulnerability management program, including newer technologies like simulated attack scenarios, as well as a vulnerability scanning tool that offers risk-based vulnerability prioritization or a solution that supports automated remediation. This will lead to a more comprehensive and effective vulnerability management strategy.

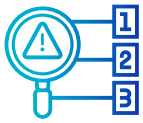
Which components of vulnerability management are you employing today?

85%

Network Vulnerability Scans

76%

Penetration Testing



65%

Vulnerability Prioritization

62%

Web Application Scanning

61%

Threat Intelligence

60%

Web Application Penetration Testing

Static Application Security Testing 48% | Breach and Attack Simulation 34% | Dynamic Application Security Testing 32% | Adversary Simulation 21% | Other 1%

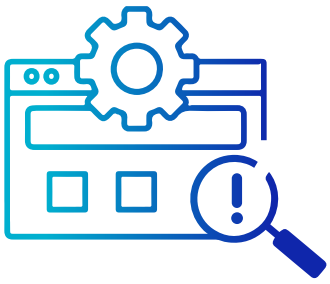
Frequency of Vulnerability Scans

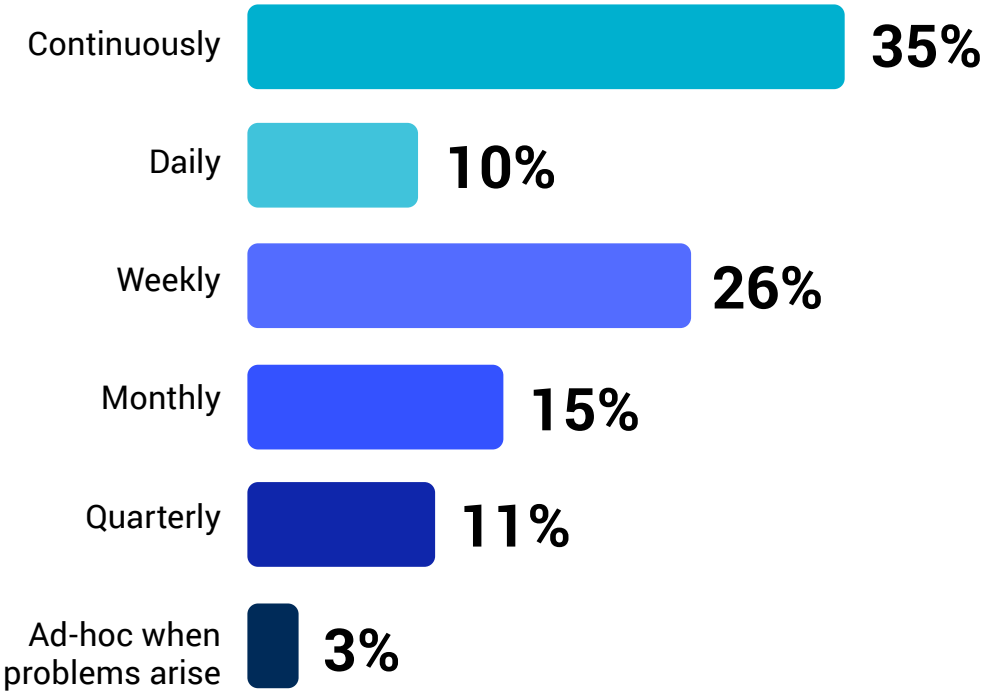
Regular vulnerability scanning is crucial to staying up-to-date with evolving cyber threats and patching any new weaknesses before they can be exploited.

Although the majority of respondents are conducting vulnerability scans continuously (35%), daily (10%), or weekly (26%), a surprising number of organizations are only scanning on a monthly (15%) or quarterly basis (11%), leaving long periods of potential exposure to cyber threats.

Organizations should aim to conduct vulnerability scans as frequently as possible, ideally continuously. This would allow them to identify and address new vulnerabilities in a timely manner. Leveraging automated solutions can help streamline this process and provide continuous, real-time visibility of vulnerabilities.

How often does your organization perform vulnerability scans?





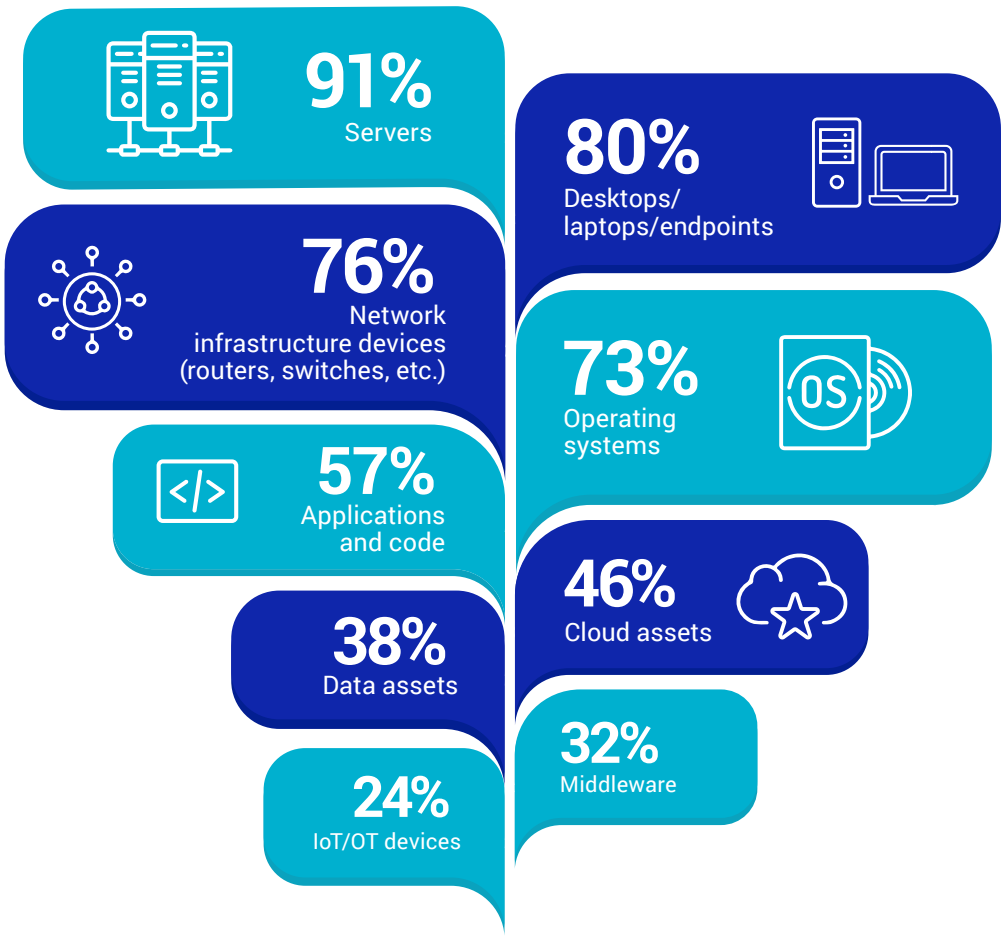
Scanning Across IT Environments

Expanding vulnerability scanning across all aspects of the IT environment is critical, as hackers can (and will) exploit weaknesses in any part of the network infrastructure.

It's reassuring to see a high percentage of organizations scanning servers (91%), desktops/laptops/endpoints (80%), and network infrastructure devices (76%). However, vulnerable areas such as IoT/OT devices (24%), middleware (32%), and data assets (38%) are being overlooked by a significant number of respondents. This is concerning as these components can be key entry points for attackers.

With the rise of remote work and hybrid environments, vulnerability management must include cloud assets, geographically dispersed devices, and often overlooked areas like IoT/OT devices. Comprehensive vulnerability management solutions can help ensure no part of the IT environment is left unguarded.

What parts of the IT environment do you typically scan for vulnerabilities?



Identifying Infrastructure Vulnerabilities

Recognizing areas in an organization's IT infrastructure that require enhanced vulnerability management is key in strengthening defenses against cyber threats. To start, enhanced visibility into an organization's infrastructure can highlight areas of improvement, helping security teams understand where to focus on reducing and mitigating risks.

Most respondents identified IoT/OT devices (49%) and cloud assets (44%) as areas needing better vulnerability management, which aligns with emerging cybersecurity trends and the previous survey question where these areas were less frequently scanned. Applications and code (41%) and network infrastructure devices (38%) are also a concern for many organizations.

Organizations should prioritize securing these areas with better vulnerability management, with a special focus on IoT/OT devices and cloud assets due to their rising relevance in modern IT environments.

Which areas of your infrastructure do you think need better/more vulnerability management?

49%
IoT/OT devices

44%
Cloud assets

41%
Applications and code

38%
Network infrastructure devices

37%
Desktops/laptops/ endpoints

32%
Servers

28%
Data assets

23%
Middleware

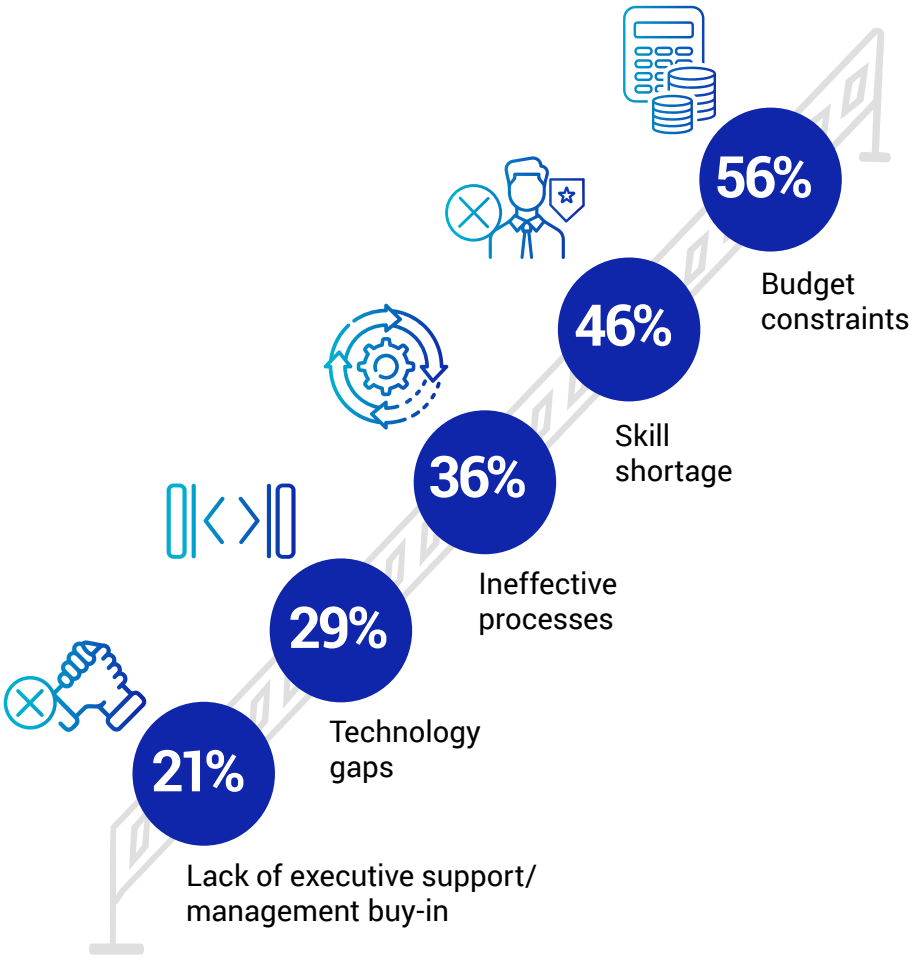
21%
Operating systems

Organizational Barriers to Vulnerability Management

When asked what barriers are holding back better vulnerability management in their organization, a majority of the respondents (56%) identified budget constraints as the leading barrier. This finding is consistent with the common challenge of IT security not being seen as a revenue-generating function, and is thus often underfunded. A skill shortage, reported by 46% of the respondents, underscores the ongoing challenge of cybersecurity talent scarcity. Ineffective processes and technology gaps, cited by 36% and 29% respectively, point at the complexities in dealing with the evolving landscape of cybersecurity threats.

Given these findings, organizations should explore comprehensive, unified solutions that combine capabilities from patch management to vulnerability management, making products more cost-effective and enabling IT and security teams at all skill levels to quickly and efficiently remediate findings. Moreover, executive education on the importance of cybersecurity and better alignment of security goals with business objectives can improve management buy-in, making vulnerability management a strategic priority rather than a sidelined function. Training and upskilling current staff, along with automating processes, could also help overcome skill shortages and process inefficiencies.

In your organization, what are the biggest barriers to better vulnerability management?



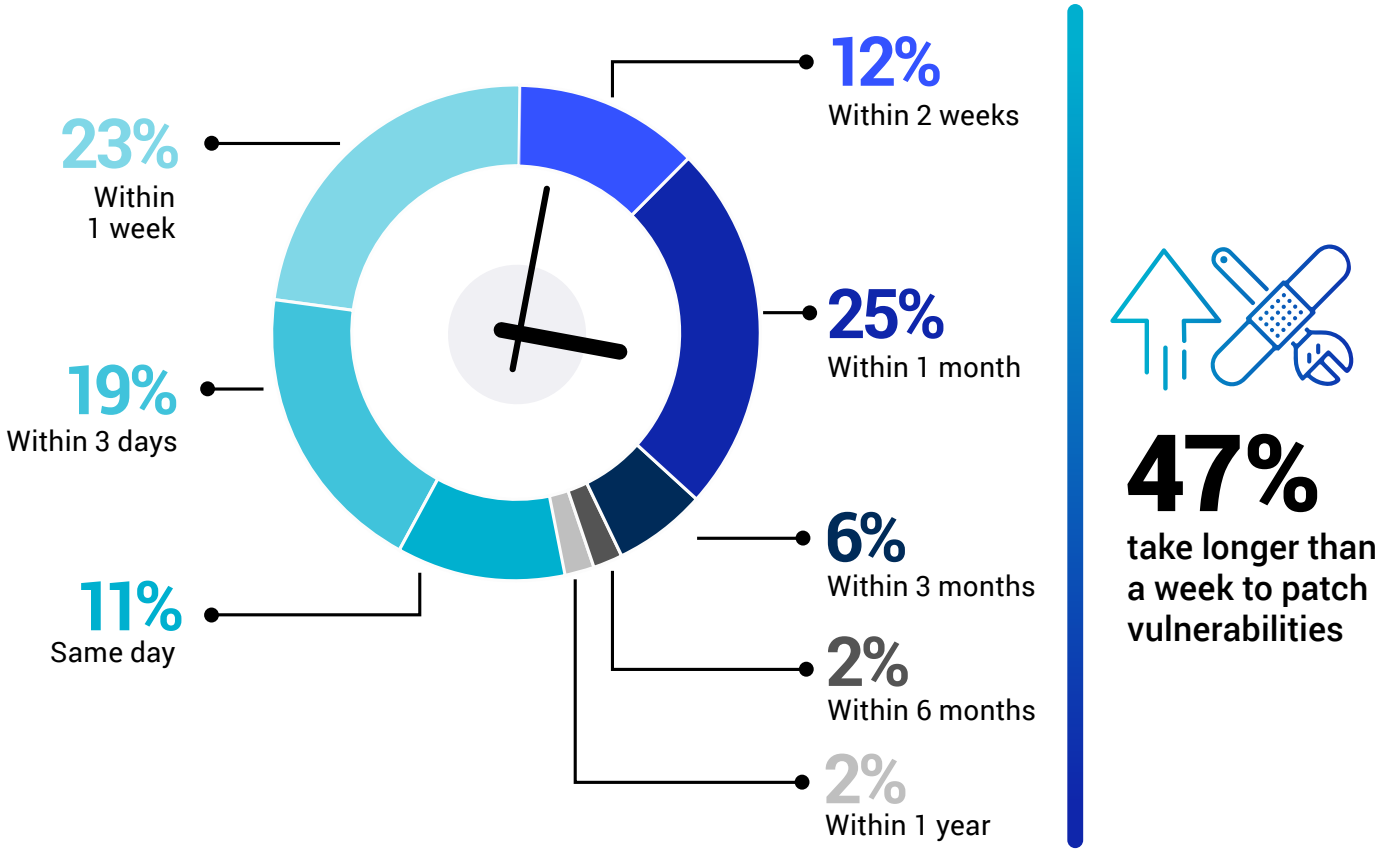
Patch Deployment Speed

The time it takes to deploy available security patches in an environment is a critical determinant of an organization's susceptibility to vulnerabilities — the quicker the patches are deployed, the smaller the window of opportunity for a cybercriminal to exploit any known vulnerabilities.

Only a small fraction of organizations (11%) manage to deploy patches on the same day they become available. 19% of organizations patch within 3 days, and 23% within a week. An alarming 47% take longer than a week. It's particularly concerning that a combined 10% take much longer than a month to patch known vulnerabilities, as delays in patch management can greatly increase an organization's risk of a security breach.

To minimize their vulnerability window, organizations should aim to significantly shorten their patch deployment timeframes. Implementing an automated patch management system can significantly reduce the time and effort required to deploy patches by streamlining the process and eliminating the manual aspects of patch deployment, especially in times of IT and cybersecurity talent shortages. Regularly monitoring the patch deployment timeframes can also help in identifying and addressing any bottlenecks in the process. Organizations should also review how they can speed up their time-to-patch by using real-time connections to endpoints to gather current device status and gain more accurate insight into which endpoints need which patches.

Once available, on average, how long does it take to deploy a security patch in your environment?



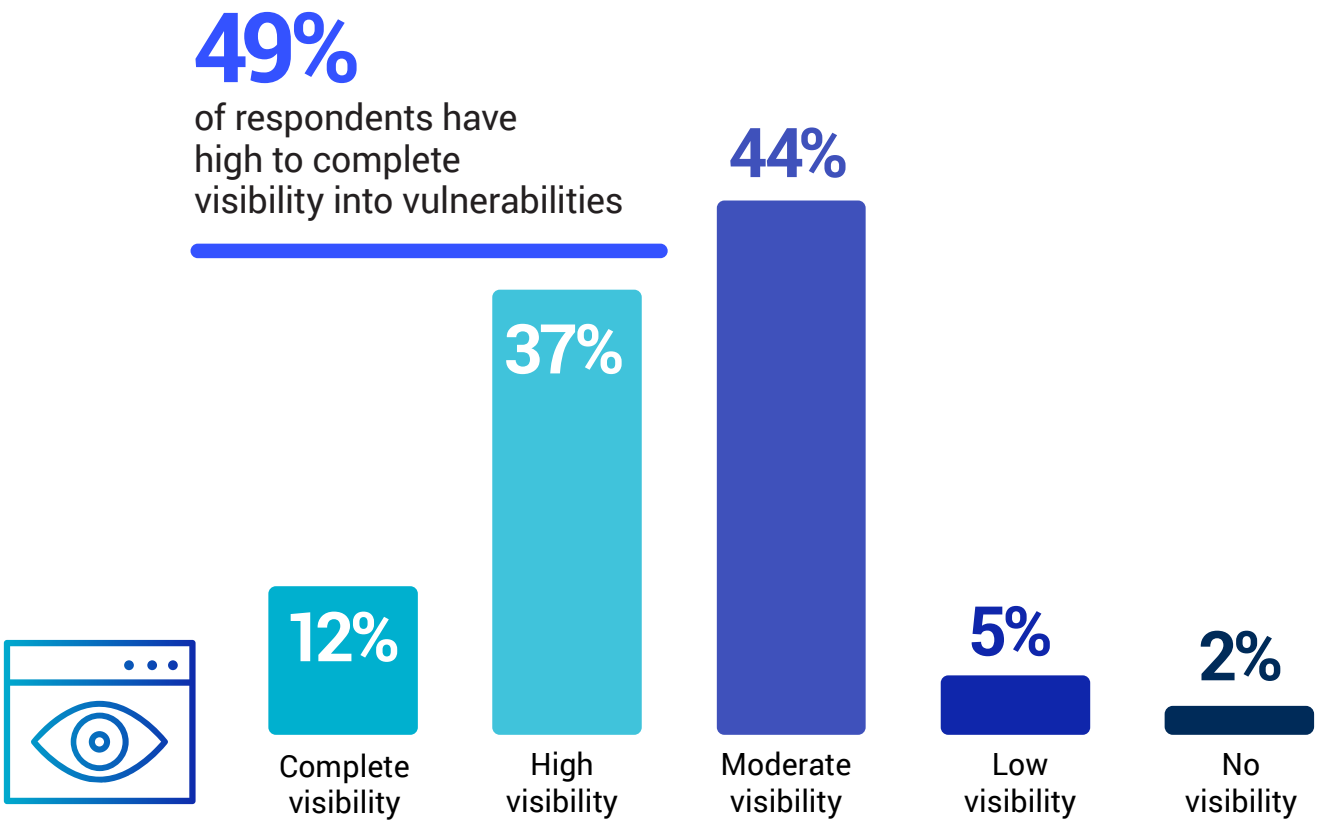
Visibility Into Vulnerabilities

Visibility into vulnerabilities across an IT environment is fundamental to effective vulnerability management. It forms the basis for identifying, assessing, and prioritizing vulnerabilities, and guides decision-making on remediation activities.

Looking at the survey results, about half of the respondents (49%) have high to complete visibility into vulnerabilities across their IT environment, while the other half (51%) have, at best, only a moderate level of visibility. This is concerning, as lack of visibility can lead to unaddressed vulnerabilities and subsequent breaches.

To increase visibility across their IT environment, organizations should consider implementing comprehensive vulnerability management solutions to provide continuous monitoring and scanning capabilities, alongside detailed reporting, to ensure that no known vulnerabilities go unnoticed.

What level of visibility do you have into vulnerabilities across your IT environment?

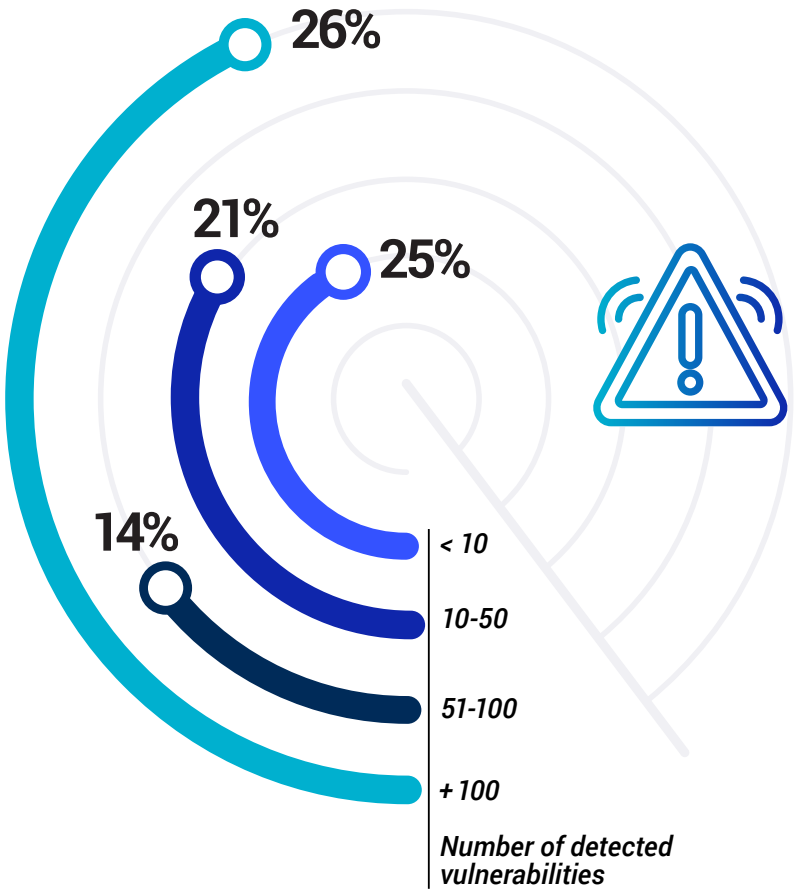


Vulnerability Volume

The frequency of detected vulnerabilities can give a rough indication of the attack surface of an organization and the efficiency of its vulnerability discovery processes. Looking at the survey, we see a fairly even distribution across the spectrum of vulnerability volumes. No organizations reported detecting no vulnerabilities, while a quarter (26%) find more than 100 per month, indicating a high level of risk. On the lower end, a quarter (25%) detect less than 10 vulnerabilities per month, and 21% detect between 10 and 50. Interestingly, a significant number (14%) are unsure about their monthly vulnerability volume, which may indicate a lack of proper tracking mechanisms or visibility.

Companies must aim to identify and reduce their detected vulnerabilities, a process that necessitates a clear understanding of the current state of the organization's environment at any given time. By gaining this visibility, security teams can implement robust vulnerability management processes and technologies, enabling continuous scanning and sophisticated analytics for the timely discovery and assessment of vulnerabilities. Businesses need to focus not merely on the number of vulnerabilities but also consider their severity and potential impact on business operations.

On average, how many vulnerabilities does your organization detect every month?



Don't know 14%

Vulnerability Trends

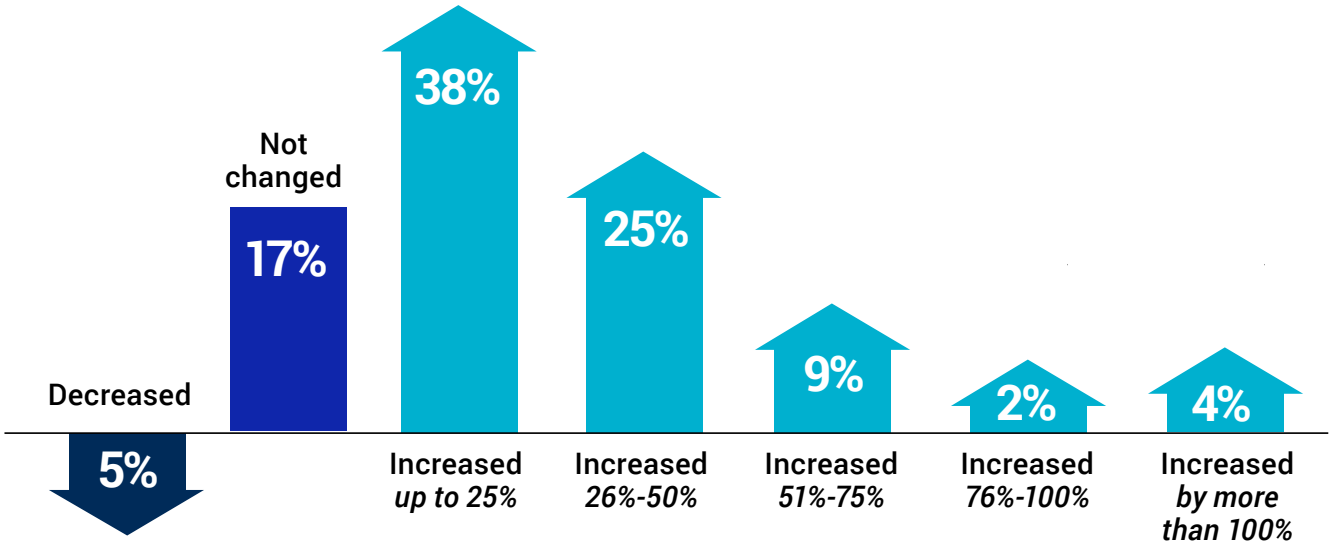
Recognizing the dynamics of vulnerability volume within an organization can provide insights into the effectiveness of existing cybersecurity measures and changes in the threat landscape. The majority of surveyed organizations (78%) reported an increase in vulnerability volume over the past 12 months, signaling a more challenging cybersecurity environment. Specifically, 38% of respondents have seen an increase of up to 25%, while 25% have experienced an increase of 26%-50%. At the higher end, 15% of organizations reported their vulnerability volume increased by 51% or more.

This data underscores the importance of staying ahead of emerging threats and continuously refining vulnerability management practices. Companies can leverage automation solutions to gain real-time visibility into emerging vulnerabilities and deploy relevant patches promptly. As vulnerability volumes increase, continuous monitoring, effective patch management, and a proactive approach to security are crucial.

How has the volume of security vulnerabilities changed over the past 12 months for your organization?

78%

of organizations reported an increase in the volume of security vulnerabilities during the past year



Vulnerability volume change

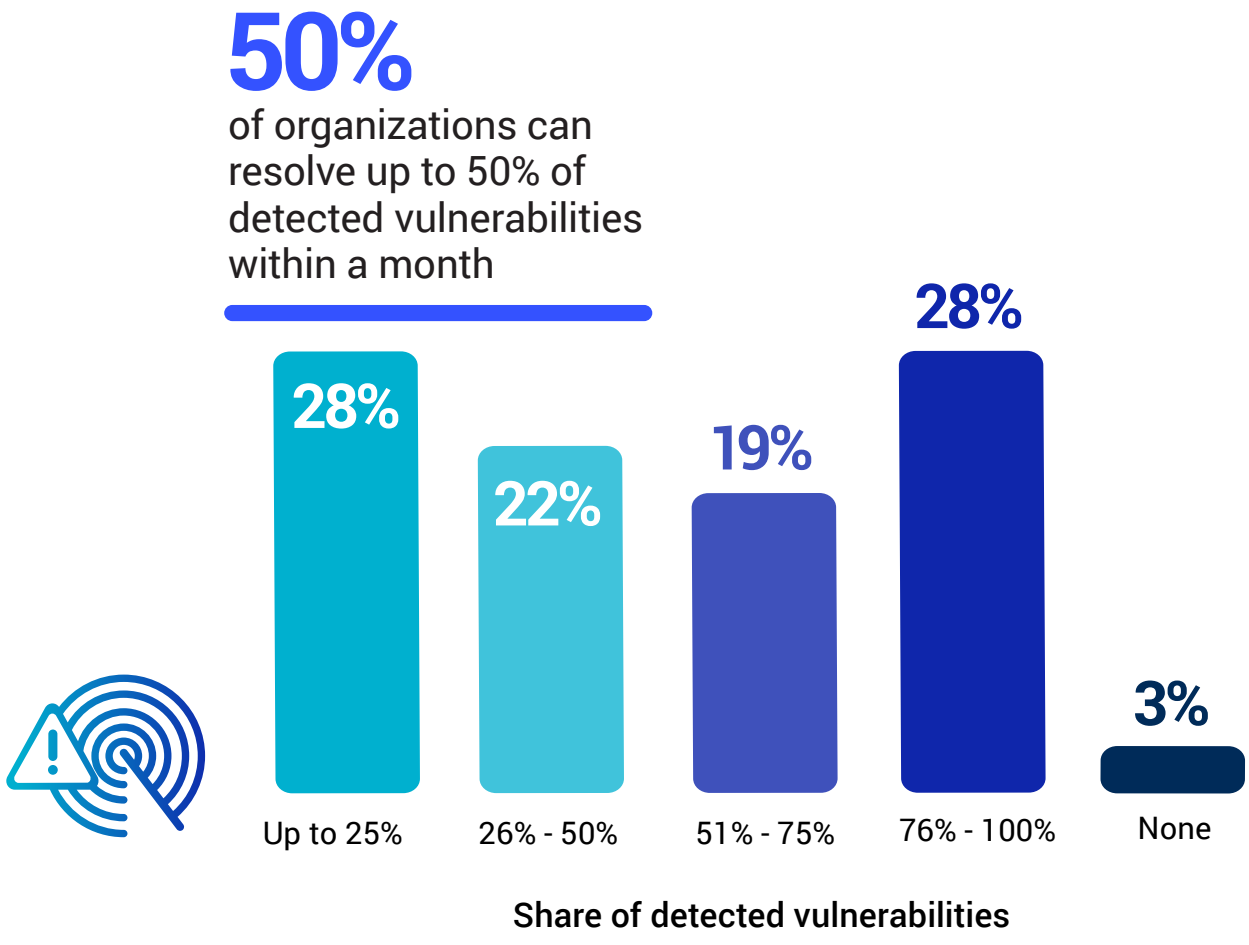
Vulnerability Resolution Rate

The rate at which an organization addresses identified vulnerabilities plays a key role in minimizing potential cyber threats and securing their IT environment.

The responses indicate a broad distribution in the rate of vulnerability resolution within a month of discovery. Half of all organizations (50%) can resolve up to 50% of detected vulnerabilities within a month. The other half resolves more than 50% of vulnerabilities within this time frame, with about a quarter of organizations (28%) solving more than 75% of all detected vulnerabilities.

These figures highlight the need for more efficient vulnerability management practices to promptly address potential security risks. Organizations should seek to raise their resolution rates to improve their security posture. Employing comprehensive vulnerability management solutions with automated patch management and real-time risk insights can greatly enhance an organization's ability to resolve vulnerabilities in a timely manner.

On average, what share of detected vulnerabilities does your organization resolve within a month?

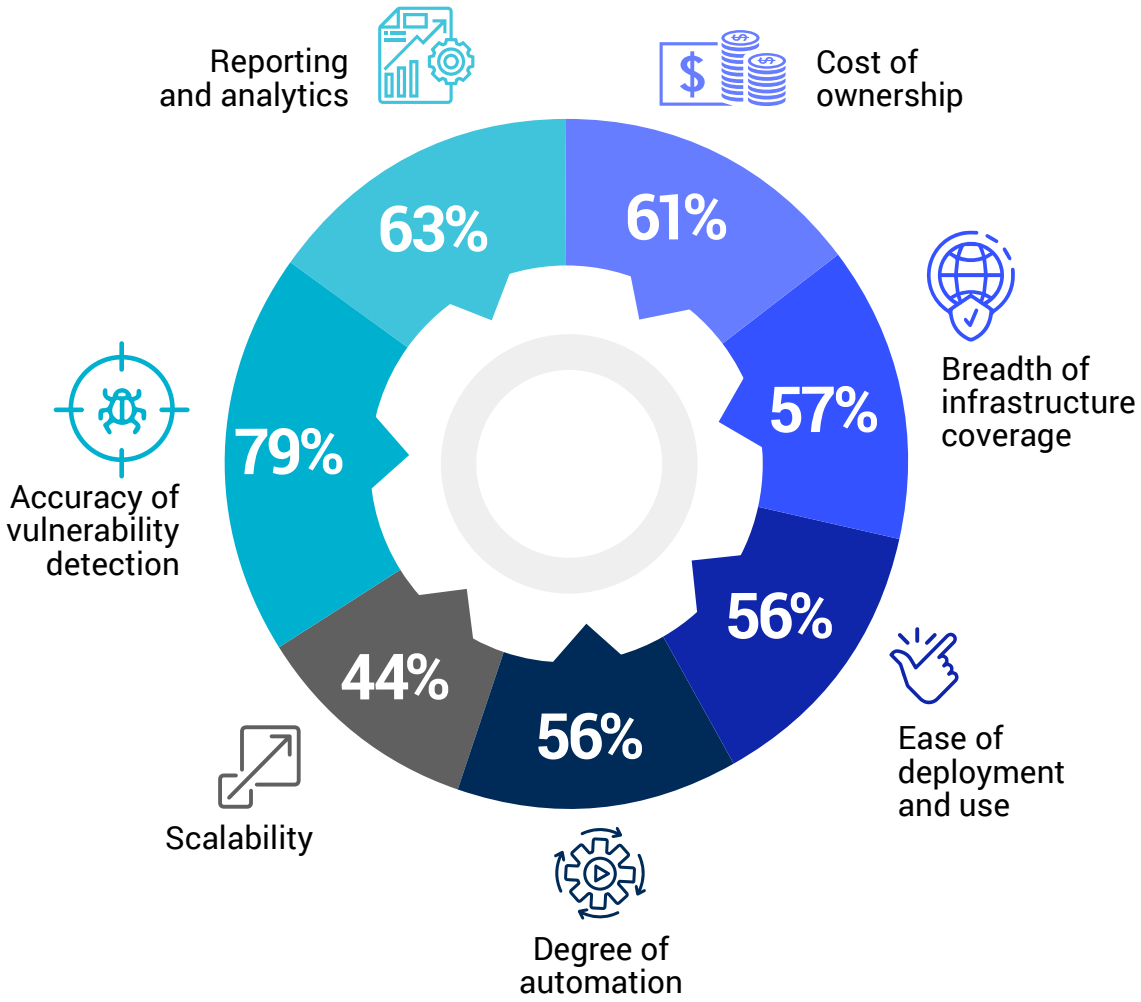


Solution Selection

The factors that guide an organization's choice when evaluating vulnerability management solutions can significantly impact the effectiveness of their cybersecurity strategies. From the survey results, the accuracy of vulnerability detection stands out as the most important criterion (79%). This is followed by reporting and analytics (63%) and cost of ownership (61%). About 57% also consider the breadth of infrastructure coverage, ease of deployment and use, and the degree of automation as crucial in their decision-making. Less than half (44%) place emphasis on scalability.

Given the high importance placed on the accuracy of vulnerability detection, organizations should look for solutions that deliver highly accurate and real-time vulnerability detection. Additionally, the solution should offer robust reporting and analytics capabilities to provide actionable insights for addressing identified vulnerabilities. Cost of ownership can be minimized by choosing solutions that also prioritize easy deployment and automation. The latter will ensure tasks can be performed with minimal manual intervention, thereby saving time and resources.

Which purchase criteria are most important to your organization when evaluating a vulnerability management solution?



Key Solution Features

Features and capabilities of a vulnerability management solution determine its efficacy in securing an organization's IT environment. The majority of respondents believe that vulnerability assessment (73%) is the most important feature, with vulnerability scanning (65%) and asset discovery (63%) also ranking high. This shows that respondents are focused on both identifying potential points of compromise and evaluating the risks they pose. Patch management is seen as important by 60% of respondents, emphasizing the significance of timely updates in managing vulnerabilities. Risk management and prioritization (58%), along with reporting and analytics (54%), were also deemed crucial by over half the respondents.

Organizations should aim for a comprehensive vulnerability management solution that encompasses these critical features. Regular vulnerability assessment and scanning will ensure prompt detection of weaknesses, while asset discovery will help keep an up-to-date inventory of devices that could potentially be exploited. Also, with risk management and prioritization, organizations can focus their efforts where it matters most. Effective patch management and detailed reporting and analytics will ensure efficient mitigation and provide valuable insights into the overall cybersecurity landscape.

Which vulnerability management solution features are most important to you?

73% Vulnerability assessment

65% Vulnerability scanning

63% Asset discovery

60% Patch management

58% Risk management and prioritization

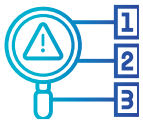
54% Reporting and analytics

51% Vulnerability intelligence

38% Configuration monitoring

Essential Practices for Robust Vulnerability Management

This guide outlines eight essential practices to strengthen your vulnerability management strategy and enhance your organization's cyber resilience.



Prioritize Vulnerability Management: Given that nearly a quarter of the surveyed organizations have suffered a breach due to an unaddressed vulnerability, it's critical to prioritize vulnerability management. It is important to implement solutions that aid in detecting and addressing vulnerabilities promptly, reducing the risk of a breach.

Regular Vulnerability Scanning: More than a third of organizations are scanning their systems continuously for vulnerabilities, with another quarter conducting weekly scans. Regular scanning is key to detecting new vulnerabilities as they arise.

Comprehensive Scanning of IT Environment: Vulnerabilities can exist anywhere within the IT infrastructure. Therefore, a robust vulnerability management approach should involve comprehensive scanning covering all assets - from desktops, network devices, and servers to cloud assets and IoT devices.

Build Mature Vulnerability Management Systems: As per the survey, organizations with higher levels of vulnerability management maturity were found to be more efficient in managing risks. Aim to build a vulnerability management program that not only assesses but also prioritizes vulnerabilities based on the specific risk they pose to your IT environment.

Prioritize Risk Remediation: Not all vulnerabilities pose the same risk. Prioritize remediation based on the severity of the vulnerabilities, the criticality of the assets, and the potential impact on the business. Consider platforms that can provide risk-based prioritization to aid in this process.

Implement Timely Patch Management: Over half of surveyed organizations are deploying security patches within a week of their availability. Implementing a robust patch management strategy can ensure that vulnerabilities are promptly addressed and the window of opportunity for attackers is minimized.

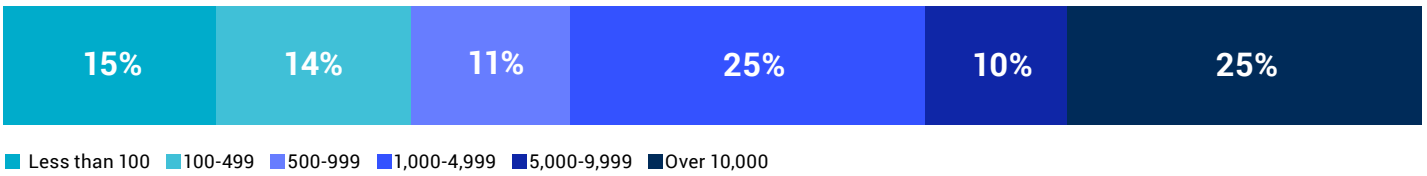
Invest in Comprehensive Vulnerability Management Solutions: Choose solutions that offer comprehensive coverage. From asset discovery, vulnerability assessment, and scanning to risk management, patch management, and reporting and analytics, each feature plays a vital role in managing vulnerabilities.

Increase Visibility and Control: Having comprehensive visibility and control over your IT assets is key to effective vulnerability management. Consider solutions that provide a single-pane-of-glass view into your environment, increasing visibility and enabling better control.

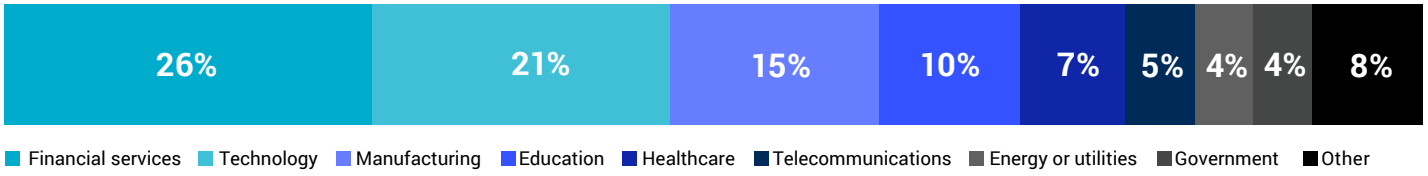
Methodology & Demographics

The 2023 State of Vulnerability Management Report is based on the results of a comprehensive online global survey of 421 cybersecurity professionals, conducted in June 2023, to gain deep insight into the latest trends, key challenges, and solution preferences for vulnerability management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes, across multiple industries.

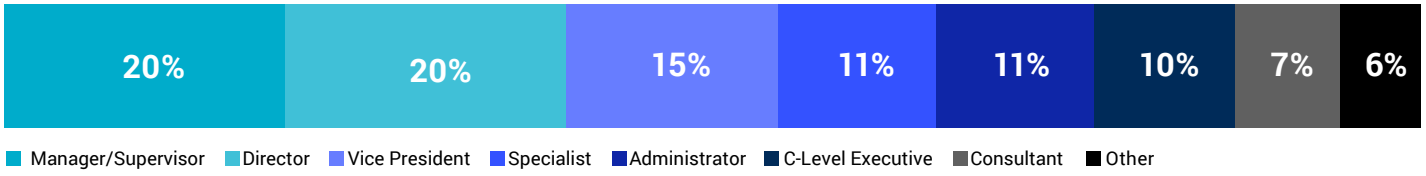
Company size



Primary industry



Job position



Department

Syxsense, the leading unified security and endpoint management (USEM) software vendor, develops cloud-native solutions that centralize patch management, vulnerability management, remediation, compliance reporting, zero trust on the endpoint, and automation and orchestration. Enterprises gain real-time visibility into devices, networks, and cloud infrastructure while improving operational efficiency and employee productivity and reducing risk. Simplify security with Syxsense.

For more, visit **www.syxsense.com**.

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at **info@cybersecurity-insiders.com** or visit **cybersecurity-insiders.com**