SANS | Research Program

2025 SURVEY

SANS Attack Surface Management (ASM) Survey 2025

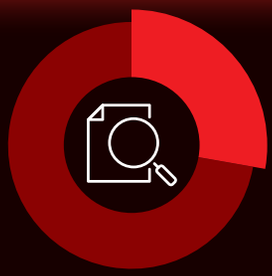
Written by **Chris Dale**
October 2025

SANS 2025 ASM SURVEY

Key Findings

55%

of organizations expect their ASM to protect both internal and external assets



Only 28%

say that their ASM platform effectively identifies sensitive files across the entire attack surface

58%

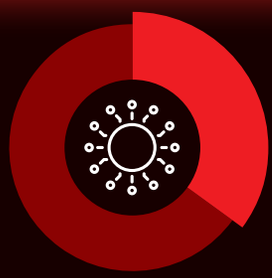
of respondents lean toward a hybrid of manual and automated operation

59%

want to scan their environment daily

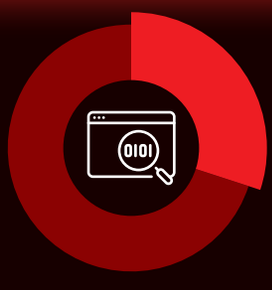
37%

want their ASM to improve their understanding of external exposures



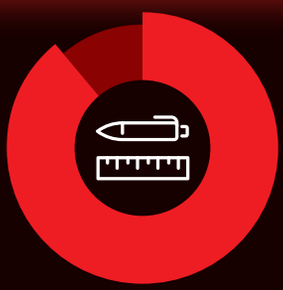
35%

want their ASM to provide current information on vulnerabilities across their attack surface



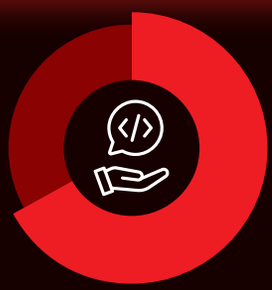
30%

want their ASM to prevent exploitation of exfiltrated data



89%

expect their ASM platform to measure and quantify risks for each asset



67%

expect their ASM platform to provide mitigation and response recommendations for existing vulnerabilities with POCs

Survey Author

Chris Dale
SANS Principal Instructor

CURRENTLY TEACHING

SEC504: Hacker Tools, Techniques, and Incident Handling™

SEC599: Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses™

VIEW PROFILE

An IT enthusiast who had childhood dreams of becoming a hacker, Chris Dale's path to a career in information security was set after his older brother hacked him. Today Chris uses his hacker skills to demonstrate risk via offensive services and incident response. Chris began his career in 2009 working for a large Norwegian ISP, doing development and IT operations. "I really learned about how all things interconnect and work," he says. Since then he's worked for multiple companies in important roles, and his last job was the head of cybersecurity at a 60-man cybersecurity consulting firm. There he managed several teams, including pen testing and incident response. In 2020, Chris founded his own company, River Security, specializing in offensive services, attack surface management and cyber consulting.

Expert Corner

After spending over a decade ethically attacking large organizations globally, one thing is clear, even the most mature companies, especially those with complex infrastructures, struggle with visibility into their true attack surface. ASM is a logical evolution to traditional asset inventory and vulnerability management. Adversary emulation exercises such as red and purple teams aim to not only bypass defenses, but exploit "blind spots" in environments. The message is simple: You can't secure what you don't know is there. ASM allows organizations to take advantage of modern approaches in automation, deep learning and AI, easing what were traditionally challenging and time-consuming activities especially in the areas of visibility and correlation.

Karim Lalji
SANS Certified Instructor

COURSES TAUGHT

SEC588: Cloud Penetration Testing™

SEC565: Red Team Operations and Adversary Emulation™

VIEW PROFILE

Executive Summary

The perpetual challenge of comprehensive asset inventory has long plagued IT organizations, with incomplete configuration management databases and outdated asset registries serving as persistent reminders of the gap between security theory and operational reality. Although IT environments undergo constant transformation through cloud adoption, DevOps practices, and distributed infrastructure, traditional asset management approaches have struggled to maintain pace with this dynamic landscape. The consequences of these inventory gaps extend far beyond administrative inconvenience—security assessments consistently reveal how unknown or forgotten assets become primary vectors for organizational compromise.

Attack surface management (ASM) represents a change in thinking in addressing this fundamental challenge, offering a solution that may finally bridge the longstanding divide between asset visibility and security effectiveness. Unlike conventional asset management tools that rely on manual processes and static inventories, ASM uses continuous discovery techniques derived from offensive security methodologies to automatically identify and catalog organizational assets from an external perspective. This approach provides comprehensive, real-time visibility that has historically eluded traditional asset management initiatives.

Attack Surface Management bridges the gap between asset visibility and security by delivering real-time, attacker's-eye discovery of organizational assets.

The strategic integration of offensive reconnaissance capabilities with defensive security operations creates a more robust foundation for organizational security postures. By adopting the same discovery techniques employed by potential attackers, ASM solutions provide security teams with an authentic view of their external attack surface while maintaining the systematic oversight required for effective defense.

This research report presents findings from a comprehensive survey of over 200 security professionals, all of whom have either implemented ASM solutions or have committed to deployment within the next 12 months. The analysis reveals how organizations are leveraging ASM to transform their approach to asset visibility and security management, potentially resolving one of cybersecurity's most persistent operational challenges.

Demographics

The survey encompassed 235 participants, a mix of organizations currently using ASM (59%) and those planning to implement it within the next 12 months (41%). More than half (54%) of respondents work for corporations headquartered in the United States, and 64% provided professional services and support in the United States. The top industries represented were the usual mix of technology (20%), cybersecurity (13%), government (12%), and banking and finance (12%), and there was a diverse representation of organization size (see Figure 1).

Figure 1. Demographics

Attack Surface Management: A Critical Foundation for Modern Defense

ASM has emerged as a cornerstone of contemporary cybersecurity strategy, driven by a fundamental principle: Eliminating attack vectors eliminates exploitation opportunities. Although organizations have long struggled with comprehensive asset management—often relegating configuration management databases and asset inventories to perpetually incomplete projects—the security implications of these gaps have become increasingly severe. Red team exercises consistently demonstrate how shadow IT infrastructure, legacy services, and unpatched systems create pathways for compromise, underscoring the urgent need for systematic visibility and control.

The Strategic Imperative of Attack Surface Management

Organizations deploy ASM to establish comprehensive oversight of potential attack vectors throughout their infrastructure, creating visibility that spans network perimeters, application layers, and cloud environments. Although many security solutions rely solely on technological implementation to drive transformation, ASM differentiates itself by integrating offensive and defensive security methodologies into a cohesive operational framework. This integration enables security teams to harness red team reconnaissance techniques alongside blue team defensive strategies, creating what practitioners recognize as "purple team synergies," a unified approach that leverages both adversarial (red team) and protective (blue team) perspectives to systematically strengthen organizational security posture.

The foundational premise of ASM rests on the recognition that an organization's attack surface encompasses all accessible assets and services. This comprehensive scope provides CISOs with critical visibility into organizational exposure, enabling evidence-based risk assessment and strategic security planning. For IT administrators and development teams, ASM offers operational benefits including release management oversight and the ability to enforce security standards before production deployment. Technology's effectiveness ultimately depends on vendors' capabilities to transform extensive asset data into actionable intelligence. This highlights the fact that while ASM excels at comprehensive data collection, its true value emerges through sophisticated analysis and presentation of security-relevant insights.

ASM: A Tool for the Outside, Inside, or Both?

Traditionally, when security practitioners discuss ASM, the common assumption has been that it is primarily an external tool, designed to help organizations understand their public-facing exposure, identify shadow IT, and map their digital footprint. This perspective often leads to the use of terms like E-ASM to specifically denote external-focused solutions. However, our research strongly indicates a significant shift in expectations, moving beyond this narrow view.

A Clear Mandate for Comprehensive Coverage

The survey findings reveal a decisive organizational preference for comprehensive ASM solutions that transcend traditional security boundaries. More than half of respondents (55%) explicitly demand ASM solutions that provide unified coverage of both external and internal assets, significantly outpacing those who prioritize external-only coverage (32%) or internal-focused protection (14%) (see Figure 2). This data exposes a critical market disconnect because although organizations overwhelmingly seek integrated visibility across their entire attack surface, most current ASM implementations remain narrowly focused on external asset discovery and monitoring.

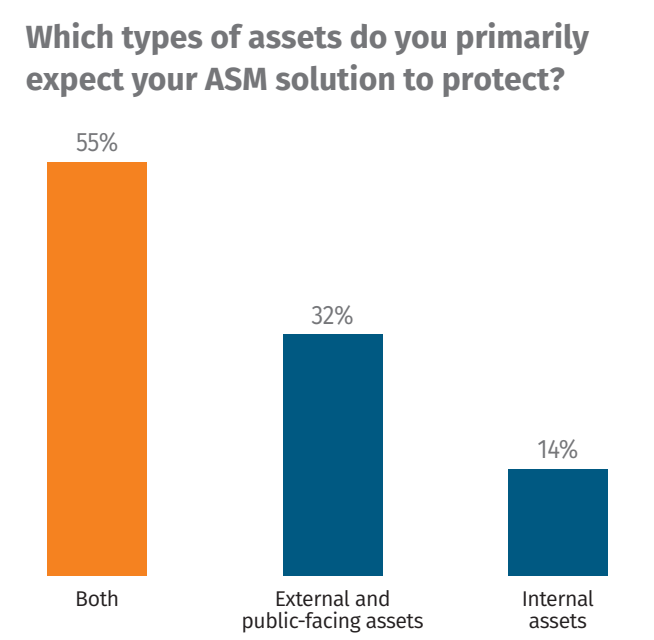


Figure 2. Majority Demand ASM Covers Both Internal and External Assets

The implications extend beyond mere feature preferences. This represents a fundamental shift in how security leaders conceptualize ASM. Organizations recognize that modern threat actors do not distinguish between internal and external attack vectors, making siloed security approaches increasingly obsolete. However, the market reality shows that few vendors currently deliver the comprehensive coverage organizations demand, creating a substantial opportunity gap between customer expectations and available solutions. This misalignment suggests that ASM vendors who can successfully integrate both internal and external asset management capabilities will be positioned to capture disproportionate market share as organizations seek to consolidate their security infrastructure.

The Distinct Challenges and Criticality of the Internal Landscape

The internal attack surface presents a vastly different—often more complex and heterogeneous—environment compared to the external façade of an organization in the following ways:

- **Vulnerability density—**Internally, vulnerability is often far more plentiful. This includes issues stemming from outdated services and unpatched systems that attackers continue to exploit.
- **Exotic attack surface—**The internal landscape can be "much more exotic and less homogenic," filled with a diverse array of systems that may not adhere to the same policies and standards as public-facing assets.
- **Prioritization complexity—**Risk acceptance and different environmental configurations make prioritization much more challenging on the inside.
- **Scanning difficulties—**Internal networks are highly susceptible to issues during scanning, facing stability and availability challenges, and sometimes containing equipment that could drastically fail if scanned improperly. Unlike the public internet, which is "all in one big smelly dump" from a scanning perspective, internal networks often require agents, scanners, and deployments across a range of segmented locations.

The internal attack surface is far more complex and fragmented than external environments, with denser vulnerabilities, more diverse systems, harder risk prioritization, more limited sensitive file visibility, and greater challenges in safely scanning segmented networks.

One alarming finding is that only 28% of existing ASM platforms effectively identify sensitive files across the attack surface. This is critical because discovering sensitive files is a primary tactic for threat actors, and the methods for doing so differ significantly between external and internal assets (see Figure 3).

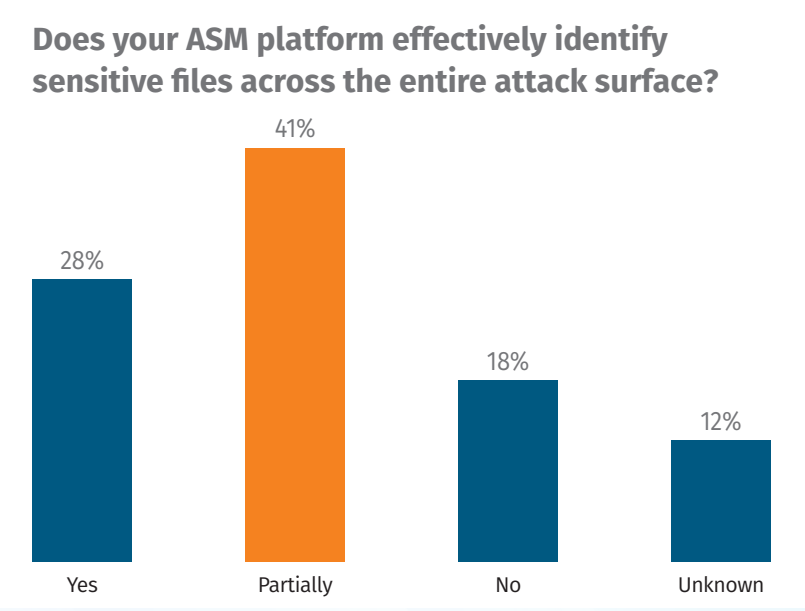


Figure 3. ASM Partially Effective in Identifying Sensitive Files

Despite these complexities, organizations can make a compelling argument to focus intensely on the internal attack surface. Many assume that it's inevitable that attackers will breach their environment and are absolutely going to get on the inside. Therefore, robust internal protection is paramount. Although others might argue that the internal environment generates too many alerts due to its complexity, the strategic imperative remains.

More Than Automation—Built to Be Used

The prevailing narrative in cybersecurity often champions full automation as the ultimate solution for efficiency and scale. For ASM, however, survey data paints a different picture. Respondents are not currently using an entirely automated solution. Only 11% expected 90% or higher automation, with the average level of expected automation hovering around 58% (median 61%) (see Figure 4). This preference for a hybrid model underscores a key insight: Organizations want automation to handle the heavy lifting of data collection and initial identification, but they expect to actively engage with the insights provided.

What is the level of automation that you are using in your ASM solution? ***Consider 0% to be completely manual and 100% to be completely automated.***

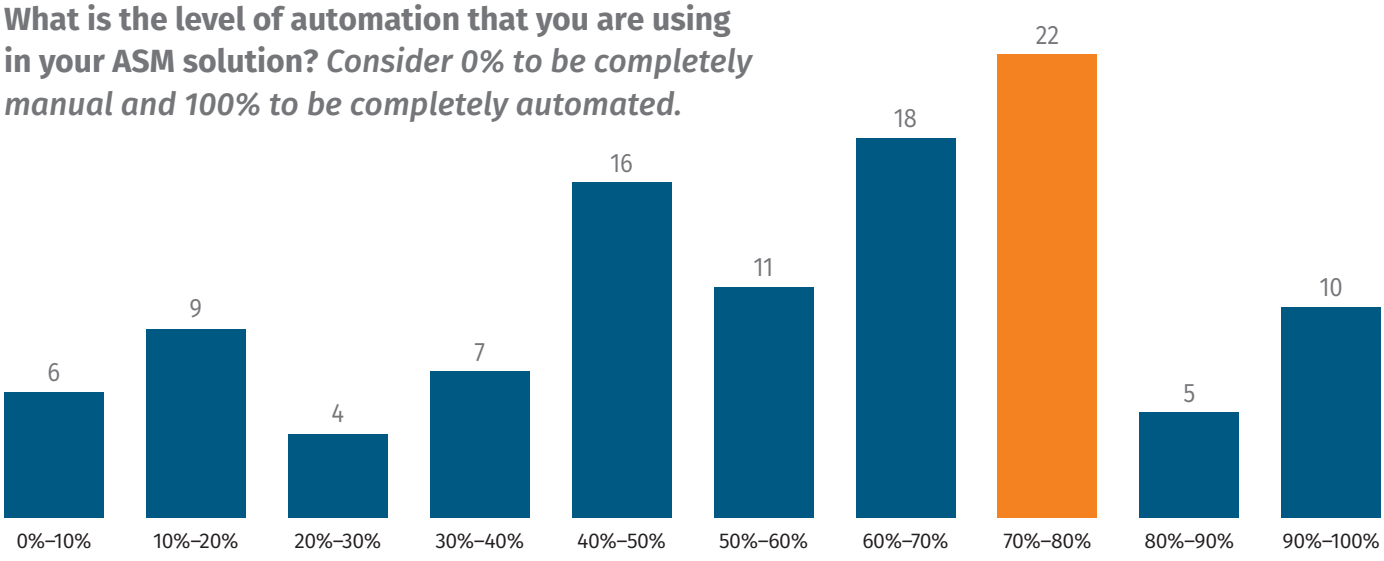


Figure 4. Level of ASM Automation

Expert Corner

While this survey offers an encouraging insight into the maturation of security organizations, it also reveals a critical challenge. Organizations are rightly no longer settling for simple inventory management; they are demanding integrated platforms that provide a clear path from discovery to remediation. However, this drive for comprehensive visibility must be balanced with caution. While a majority of respondents (59%) desire daily scans, it's vital to recognize that such frequency is not without risk, especially on sensitive internal networks. If an organization's ASM tool is running internally with elevated privileges—which is often the case—it can become a high-value target for attackers, creating a potential pivot point for a full compromise. Ultimately, while we see a positive evolution in the adoption and capabilities of ASM tooling, we must remember that it is a powerful enabler for, not a replacement of, advanced human-led testing like red teaming.

VIEW PROFILE

Jean-François Maes
SANS Certified Instructor;
CEO at Offensive Guardian

COURSES TAUGHT

SEC565: Red Team Operations and Adversary Emulation™

SEC699: Advanced Purple Teaming – Adversary Emulation & Detection Engineering™

Automated Scans, Human-Driven Action

Considering the scan frequency further clarifies this hybrid expectation. A significant 59% of respondents expressed a preference for daily scanning, while a mere 10% desired on-demand scanning (see Figure 5).

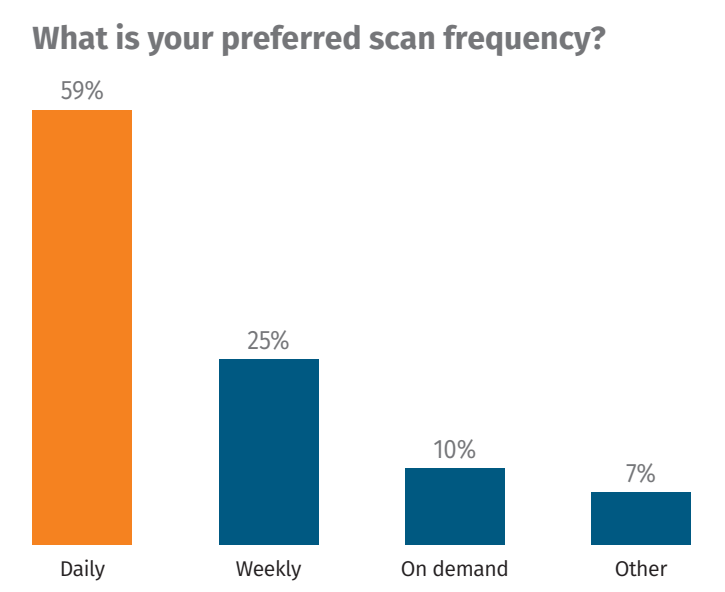


Figure 5. Daily Scanning Preferred

These responses indicate that organizations expect ASM solutions to mostly automate the scanning process, providing a constant, up-to-date view of the attack surface. Yet, the primary desired outcomes from an ASM program are deeply rooted in human understanding and strategic decision-making (see Figure 6):

- The No. 1 response, by 37% of respondents, was understanding external exposure. This highlights the need for clear, actionable insights into where an organization might be lacking protection.
- The second highest response (35%) was receiving current information on vulnerabilities across the attack surface. This points to the demand for vulnerability intelligence, which includes knowing if a vulnerability is exploitable, actively exploited by others, or has a public proof-of-concept (POC).

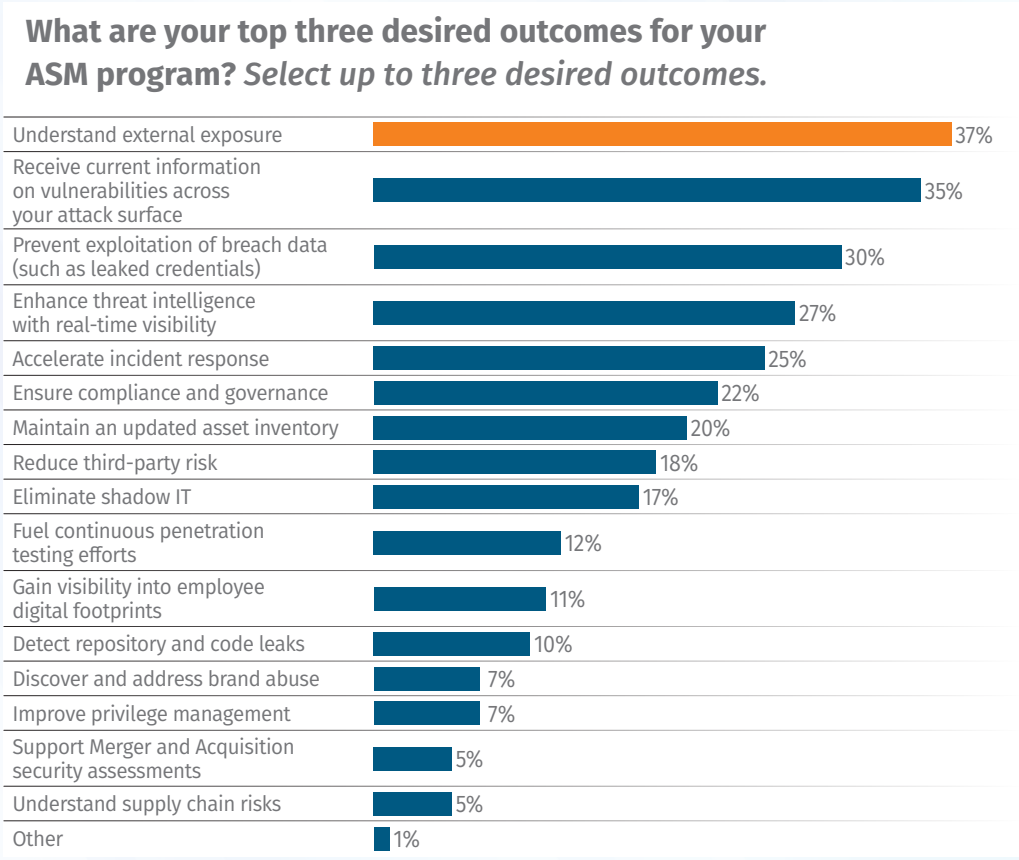


Figure 6. Desired Outcomes for the ASM Program

Indeed, 89% of respondents expect their ASM platform to measure and quantify risks for their assets, further supporting the importance of integrated vulnerability intelligence. When an ASM solution identifies a vulnerability with a publicly available POC, 67% of respondents consider mitigation and response recommendations as critical to include in the notification. This reinforces the need for human guidance and actionable advice, not just automated alerts.

Beyond Alerts: Refining Defensive Tradecraft

The fact that respondents don't want just another automated tool is an incredibly positive sign. It suggests a shift away from passively consuming alerts and toward actively using ASM to refine security operations. This aligns with the idea that ASM has the potential to become a tool that refines both defensive (blue team) and offensive (red team) tradecraft, fostering greater "purple synergy."

Security teams who can "seed" the platform with their own assets and knowledge make ASM more powerful, improving accuracy and coverage. This collaborative approach helps identify crucial assets like shadow IT or lookalike domains that purely generic scans might otherwise miss.

Unlike with security controls such as antivirus or EDR, practitioners should not fear the presence of false positives in ASM. Instead, they should view false positives as an indicator that the platform is collecting enough data. The ASM tool's role is then to make these false positives easy to manage, potentially through AI and scoring algorithms.

ASM as Fuel for Continuous Penetration Testing

The ultimate expression of ASM being built to be used lies in its potential to fuel continuous penetration testing efforts. A significant 47% of respondents indicated their ASM platform integrates with penetration testing platforms or workflows (see Figure 7). Given that traditional pen tests can quickly become stale due to the high velocity of IT change, ASM offers a continuous, evolving view of the attack surface. In this vision, ASM could effectively operate like a SIEM, where alerts are not "problems" to remediate, but instead are opportunities to hack. This represents a powerful shift toward proactive, continuous security validation, driven by an actively utilized ASM platform.

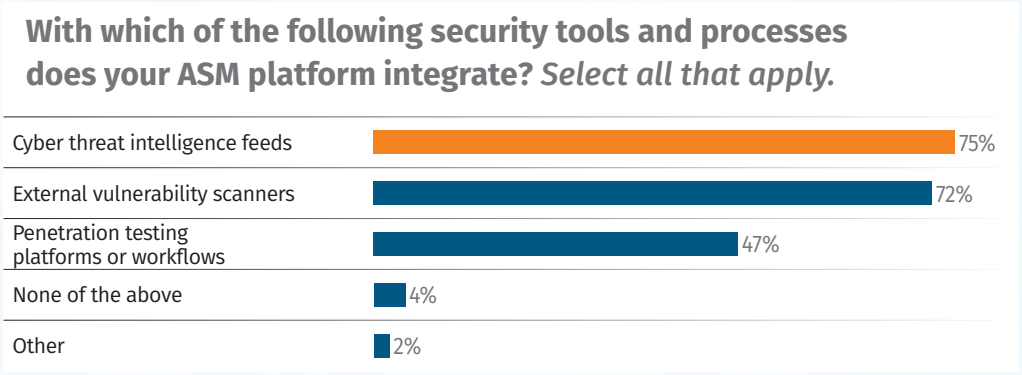


Figure 7. ASM Integration with Tools and Processes

From Red Team to ASM: Teaching Tools to Think Like Attackers

The foundational element of any successful security operation, particularly from an attacker's perspective, is reconnaissance. Respondents indicated a clear desire for ASM solutions to excel in this area, moving beyond basic asset identification to deeply understand an organization's digital footprint.

Current State of Asset Discovery

When asked how their ASM solution discovers assets, an overwhelming majority of respondents (81%) indicated that their solutions use ASN and IP range enumeration (see Figure 8). Although we expected this, the survey also showed a diversity of "other" responses, indicating that there are many more ways ASM solutions can discover assets in addition to the options provided in the survey.

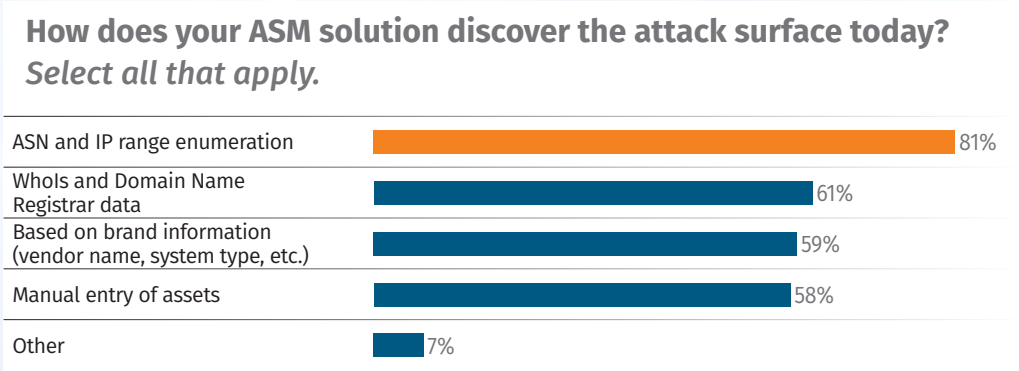


Figure 8. Attack Surface Discovery Methods

Red teamers often refer to asset discovery as reconnaissance, emphasizing it as arguably the most important phase of any engagement. The attacker with the best reconnaissance is frequently the most successful. Reconnaissance can range from basic to highly complex, depending on the threat actor's talent, techniques, and capabilities.

The Imperative of 'Deep' Reconnaissance

Many ASM vendors have "wide" reconnaissance, which involves broadly scanning for domains, IPs, networks, and ASNs. However, vendors who go "deep" will likely quickly become leaders in the ASM market. Going deep means delving into applications and technologies to provide profound insights beyond just network services, enumerating the actual "meat on the bone" of these services. This includes understanding how to enumerate content and dependencies across various application technologies, such as Single Page React applications versus WordPress applications or Django APIs, as they differ significantly.

A potential sign of immaturity for an ASM platform is if it does not properly enumerate assets deeply, relying solely on IP addresses and domains, as the attack surface encompasses much more. This distinction between specialists and more generic vendors will likely become a key differentiator in the market.

Integrations Will Be Important: Red and Blue Becomes Purple

Although external reconnaissance is crucial, supplementing this with internal knowledge—a blend of offensive and defensive insights and capabilities achieving purple synergy—provides true effectiveness. Figure 9 outlines how practitioners want ASM platforms to expand beyond traditional data collection.

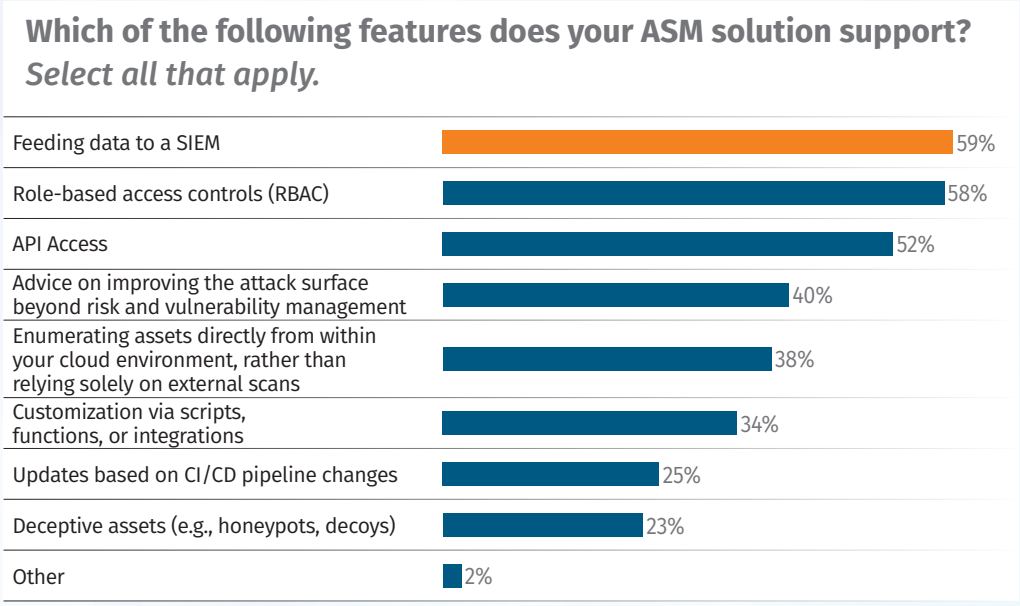


Figure 9. ASM Features

Looking at this data, we see the following:

- **Internal cloud environment enumeration—**A significant portion of respondents, 38%, indicated their desire for ASM solutions to enumerate assets directly from within their cloud environment, rather than solely relying on external scans. This direct access to internal cloud data provides a "next-generation defense" capability, as attackers lack this privileged integration. It allows for a more comprehensive and accurate view of cloud assets.
- **CI/CD pipeline integration—**The survey revealed that 25% of respondents' ASM platforms support updates based on CI/CD pipeline changes. This integration with the software development life cycle (SDLC) is transformative, enabling automatic notifications to the ASM tool about new builds and deployments. This capability facilitates continuous vulnerability scanning, hygiene monitoring, and even penetration testing triggered by code changes, ensuring that the attack surface remains well-understood as IT evolves.

A substantial 71% of respondents reported that their ASM platform integrates into cyber threat intelligence (CTI) feeds (see Figure 10). This integration is critical for transforming a flood of data into actionable insights.

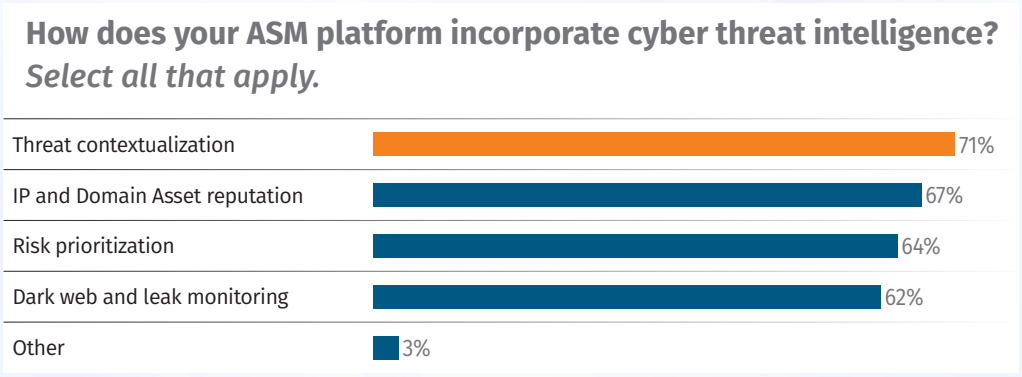


Figure 10. Methods of Integrating Cyber Threat Intelligence

Nearly three-quarters of respondents (72%) confirmed that their ASM platform integrates with external vulnerability scanners. This often occurs via API or webhooks (77%) or natively (45%) (see Figure 11). These integrations enhance the vulnerability intelligence provided by ASM, complementing its discovery capabilities. When ASM identifies a vulnerability with a publicly available POC, 67% of respondents consider mitigation and response recommendations critical to include in the notification, demonstrating the demand for actionable vulnerability intelligence.

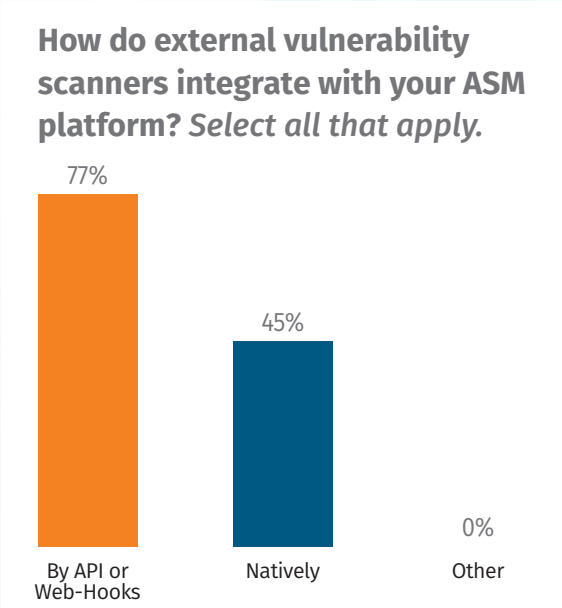


Figure 11. ASM Integration with External Vulnerability Scanners

By embracing these integrations, ASM platforms move beyond simple asset inventory, which has historically been a challenge for many organizations. They become dynamic, intelligent systems that provide a holistic and continuously updated view of the attack surface, leveraging both external reconnaissance and rich internal context. This collaborative approach between red and blue teams, facilitated by integration, is key to enhancing overall defensive posture and proactive security validation.

ASM as the SIEM for Continuous Penetration Testing

Almost half of respondents (47%) said that their ASM platform integrates with penetration testing platforms or workflows. This suggests that if an ASM platform is sufficiently robust, it can act as the fuel for continuous penetration testing.

The need for continuous penetration testing stems from the inherent difficulties with traditional, point-in-time assessments. Many security practitioners have lost confidence in pen testing as results quickly become stale due to the high velocity of change within IT environments. They describe IT as a moving target, meaning what is secure today may not be tomorrow.

Do ASM platforms have the potential to transform into critical enablers for more effective and dynamic continuous penetration testing efforts?

Given these challenges, there's a growing expectation that pen testers will increasingly view ASM as a viable solution to facilitate continuous penetration testing. ASM's ability to provide a constantly updated view of the attack surface allows for ongoing assessment rather than periodic snapshots.

Organizations can conceptualize ASM as a "SIEM for hacking opportunities." Within this framework, the ASM platform generates alerts that teams should not view merely as "problems" requiring remediation. Instead, security professionals can reframe these alerts as "opportunities to hack"—opportunities providing direct insights that enable offensive security teams to validate vulnerabilities and identify exploitable paths. This approach reinforces the concept of purple synergy between red and blue teams, empowering both groups to use the ASM platform for their respective objectives.

This also highlights ASM's potential to evolve beyond a mere defensive tool into a proactive platform that actively supports and enhances both blue team defenses and red team operations, leading to a more integrated and effective security posture.

The Future of Cybersecurity: ASM as the Strategic Cornerstone

The findings from the SANS 2025 ASM Survey reveal a fundamental shift in how organizations approach cybersecurity—attack surface management is not merely another security tool, but rather an emerging strategic cornerstone that promises to revolutionize organizational defense posture. As digital transformation accelerates and attack vectors multiply, ASM has positioned itself as the comprehensive solution organizations have long sought to achieve true visibility and control over their expanding digital footprint.

The survey data demonstrates that ASM's evolution transcends traditional security boundaries, encompassing holistic exposure management, proactive risk validation, enhanced stakeholder engagement, intelligent integration capabilities, and sophisticated data visualization. This comprehensive approach addresses the core challenge that has plagued cybersecurity for decades: the gap between data collection and actionable intelligence.

Perhaps most significantly, the survey reveals a maturation in organizational expectations. Security teams are demanding solutions that deliver operational value, not merely automated alerts that contribute to alert fatigue. This shift represents a crucial departure from the "sleeping SOC" phenomenon that has undermined security operations in the past. Organizations are investing in ASM with the explicit intention of leveraging its insights into strategic decision-making and tactical improvements.

The convergence of comprehensive asset discovery, continuous monitoring, and intelligent analysis positions ASM as more than a security solution. It represents a new operational paradigm where "attack surface means everything" translates into actionable organizational intelligence. As we look toward the future of cybersecurity, ASM stands as proof that the industry is finally bridging the divide between data abundance and security effectiveness, offering organizations the strategic visibility they need to thrive in an increasingly complex threat landscape.

Sponsors

SANS would like to thank this survey's sponsors:

netwrix

okta

Qualys.
Continuous Security

WIZ

SANS | Research Program

About the SANS Research Program

The SANS Research Program is a key initiative by the SANS Institute and a premier global provider of cybersecurity research and information. SANS Research Program is designed to provide cybersecurity practitioners and leaders with data-driven insights, thought leadership, and solutions that help them better understand and respond to evolving security challenges. All content is authored by SANS instructor experts from around the world who apply their years of experience from hands-on practitioner work in the field, advisory roles, and the classroom to provide education, guidance, and actionable insights that help make the cyber world a safer place.

To learn about sponsorship opportunities for research, content, and in-person or virtual events, email us at **Sponsorships@sans.org** or go to **www.sans.org/sponsorship**.