Enterprise Strategy Group by TechTarget

SHOWCASE

JUNE 2023

Toward Comprehensive Attack Surface Management

Jon Oltsik, Distinguished Analyst and Fellow

Abstract: As organizations embrace digital transformation and take advantage of cloud-based resources, the external attack surface is in a constant state of change and growth. This can lead to dozens or hundreds of unknown, unmanaged, or poorly managed assets, greatly increasing the risk of a cyberattack. Cobbling together technologies and manual processes doesn't address modern attack surface management (ASM) requirements. Organizations need comprehensive ASM solutions that accurately discover assets, map attack paths, understand exploitability, calculate risk scores, and guide remediation priorities.

Overview – The Problem

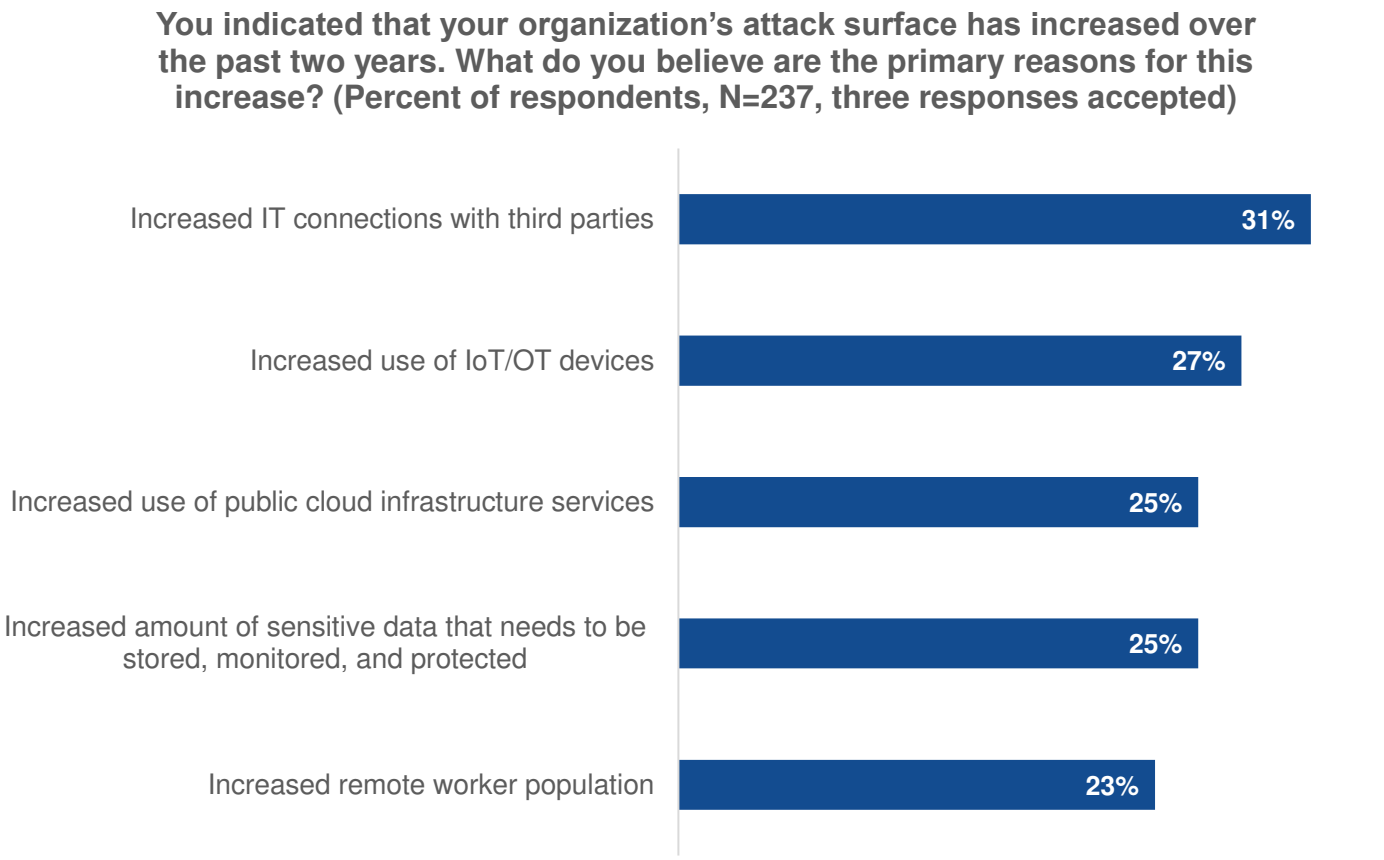
A few short years ago, ASM was relatively unknown and limited to a subset of the largest organizations, but this is no longer true. ASM has become a critical component of cyber-risk mitigation and a mainstream practice. Why the transition? Recent research from TechTarget's Enterprise Strategy Group reflects the state of ASM today:[1]

- **A vulnerable attack surface presents an easy target for cyber-adversaries.** In fact, 76% of organizations say they've experienced a cyberattack because of an unknown, unmanaged, or mismanaged asset on their internet-facing asset.
- **Many organizations admit to blind spots on their attack surface.** Nearly three-quarters of enterprises (73%) believe they have strong awareness of less than 80% of their assets. This means that 1 in 5 internet-facing assets could be vulnerable to attack or exploited easily.
- **The attack surface is growing and changing constantly.** More than half (62%) of organizations claim that their attack surface has grown over the past two years, driven by increasing third-party connections, device proliferation, and increased use of public cloud infrastructure (see Figure 1). Many firms are also active in mergers and acquisitions, expanding the attack surface. This may be another reason why so many organizations are adopting ASM practices.
- **Discovering the attack surface and creating an accurate inventory can be extremely resource-intensive.** Nearly half (48%) of organizations claim that it takes them more than 80 hours to do a full attack surface discovery using their existing processes and technologies.

This data captures current attack surface management challenges. The attack surface is dynamic and expanding, but organizations continue to use antiquated manual processes and a potpourri of tools to try and keep up. The result? Increasing cyber-risks and cyberattacks. Addressing this mismatch should be a high priority for CISOs.

[1] Source: Enterprise Strategy Group Complete Survey Results, *Security Hygiene and Posture Management Remains Decentralized and Complex*, June 2023.

Figure 1. Top 5 Reasons Why the Attack Surface Has Increased



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

What's Needed for ASM

Many CISOs now realize they need to better protect their attack surface. Unfortunately, the security technology industry is fraught with hyperbole, leading to massive confusion on what ASM is, what it does, and the use cases it supports.

What are the most important capabilities of ASM? Enterprise Strategy Group believes ASM solutions should provide:

- **Continuous and accurate asset discovery.** ASM should provide an adversary's view by scanning the attack surface and discovering all known and unknown assets (i.e., servers, web applications, digital certificates, cloud-based assets, SaaS platforms, etc.). It's also important to identify assets and connections in the digital supply chain by mapping web links and DNS records. Leading solutions remain active, discovering and reporting on attack surface changes as they occur.
- **Context around business-critical assets.** Beyond discovery, ASM solutions should offer some context around asset type, known exploits, and asset classification. For example, ASM should understand that a honeypot vulnerability is far less concerning than a misconfigured DNS setting on the company's partner portal. The best ASM offerings assess multiple asset attributes to calculate a risk score and back this risk score with a clear contextual description, helping security professionals prioritize cyber-risk mitigation actions.
- **Attack-path mapping.** Cyber-adversaries follow a kill chain progression by exploiting vulnerable assets, downloading malware to compromised systems, and then moving laterally across networks in pursuit of some

end goal (i.e., data exfiltration, data encryption/ransomware, denial of service, etc.). ASM solutions are often built on top of a graph database. This gives them the ability to understand asset relationships, connections, and ultimately, attack paths. By identifying attack paths originating from the digital supply chain, ASM can help organizations pinpoint the vulnerable *entry points*—i.e., those assets at risk from outside the organization. Armed with this knowledge, security and IT operations teams can prioritize remediation actions, closing off multiple attack paths in the process.

- **An intuitive, customizable UI/UX that supports different users and needs.** ASM is used throughout the organization by multiple security and IT operations teams. Therefore, leading solutions should provide customizable dashboards for different users like security operations center (SOC) analysts, VM analysts, CISOs, IT operations, auditors, risk management personnel, etc., helping them to reduce noise and increase their productivity. As part of the user experience, ASM should offer alerts and reporting for each type of user. For example, the vulnerability management team should be alerted when a new asset is discovered, while security and IT operations teams should receive an alert with a clear description of remediation priorities.

Standard ASM use cases typically:

- **Include cyber-risk management assessment and reporting.** Under the theme of, “You can’t manage what you can’t measure,” ASM can provide both detailed and aggregated views of cyber-risk from an "outside-in" perspective. With an ASM map in hand, CISOs can communicate and work with executive boards on cyber-risk management strategies, security posture priorities, and longer-term security strategy.
- **Boost the operational efficiency of the vulnerability management program.** Vulnerability management programs are limited to known assets and IP ranges, so they miss unknown internet-facing systems, which are often used as a gateway for cyberattacks. ASM not only discovers these assets, but leading solutions apply risk scores and attack path maps to them. These can help security and IT teams conduct more effective vulnerability scans, especially on newly discovered assets. Ultimately, ASM can also help organizations transform vulnerability management into exposure management, where remediation actions are focused on high-value vulnerable assets with known exploits "in the wild."
- **Help IT operations accelerate remediation actions and improve collaboration.** When some security teams complete vulnerability scans, they “throw the results over the fence” to IT operations teams, forcing them to figure out the remediation approach based on things like CVEs, vendor vulnerability bulletins, and asset classification. ASM risk scoring and attack path mapping adds exploitability context to vulnerability data, helping organizations determine remediation priorities.
- **Provide additional context for security investigations.** Security analysts can improve the efficacy and efficiency of security investigations with ASM data. How? When the SOC team detects a cyberattack in progress, they can use ASM data to correlate alerts and incidents with attack paths and exploitable vulnerabilities. This knowledge can help them determine root cause, track adversary progress, and anticipate further tactics, techniques, and procedures.

In summary, leading ASM solutions translate security issues, vulnerabilities, and misconfigurations into prioritized IT action items through a process flow: (1) asset discovery; (2) testing and scanning for issues; (3) computing risk scores; and (4) generating lists of prioritized IT remediation actions.

IONIX for ASM

Enterprise organizations face confusing choices around ASM. Should ASM be part of threat detection and response, threat intelligence, or vulnerability management? In many cases, ASM presented as a feature of other solutions, but this may not be sufficient for enterprise organizations with a growing, dynamic attack surface. Rather, these organizations should seek full solutions, like IONIX, that align with the requirements defined above. IONIX ASM can help organizations:

- **Discover the entire attack surface**. IONIX Connective Intelligence uses multiple technologies such as machine learning and connection intelligence to map an organization’s attack surface, including the digital

supply chain. IONIX uses a dynamic, graph-based data model with nodes and dependencies that are continuously updated and evaluated. This helps maintain up-to-date and accurate attack surface monitoring.

- **Uncover asset connections and associated risks for remediation prioritization**. After attack surface discovery, IONIX assesses risks based on asset value, attack paths, exploitability, and correlated threat intelligence data. It uses this analysis to calculate risk scores. This helps organizations identify urgent needs and track overall progress over time.
- **Accelerate remediation workflows.** To support existing remediation processes, IONIX integrates with security operations technologies like SIEM and SOAR (security orchestration, automation, and response), as well as ticketing systems. IONIX also provides something it calls "Active Protection." When IONIX detects a vulnerable DNS record, S3 bucket, or Azure blob, Active Protection automatically neutralizes the threat.

Conclusion

In an era of cloud-native applications, a remote workforce, and digital transformation applications, constant attack surface growth and changes are unavoidable. Lengthy, periodic attack surface discovery is no longer adequate for ASM. Rather, CISOs need scalable, intelligent, and watchful ASM solutions to manage cyber-risks and support the business. Those looking for such a solution may want to evaluate IONIX.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com