ARMADA
Powered by risk3sixty

SEE WHAT ATTACKERS SEE

A Practical Guide to Enterprise Attack Surface Management (ASM)

Key Takeaways

- Why the time for ASM is now and the economics of breach prevention
- 3 primary vectors where breaches actually start
- The ASM lifecycle, who benefits, and ROI



EXECUTIVE SUMMARY

By 2025, nearly every organization operates in a distributed, cloud-first model. The result is an external footprint that is constantly shifting and expanding with every new SaaS integration, contractor deployment, cloud service, and employee-driven technology adoption.

While this accelerates business agility, **it also creates blind spots large enough for attackers to exploit long before companies know they exist.**

Traditional security controls were not built for this pace. Static asset inventories become outdated quickly, vulnerability scanners focus only on what is already known, and penetration tests, while valuable, provide only point-in-time assurance.

Meanwhile, modern attackers have adopted continuous techniques for scanning, harvesting, credential stuffing, and exploiting new vulnerabilities within hours of disclosure.

Attack Surface Management (ASM) has emerged as the discipline that closes this gap. It provides continuous, threat-informed visibility into all external-facing assets including known, unknown, orphaned, or inherited through vendors.

In this whitepaper, Cory Wolff, Director of Offensive Security at risk3sixty, offers a practical, real-world view into modern ASM.

Through statistical evidence, real breaches, and operational experience from risk3sixty's Armada team, it explains how organizations can reduce risk by discovering what they own, validating what's exploitable, and remediating what matters most.

"Most organizations don't even realize how big their external footprint actually is. ASM exists to see what attackers see before they can use it against you." – Cory Wolff

WHY ASM NOW? THE ECONOMICS OF BREACH PREVENTION

Modern organizations face a simple and sobering reality: **More surface area, interdependencies, credentials, and third-party systems means more opportunity for attackers.**

Even mature security programs struggle with visibility gaps that arise from SaaS sprawl, cloud misconfigurations, and vendor access.

The financial impact of these gaps is clear. IBM's 2025 Cost of a Data Breach Report places the average incident at $4.4 million, not including indirect costs like long-term customer churn, regulatory obligations, and operational downtime.

Breaches have measurable market impact as well. Public companies underperform peers by 3.2% six months after disclosure. But the headline costs often obscure a more important truth. **Many of these incidents began with small, preventable exposures.**

- A contractor's forgotten VM
- A misconfigured helpdesk subdomain
- A leaked cookie from an unmanaged browser
- A third-party plugin vulnerable to a known exploit

These footholds rarely look significant until attackers use them to pivot deeper. The MGM ransomware case illustrates this point clearly. A single social engineering-enabled intrusion cascaded into **$100 million in quarterly losses**, business disruption, and industry-wide scrutiny. ASM addresses the root problem that an organization cannot secure what it cannot see.

"Whether caused by a breach or a faulty update, if you're down, you're losing money ." – Cory Wolff

THE 3 PRIMARY VECTORS WHERE BREACHES ACTUALLY START

The 2025 Verizon Data Breach Impact Report shows a consistent pattern in that **attackers rarely rely on sophisticated zero-days.** Instead, they exploit simple weaknesses that are much harder for defenders to track at scale.

1. Stolen & Abused Credentials (22%). Modern **infostealers** collect browser cookies, password vault entries, and authentication tokens, silently exfiltrating them to criminal marketplaces. Attackers buy valid credentials that still work and walk directly into systems without triggering alarms.

The Snowflake credential compromise demonstrated the global impact of stealer logs. Dozens of major corporations, including Ticketmaster and Santander, were affected not because Snowflake was compromised, but because attackers purchased contractor credentials that granted downstream access.

Credential theft is now an external attack vector, not merely an endpoint problem. ASM programs that incorporate dark-web and stealer log monitoring provide early warning before threat actors move laterally or escalate privileges.

2. Vulnerability Exploitation (20%). Despite years of patch management innovation, externally exposed vulnerabilities remain a top cause of breaches. Attackers weaponize proof-of-concept exploits within hours of publication. **When an organization lacks complete asset visibility, even a single forgotten server or unpatched appliance can become the entry point.**

Recent examples, including Cisco ASA, VPN appliance, and cloud configuration vulnerabilities, show how quickly attackers probe exposed surfaces once new CVEs appear.

3.Third-Party Pathways (2x YoY Increase). The modern enterprise is woven together with integrations. A vulnerability in a small plugin, a misconfiguration in a vendor-managed environment, or a contractor's personal laptop can open a pathway into core systems. The Salesforce tenant compromise is a textbook illustration. Salesforce itself remained secure, but a vulnerable third-party integration provided attackers the foothold they needed.

Third-party pathways are now one of the fastest-growing attack vectors yet they are the least visible to traditional security teams.

SAAS SPRAWL, SHADOW IT & THE EXPANDING EXTERNAL FOOTPRINT

One of the most underestimated contributors to external exposure is SaaS growth. The average company uses **106 SaaS applications**, many procured without IT involvement. Each brings:

- Authentication surfaces
- Subdomains
- Access rights
- API endpoints
- Configurations
- Plugins
- Vendor dependencies

While these services provide tremendous value, they also distribute responsibility for security across dozens or even hundreds of environments. **When teams decommission a SaaS tool, they rarely remove DNS records or revoke app tokens.** This creates opportunities for subdomain takeovers, abandoned assets, or unintended data exposure.

Cloud infrastructure adds another layer of complexity. Developers can deploy internet-facing assets in seconds, but centralized security teams may not see them for months, if ever. An example is a contractor who spins up Azure VMs without IT's knowledge. **This is not rare**. In many organizations, ASM uncovers internet-facing systems that the security team has never seen before.

This scenario and many like it makes continuous discovery (not annual assessments) essential.

WHAT PROFESSIONAL ASM ACTUALLY LOOKS LIKE

Many organizations begin their ASM journey by evaluating automated tools, only to discover that tooling alone cannot produce meaningful assurance. Automation is excellent for scale, but it is poor at context, prioritization, and determining whether something truly matters.

Professional ASM combines human expertise with technology to create a continuously updated understanding of the organization's real attack surface.

With risk3sixty's Armada team, this approach blends four pillars:



1. Threat-Led Discovery. Rather than scanning everything indiscriminately, discovery efforts are guided by how attackers actually operate. Intelligence is pulled from stealer logs, dark-web marketplaces, Telegram channels, and OSINT feeds to uncover where threat actors may already have a foothold.



2. Human Validation. Analysts verify whether each finding is exploitable and relevant. This eliminates noise and ensures that every issue reaching the client is both real and actionable.



3. Contextualized Threat Intelligence. Organizations receive tailored intelligence that bridges the gap between global threat trends and their own environment. This includes activity targeting their tech stack, assets, and industry.



4. Continuous Monitoring & Remediation Support. ASM persists beyond simply reporting exposures. The program validates fixes, confirms remediation, and tracks improvements in MTTD and MTTR over time.

The result is not a list of vulnerabilities, but an ongoing feedback loop between offensive experts and internal teams.

THE ASM LIFECYCLE: A THREAT-LED MODEL

The ASM lifecycle is best understood as a continuous loop:

- **Discover:** Identify all external-facing assets, including unknown, forgotten, or vendor-controlled systems
- **Validate:** Analysts confirm what is exploitable and add business context
- **Prioritize:** Issues are ranked by threat likelihood, impact, and relevancy
- **Remediate:** Clear, actionable guidance helps teams address root causes
- **Verify:** ASM confirms remediation and monitors for regressions
- **Report:** Teams receive both technical granularity and executive-ready summaries

This model emphasizes that ASM is not an event but a practice that matures and improves over time.

WHO BENEFITS MOST FROM ASM?

Organizations with distributed infrastructures, multi-cloud environments, or large vendor ecosystems experience the greatest immediate value. But ASM also benefits smaller teams that lack the resources to run continuous external monitoring.

Companies undergoing mergers or acquisitions, those rolling out new SaaS initiatives, and those in regulated industries consistently rely on ASM to understand and secure their evolving attack surface.

The common thread is that anyone who cannot confidently answer the question, **"What do we have exposed to the internet right now?"** is a candidate for ASM.

BUILDING THE BUSINESS CASE: ROI AND RISK REDUCTION

A strong ASM program demonstrates measurable improvements that matter to executives including:

- Reduction in unknown assets
- Faster remediation timelines
- Lower vulnerability recurrence
- Validation of third-party exposures
- Increased defensibility for insurers and regulators
- Clear risk trending over time

It's recommended to use expected annual loss (EAL) to demonstrate ROI. **Even conservative estimates using the $4.4M breach cost and realistic incident probabilities can quickly justify the investment.** Organizations that adopt ASM often experience compounding returns.

- Fewer incidents
- Faster triage
- Stronger alignment between offensive and defensive teams

WHAT TO ASK WHEN EVALUATING AN ASM PROVIDER

Selecting the right ASM partner requires asking the right questions:

- Do they validate findings manually?
- How do they confirm remediation?
- Do they provide on-demand executive reporting?
- What intelligence sources do they monitor?
- Can they attribute findings to specific owners?
- Is their methodology threat-led?

If the answer is "no" to any of these questions, the program may produce data but not meaningful outcomes.

CONCLUSION

The modern enterprise cannot defend what it cannot see yet its attack surface is expanding faster than most teams can inventory.

Attack Surface Management fills this critical gap by continuously discovering what is exposed, validating what is real, and prioritizing what attackers are most likely to exploit.

In an era where outages cost billions, ransomware disrupts global operations, and credential theft fuels countless intrusions, ASM offers one of the most effective ways to reduce risk while strengthening operational resilience.

"ASM's job is to discover the exposures, validate them, and help you fix them before an attacker ever gets the chance." – Cory Wolff

About the Author



Cory Wolff

Director of Offensive Security, risk3sixty

With over 20 years of experience in IT, security, and development, Cory Wolff is a passionate and skilled hacker who leads the offensive security practice at risk3sixty.

He holds multiple certifications, including the Offensive Security Certified Professional (OSCP) and the Certified Information Systems Security Professional (CISSP), and has a proven track record of building and breaking various technologies since his first computer in 1988.

LET'S CONNECT

Interested in learning more about ASM and how it can help continuously protect your most valuable assets. Let's connect!



Ross McCurdy
ross.mccurdy@risk3sixty.com

CREST SECURITY TESTING Penetration Testing

CREST MEMBER

risk3sixty and it's Armada team are CREST Accredited for Penetration Testing, one of the most respected, rigorous, and globally recognized credentials in the security industry.

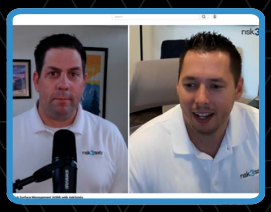
MORE ASM AND OFFENSIVE SECURITY RESOURCES:



Why MapLarge Chose Attack Surface Management With risk3sixty



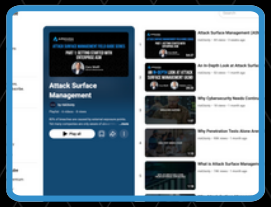
Attack Surface Management (ASM): Getting Started With Enterprise ASM (Part 1)



An In-Depth Look at Attack Surface Management (ASM) with risk3sixty



Inside Infostealers: Evasion, Exploitation, and Lessons from Change Healthcare and Snowflake



ASM Playlist



Threat-Led Penetration Testing for DORA



Hardware Hacking: Discovering a DoS in NetGear Router



Exploiting SharePoint Permissions the Co-Pilot Way

ARMADA
Powered by risk3sixty

CREST SECURITY TESTING Penetration Testing
CREST MEMBER

risk3sixty and it's Armada team are CREST Accredited for Penetration Testing, one of the most respected, rigorous, and globally recognized credentials in the security industry.

ARMADA ASM

Armada Attack Surface Management is a tech-enabled service that allows you to **identify, monitor, and mitigate** vulnerabilities across your entire digital footprint.

Our unique approach uses **advanced technology and expert consultants** to provide the intelligence you need to minimize the risk of cyberattacks.

Continuous Monitoring



Gain real-time insights into your digital assets, identifying and mitigating risks before they become threats.

Automatic Discovery



Automatically identify and catalog all digital assets, including those outside the traditional security parimeter.

Proactive Threat Detection



Utilize our advanced identification engine to detect and address vulnerabilities, ensuring your organization remains secure against emerging cyber threats.

Risk Prioritization



Leverage advanced algorithms to prioritize vulnerabilities based on risk, enabling focused remediation efforts.

Enhanced Visibility



Achieve a comprehensive view of your digital environment, including shadow IT and third-party integrations to better understand and manage your attack surface.

Remediation Validation



Ensure vulnerabilities are effectively addressed with built-in remediation validation, providing automated checks to confirm fixes are successfully implemented.

ARMADA ASM

We go beyond automation. With operators **skilled at exploitation**, our team comprehensively challenges your security posture using the same TTPs as threat actors.

Our **proprietary cyber asset identification engine** is developed in-house by the same team testing your environment.

Receive comprehensive monthly reports and readouts, **broken down in detail by our experts** with in-depth remediation recommendations.

ARMADA
Powered by risk3sixty

- **ARMADA** ASM
- **ARMADA** Red Team
- **ARMADA** Continuous
- **ARMADA** Advanced Testing

Qualified Experts

OSCP · PNPT · CISSP Certified

CONTACT US TODAY!



Cory Wolff
cory.wolff@risk3sixty.com



Ross McCurdy
ross.mccurdy@risk3sixty.com