Atlantic Vantage Point

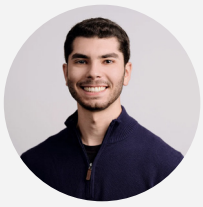
avpcap.com

Defending Against 2030 Cyber Threats

Part 2: Advancing Detection and Remediation

Jessica Hayes

Ethan Ellinger

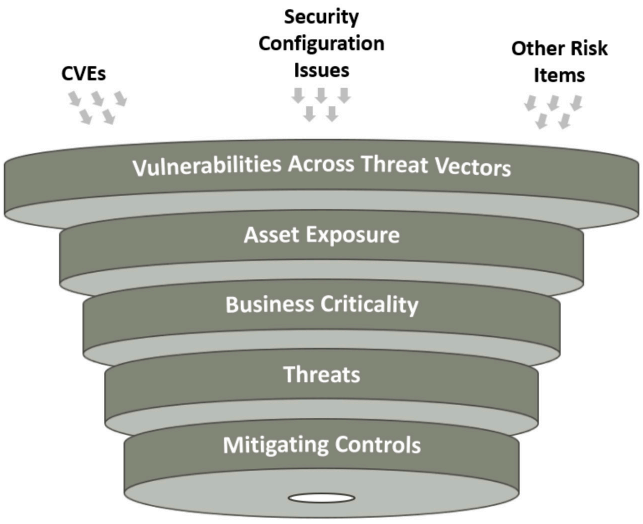


Ethan Volk

Bringing perspectives and investing in tech from both sides of the Atlantic

Keeping up with vulnerabilities feels like playing whack-a-mole — except the moles are multiplying and the hammer is manual remediation. Vulnerability solutions focus on spotting risks, assigning owners, and automating fixes, but here's the problem: more than half of vulnerabilities don't have a clear remediation path, and almost all remediations require at least some component of time-consuming, manual work. Meanwhile, attackers are moving faster than ever, exploiting critical flaws within five days, while security teams take weeks (or months) to patch[1]. An average enterprise spends 400+ hours per week on just vulnerability detection, remediation, and reporting[2]. Further, breaches now cost an average of $5 million[3].

Back in the early 2000s, vulnerability management was able to move at a slower pace. Security teams scanned software, found a few thousand vulnerabilities per year, and patched what they could. Fast-forward to today, and that number has exploded thanks to cloud migration, containers, and the never-ending flood of new assets. Security teams now must coordinate with IT, DevOps, and engineering teams while juggling misconfigurations, application security fixes, and infrastructure patching.



Vulnerability Remediation: Preventing and Fixing Gaps

Prioritization: For years, security teams relied on Common Vulnerability Scoring System (CVSS) scores to prioritize threats. Sounds logical, right? The problem is, CVSS wasn't designed to measure actual risk. A "high" score doesn't always mean immediate danger, while a "medium" score could be a hacker's golden ticket if it's actively exploited in the wild. And context matters — what may be a critical threat for one company might be a total non-issue for another.

1. https://zestsecurity.io/the-impact-cloud-risk-exposure-2025/
2. https://vulcan.io/resources/new-vulnerability-management-then-and-now-a-brief-history/
3. https://www.ibm.com/reports/data-breach

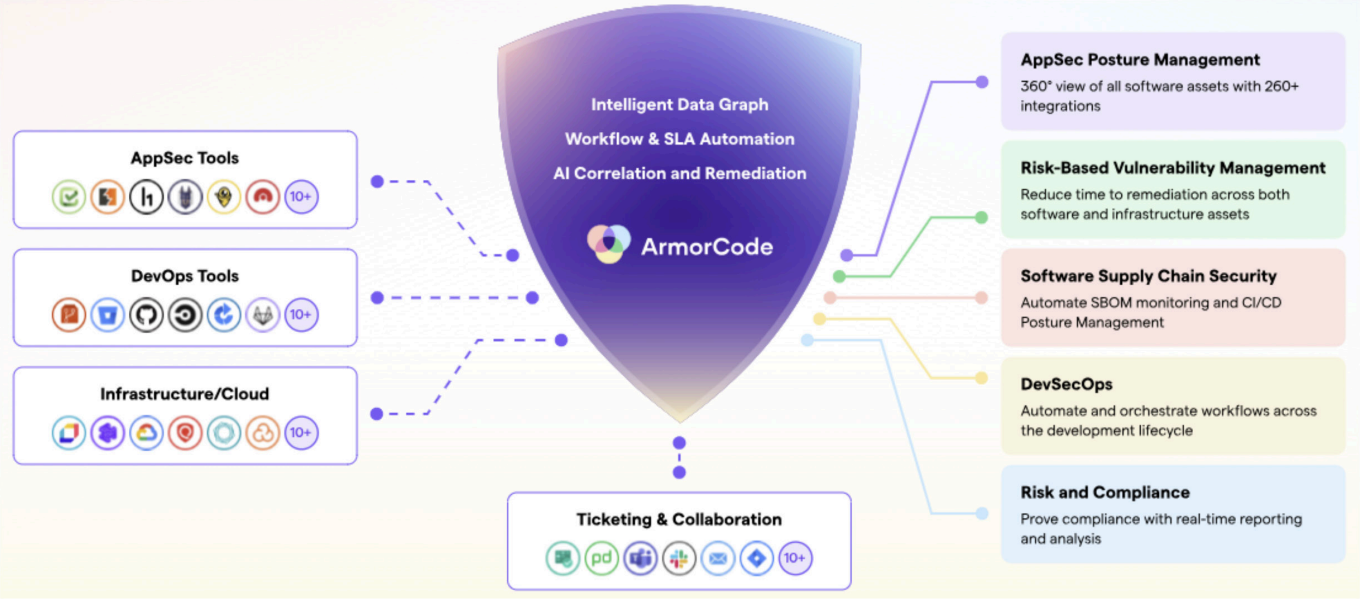
Patching and mitigating: Patching should be simple — see a problem, apply a fix, move on. However, vendor patches don't always play nice with every system, and sometimes fixing one issue creates a bigger one (like downtime). What if a critical business application is running on a legacy server that can't be patched? Now you're looking at a bigger decision: accept the risk, invest in a workaround, or go all-in on a system replacement.

The Evolution of Vulnerability Management

- **2000s:** First-gen tools like Qualys, Rapid7, and Tenable helped security teams find vulnerabilities for infrastructure, but the increasing number of assets resulted in a tidal wave of alerts
- **2010s:** Risk-based solutions like Balbix, Cyesec, and Kenna (now part of Cisco) stepped in to quantify risk and financial impact
- **Late 2010s:** Companies like Brinqa, Nucleus, and Vulcan (acquired by Tenable) started connecting the dots across infrastructure, applications, and cloud
- **Recently,** large players like Zscaler (acquiring Avalor) and Wiz (acquiring Dazz) are doubling down on contextual vulnerability data fabric solutions and automated cloud remediation workflows

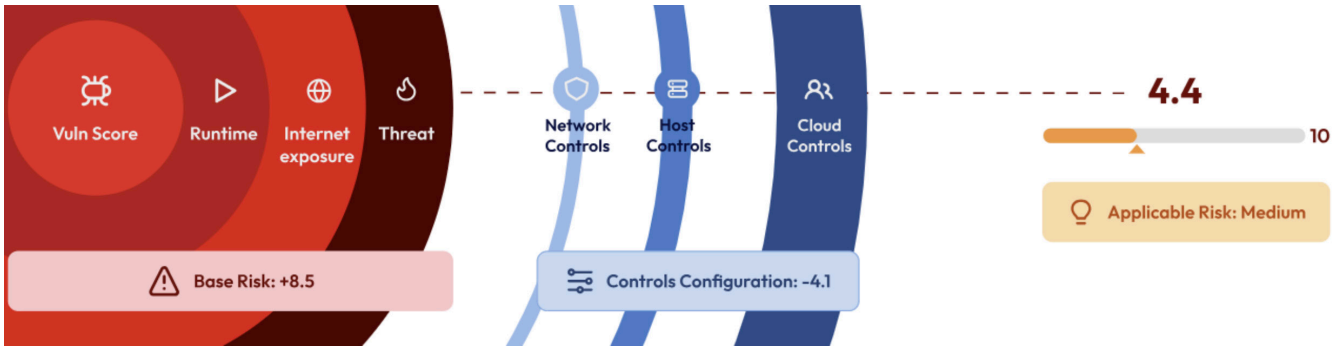
Market Opportunities and Considerations

Bridging the Security and DevSecOps gap: Security, engineering, and DevOps teams often don't have the same priorities. That's where Application Security Posture Management (ASPM) tools like ArmorCode, Apiiro, and Cycode come in. They pull vulnerabilities from code, infrastructure, and containers into one place, making it easier to automate security checks right inside a developer's workflow. Meanwhile, cloud misconfiguration tools like Gomboc help security teams enforce cloud policies through Infrastructure as Code (IaC).



Source: ArmorCode

Smarter attack path analysis and remediation pathways: Automated Security Control Assessment (ASCA) tools like Nagomi, Zafran, and Veriti help security teams focus on what matters. By mapping security tool configurations and correlating them with vulnerabilities, these tools prioritize the most critical fixes. Machine learning adds another layer — simulating attack paths, reducing false positives, and ensuring remediations won't cause more harm than good.



Source: Zafran

Remediation with AI Agents: Agentic remediation is one of the most exciting frontiers in vulnerability management, using planning and decision making AI agents to analyze risks, identify root causes, and act safely. While most teams are starting with low-risk automations, the potential for AI agents to handle even critical fixes is growing. Companies like Opus, Zest, and Averlon are leading the charge, developing agentic solutions that can make complex security decisions with minimal human intervention. As these technologies prove their stability and reliability, they could completely transform how security teams approach remediation.

Securing the Perimeter: Attack Surface Management and Next-Gen Pen Testing

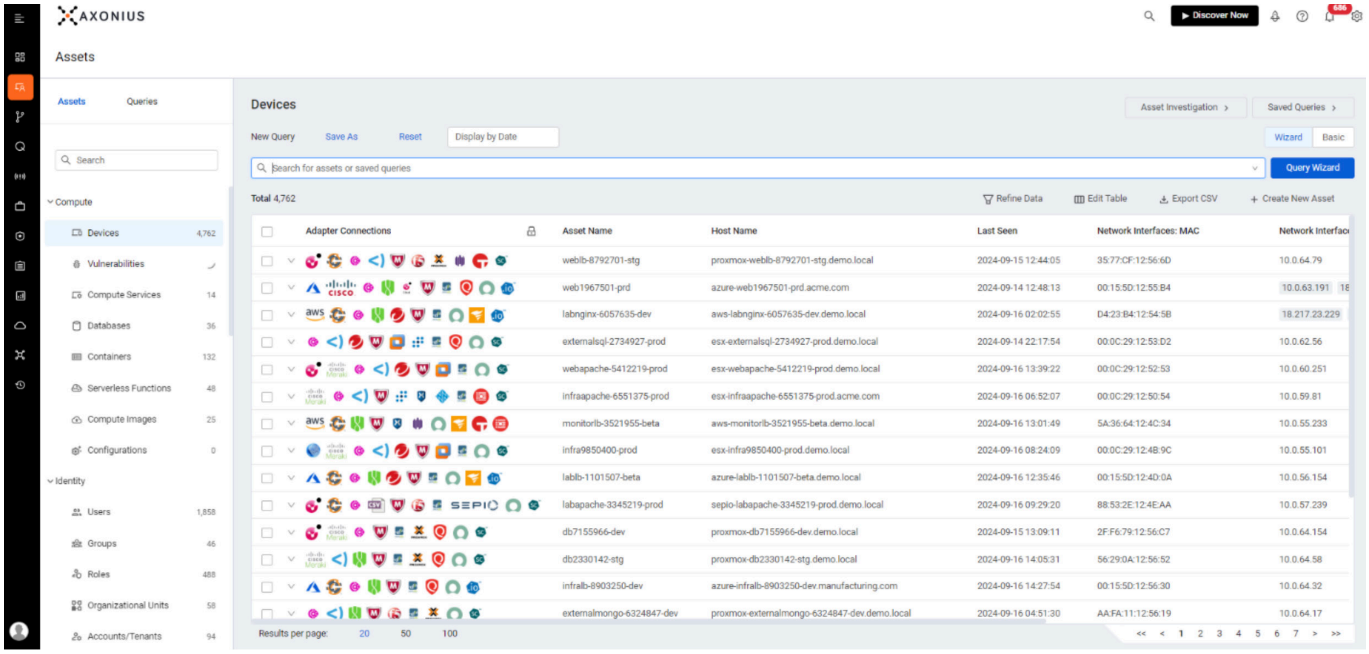
Attack Surface Management

SOC teams have become flooded with an increasing volume of alerts in part due to the increase in the attack surface. Historically, attack surface management was fragmented, manual, and reactive. Teams relied on spreadsheets, periodic audits (rather than continuous, real-time monitoring), and siloed tools to track assets and exposures. As companies shift applications, infrastructure, and identities from on-prem to the cloud, the IT attack surface is expanding dramatically, exposing the limitations of traditional approaches.

Modern attack surface management (ASM) spans three core capabilities:

1. **Cyber Asset Attack Surface Management (CAASM)** integrates with internal systems to provide a real-time, unified inventory of all assets and their security posture
2. **External Attack Surface Management (EASM)** identifies shadow IT, rogue infrastructure, and legacy systems that may not be tracked internally
3. **Digital Risk Protection Services (DRPS)** monitor the dark web, social media, and chat forums for signs of stolen credentials and leaked data

Several companies have entered the fold to provide modern approaches. JupiterOne offers a plug-and-play CAASM platform with a deep bench of out-of-the-box integrations. Its solution enhances asset visibility and security by providing a comprehensive inventory of assets and their interrelationships, along with automated workflows to quickly identify and remediate security gaps. Axonius also focuses on CAASM by integrating with hundreds of existing security and IT tools to build a unified, real-time inventory of all digital assets. Through their Adapter Network, Axonius integrates bi-directionally with over 1,200 IT systems, applications and data sources, creating a complete and continuous model of every asset within an organization.



Source: Axonius

Censys focuses on EASM, offering a platform that continuously scans the internet to identify exposed assets — both those an organization is aware of and those that may be unknown, such as shadow IT, rogue infrastructure, or legacy systems. The platform then maps these external assets to known vulnerabilities, misconfigurations, expired certificates, and outdated software, transforming broad internet scanning into actionable security intelligence.

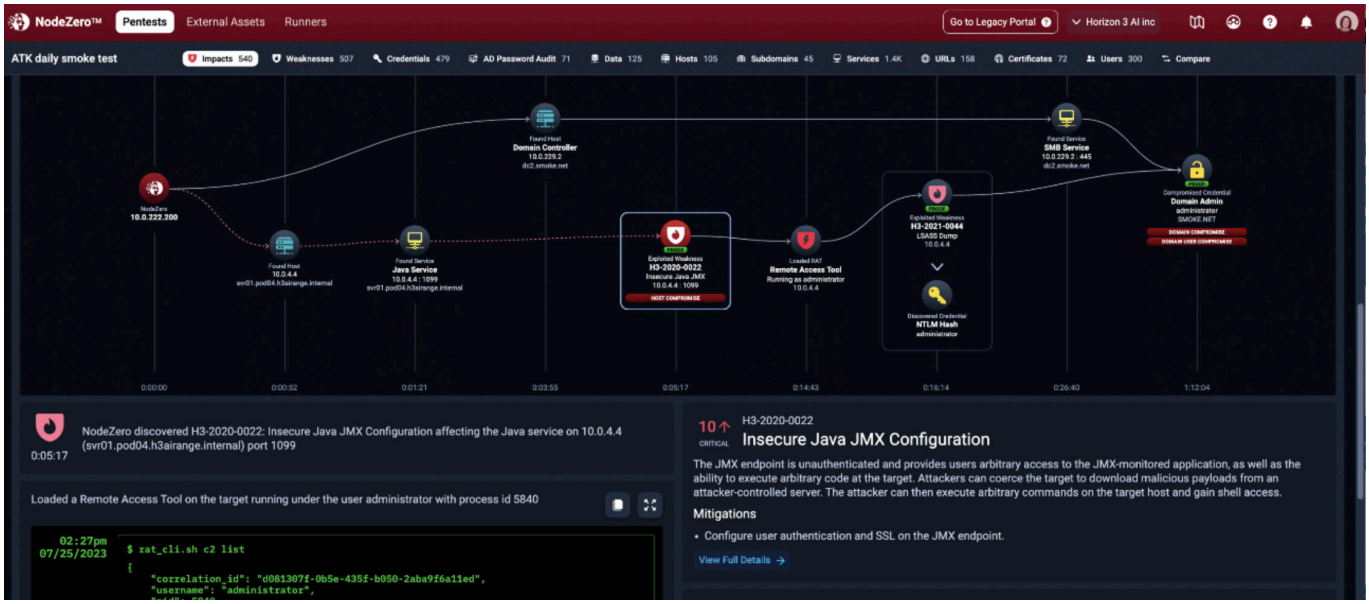
As an environment scales and spreads, continuous attack surface visibility — both internal and external —is a must-have for SOC teams looking to understand where threats may originate from.

Next-Gen Pen Testing

Penetration testing, or pen testing for short, can also be improved with modern approaches. Pen testing is a simulated cybersecurity exercise where experts attempt to identify and exploit security vulnerabilities. While effective, legacy approaches to pen testing have come with several drawbacks:

1. Assessments are based on a **snapshot in time** (often once or twice per year), providing a view into security posture at a specific moment
2. Service-driven pen testing is **resource intensive**, requiring teams of security professionals to plan, conduct and assess the pen test over the course of weeks
3. Pen tests are **expensive and don't scale** with growing infrastructure, meaning that organizations may be forced to choose which assets to test as opposed to testing the entire infrastructure

Modern approaches to pen testing aim to solve these limitations by providing faster, continuous, automated, scalable and integrated pen testing capabilities. For example, Pentera and Horizon3.ai focus on **automated penetration testing and security validation**, offering agentless platforms that simulate real-world attacker behavior across an organization's internal infrastructure. Meanwhile, companies like Hadrian are focused on autonomous pen testing from the perspective of an outside attacker. Using AI-driven red teaming, Hadrian helps organizations cut traditional red-team costs by 30% while avoiding false positives generated by other tools.



Source: Horizon3.ai

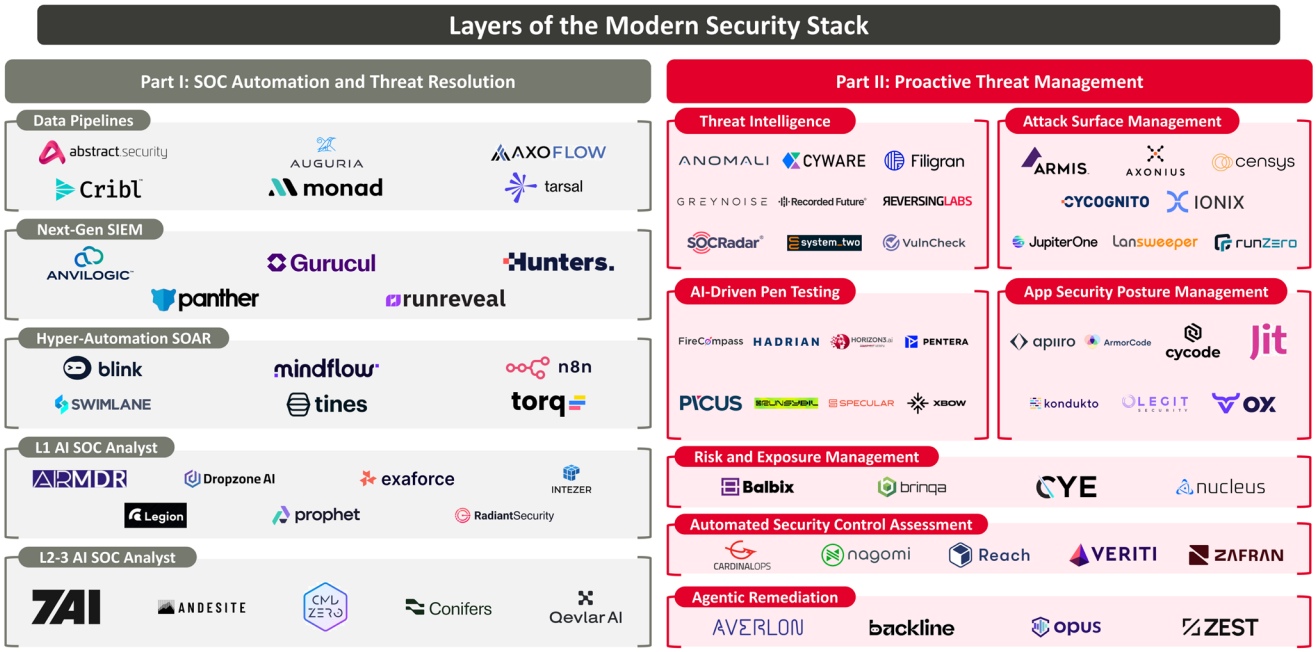
Meanwhile, Xbow and RunSybil are earlier stage pen testing platforms built with AI at their core. Xbow boosts offensive security with AI, autonomously finding and exploiting vulnerabilities in 75% of web benchmarks. Similarly, RunSybil offers an AI-driven pen tester with active defense capabilities, simulating attacker behavior and automating hacker intuition.

Together, these companies reflect a shift in the industry from point-in-time, human-driven pen tests to **continuous, intelligent, and scalable offensive security validation**, better aligned with how modern organizations build and operate their systems.

Conclusion

Despite multiple decades of progress and automation in cybersecurity, the SOC faces similar problems as they did 20+ years ago: too many alerts, too few people, and vulnerabilities that are too challenging to mitigate. As cyber defense systems become more sophisticated, so do the malicious actors. Fortunately, we believe the critical mass of innovators and thought leaders in the digital landscape are "good guys" developing creative solutions to cybersecurity rather than cybercriminals.

We see an exciting market opportunity for companies solving these problems and building the Next Gen SOC:



Logos sorted alphabetically. Illustrative and non-exhaustive lists.

At AVP, we are eager to partner with the people building next generation platforms that protect our data, physical infrastructure, and IT systems. If you are an early stage or growth stage company in this space, we would welcome an opportunity to meet with you.

You can reach out to jessica.hayes@avpcap.com, ethan.volk@avpcap.com, ethan.ellinger@avpcap.com, or connect with the rest of our colleagues at avpcap.com.

avpcap.com

Atlantic Vantage Point

Bringing perspectives and investing in tech
from both sides of the Atlantic

New York Paris London