

EXECUTIVE BRIEFING

AI Attacks Demand Better Vulnerability Management

There is a fundamental mismatch between the rate at which new vulnerabilities are discovered and how quickly security teams can address them. Security professionals find themselves drowning in exposure alerts, managing disparate scanning tools, and fighting an endless battle against risks they cannot effectively prioritize, remediate, and patch.

[According to the 2025 Unit 42 Global Incident Response Report](#), the median time from compromise to data exfiltration has contracted to as low as five hours, and adversaries can build attacks 100 times faster by operationalizing AI and automation. However, traditional vulnerability management remains built around reactive scanning and manual risk assessment frameworks that generate massive backlogs without providing clear guidance on which vulnerabilities truly matter.

Doubling down on reactive, manual, fragmented solutions isn't the way forward. Security teams need get a step ahead with proactive AI-driven exposure management.

100X
faster attacks
using AI and
automation.



The Vulnerability Management Crisis

The Remediation Speed Challenge

Vulnerability management teams often operate in environments where disconnected scanning tools and fragmented data repositories create massive backlogs in remediation efforts. Separate scanners for networks, endpoints, cloud environments, and applications each generate their own reports that must be manually correlated before remediation can begin.

Because of these silos, many organizations still track critical exposures in spreadsheets, requiring manual updates and approvals that can delay remediation by days or weeks, exactly the timeframe attackers need to successfully exploit these exposures. The inefficiency compounds when security teams attempt remediation without intelligent prioritization.

Organizations waste time and resources addressing low-risk exposures while critical, exploitable risks remain untouched. Security teams can spend weeks remediating hundreds of theoretical vulnerabilities only to discover that attackers exploited a different, higher-priority exposure that never made it to the top of their manual priority lists. This misdirection of remediation efforts not only wastes valuable security resources but also increases overall risk by creating a false sense of security while the most dangerous exposures persist in the environment.



5 HOURS
median time from
compromise to data
exfiltration.

The Automation Gap in Remediation Coverage

Even when organizations successfully identify critical exposures, traditional approaches create a critical coverage gap that only automation can solve. Legacy exposure management solutions identify thousands of exposures but lack the automated remediation capabilities needed to address them at scale. Manual remediation processes simply cannot keep pace with the volume of exposures discovered across modern attack surfaces, and security teams find themselves in a losing battle where new exposures are discovered faster than existing ones can be patched or remediated.

The result is a constantly growing backlog of unmitigated risks, where critical exposures may sit unremediated for weeks or months not due to oversight, but because manual processes cannot achieve the coverage required to address the full scope of discovered risks at the speed modern threats demand. This not only increases operational costs but also leads to analyst burnout and high turnover rates in an already challenging hiring market for cybersecurity professionals.

Strategic Misalignment in Risk Management

Perhaps more critically, ineffective vulnerability management creates strategic misalignment between security initiatives and business risk reduction. When security teams cannot demonstrate clear connections between vulnerability remediation activities and actual risk reduction, they struggle to secure adequate funding and executive support for necessary improvements. This misalignment becomes particularly problematic when organizations need to innovate and adopt new technologies but cannot confidently assess and manage the vulnerability implications.

The Need for Proactive Exposure Management

Leading industry analysts have recognized the critical need for organizations to transform their approach to vulnerability management and adopt proactive exposure management practices.

In ["Transform SecOps via Proactive Exposure Management and Threat Defense"](#), Gartner® notes: "Fragmented data pipelines, inadequate prioritization of critical information and lack of contextual insights are hampering cybersecurity programs. Security operations leaders should integrate exposure data and threat detection, investigation and response practices to improve resiliency and ROI."

Gartner survey data also shows that "An average of 73% of respondents who've implemented continuous threat exposure management (CTEM) perform better at detecting and responding to security incidents versus those who haven't yet implemented CTEM."

Gartner notes that "leveraging a SecOps data fabric powered by exposure data offers at least four key benefits, including the ability to:

- Enhance threat detection and data management processes
- Improve investigation accuracy and timeliness
- Optimize incident response functions
- Strengthen defenses by integrating exposure validation into TDIR practices"

Gartner also projects that "by 2028, organizations enriching SOC data with exposure information will enhance threat evaluation and accelerate incident response, reducing the frequency and impact of cyberattacks by 50%." We believe that this represents a fundamental shift in how organizations should approach vulnerability management.

“ By 2028, organizations enriching SOC data with exposure information will enhance threat evaluation and accelerate incident response, reducing the frequency and impact of cyberattacks by 50%.

— Gartner

Source - Gartner, Transform SecOps via Proactive Exposure Management and Threat Defense, Jonathan Nunez, Mitchell Schneider, 6 May 2025

Exposure Management with XSIAM 3.0

Transforming Vulnerability Management Through Unified Data and AI

Rather than treating vulnerability scanning, exposure management, and exposure remediation as separate domains, organizations need an integrated environment that provides security teams with an accurate inventory, clear prioritization, and automation tools to remediate vulnerabilities at scale with minimal human involvement. This means adopting a unified platform where exposure data continuously informs incident response, and threat intelligence continuously updates risk prioritization.



With a unified approach like Cortex Exposure Management, security teams gain comprehensive visibility into exposures across all environments through native scanning capabilities, use AI to cut through exposure noise by up to 99%, and identify which exposures have weaponized exploits and lack compensating controls. Most importantly, they can automatically deploy mitigating controls or patches for critical exposures, enabling immediate remediation before exploitation occurs.

AI-Driven Exposure Management: Precision Over Volume

The exposure management capabilities in XSIAM transform traditional risk assessment through three key innovations that address the pain points security teams face with overwhelming exposure backlogs.

Full Inside-Out and Outside-In Visibility Into Exposures: The platform provides comprehensive exposure visibility through a unified solution spanning native network, endpoint, and cloud scanners, extended with integration from any third-party exposure data source. This eliminates the blind spots and overlaps that exist when organizations rely on disparate scanning tools that don't communicate with each other, providing a complete picture of the organization's exposure landscape.

AI-Driven Prioritization Cuts Alert Noise by 99%:

Rather than overwhelming security teams with every possible exposure, XSIAM 3.0 uses advanced AI analytics to prioritize high-risk, exploitable exposures that are externally facing and lack compensating controls. The platform focuses on actual risk rather than compliance checkbox approaches, eliminating the false alarms that overwhelm security teams and prevent them from focusing on genuine exposures that could lead to compromise.



Industry-Leading Automation to Prevent Future Attacks: The platform closes the exposure management loop with automated remediation capabilities. Rather than simply identifying exposures and waiting for someone to eventually address them, XSIAM 3.0 seamlessly creates new compensating controls in native network, cloud, and endpoint solutions. It automates remediation, drastically reducing reliance on human intervention and traditional patching for routine exposure management tasks.

Integrated Threat Context for Exposure Prioritization

Unlike traditional risk assessment tools that operate in isolation, Cortex Exposure Management is deeply integrated with the XSIAM platform's threat detection and response functions.

When exposures are discovered through the platform's native scanning capabilities or integrated third-party tools, they are immediately enriched with threat intelligence context, data across threat vectors, business impact assessments, and compensating control analysis. This comprehensive view enables security teams to make informed decisions about remediation strategies based on actual risk rather than theoretical scores.

The Advantage of Proactive Exposure Management

Organizations that successfully implement proactive exposure management through platforms like XSIAM can proactively address exposures before exploitation, prioritize remediation efforts based on actual risk, and finally eliminate the backlog of unresolved exposures that plague most organizations today.

For security teams, this transformation means:

- Enhanced visibility across the complete exposure landscape
- The ability to proactively address exposures before exploitation
- Better prioritization of limited resources on genuinely exploitable exposures
- Increased efficiency through automation of routine tasks

For the broader business, proactive exposure management:

- Reduces business disruption from cyberattacks
- Lowers remediation costs through early intervention and automated controls
- Improves regulatory compliance through comprehensive risk management
- Enhances ability to innovate and adopt new technologies securely



“73% of organizations saw improvement in detection and response metrics after implementing continuous threat exposure management.”

— Gartner

Conclusion

The cybersecurity industry stands at a critical point in vulnerability management. Traditional approaches based on reactive scanning, manual prioritization, and fragmented tools are no longer sufficient against AI-powered attacks that exploit exposures at machine speed. Organizations that continue to operate with overwhelming exposure backlogs, disconnected scanning tools, and manual remediation processes will find themselves increasingly disadvantaged.

Cortex Exposure Management represents more than just another risk scanner—it embodies a fundamental transformation in how organizations can approach exposure management. By unifying vulnerability scanning, exposure management and remediation in a single platform driven by AI and automation, organizations can finally move from constantly playing catch-up with exposure backlogs to proactively managing their risk landscape.

The path forward is clear: The future belongs to organizations that can consolidate their vulnerability management approaches, leverage unified data and AI-driven insights, and operate risk assessment as a proactive, automated function rather than a reactive scanning process. For security professionals tired of fighting an endless battle with overwhelming exposure backlogs and unclear prioritization, Cortex Exposure Management offers the opportunity to transform their risk programs and regain the advantage in the fight against increasingly sophisticated cyberthreats.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <http://www.paloaltonetworks.com/company/trademarks.html>

All other marks mentioned herein may be trademarks of their respective companies.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.