EXECUTIVE BRIEFING

Why Traditional Vulnerability Management Leaves Organizations Exposed to AI-Powered Attacks

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.

The median time from compromise to data exfiltration has contracted to as low as 5 hours, and adversaries can build attacks 100 times faster by operationalizing AI and automation.[1] 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 matter.

The answer does not lie in adding more tools to an already fragmented stack, but in fundamentally transforming how organizations approach vulnerability management. Security teams need to match speed with AI-driven exposure management and intelligent prioritization so they can stay ahead of increasingly sophisticated threats rather than always being one step behind.

100X
faster attacks using AI and automation.

1. *2025 Unit 42 Global Incident Response Report*, Palo Alto Networks Unit 42, February 2025.

Quantified Impact of Modern Exposure Management

A Forrester® Consulting Total Economic Impact™ (TEI™) study commissioned by Palo Alto Networks found that organizations deploying AI-driven security platforms achieved significant risk reduction and operational efficiency:[2]

60% improvement in security posture, valued at **$2.2** million over three years.

85% reduction in mean time to remediation (MTTR).

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 teams must manually correlate before remediation can begin.

5 HOURS
median time from compromise to data exfiltration.[3]

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 time frame that 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 both wastes valuable security resources and increases overall risk by creating a false sense of security while the most dangerous exposures persist in the environment.

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 cannot keep pace with the volume of exposures discovered across modern attack surfaces. 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 continuous growing backlog of unmitigated risks. It's where critical exposures might sit unremediated for weeks or months but not due to oversight. Rather, it's because manual processes cannot achieve the coverage required to address the full scope of discovered risks at the speed modern threats demand. This both increases operational costs and leads to analyst burnout and high turnover rates in an already challenging hiring market for cybersecurity professionals.

Research demonstrates the financial impact of this automation gap. According to the Forrester TEI™ study, Forrester researchers interviewed organizations that deployed Palo Alto Networks AI-driven platforms with automated remediation capabilities. The study reports that these organizations achieved $1.5 million in productivity value over three years through enhanced case management, with 70% fewer incidents requiring manual investigation.[4]

2. *The Total Economic Impact™ Of Palo Alto Networks Cortex XSIAM*, a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, October 27, 2025. Results are for a composite organization based on interviewed customers.
3. Palo Alto Networks Unit 42, *Global Incident Response Report.*
4. A commissioned study by Forrester Consulting on behalf of Palo Alto Networks, *The Total Economic Impact™*. Results are for a composite organization based on interviewed customers.

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:[5] "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."

Survey data from the Gartner study indicates: "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 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 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

5. *Transform SecOps via Proactive Exposure Management and Threat Defense*, Jonathan Nunez and Mitchell Schneider, Gartner, May 6, 2025. This source applies to all data provided in this section.

Cortex XSIAM 3.0 Exposure Management: A New Paradigm for Risk Assessment

Transforming Vulnerability Management Through Unified Data and AI

Vulnerability scanning, exposure management, and exposure remediation are not separate domains and should not be treated that way. Instead, 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. They use AI to cut through exposure noise by up to 99% and identify which exposures have weaponized exploits and lack compensating controls.

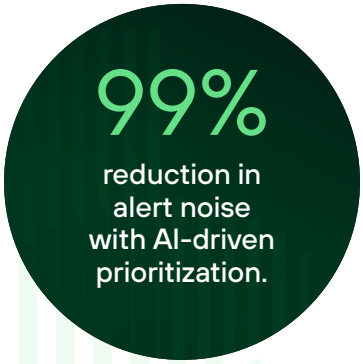
In the Forrester TEI™ study, interviewed organizations consolidating more than 20 disparate security tools into Palo Alto Networks unified platform saved $3.1 million over three years.[7] Most importantly, they can now automatically deploy mitigating controls or patches for critical exposures, enabling immediate remediation before exploitation occurs.

AI-Driven Exposure Management: Precision Over Volume

The exposure management capabilities in Cortex 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, Cortex 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.

6. *Migrating legacy SIEMs to a cloud-native analytical platform*, S&P Global 451 Research, November 7, 2024.
7. A commissioned study by Forrester Consulting on behalf of Palo Alto Networks, *Total Economic Impact*™. Results are for a composite organization based on interviewed customers.

Proven Efficiency Gains

Research shows that AI-driven SOC platforms can reduce alert volumes by **85% by year three**, saving over **$930,000** in triage and Tier 1 operations while allowing security teams to focus on genuine threats.[8]

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, Cortex 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 Cortex 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 Cortex XSIAM can proactively address exposures before exploitation, prioritize remediation efforts based on actual risk, and 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 the ability to innovate and adopt new technologies securely.

> "73% of organizations saw improvement in detection and response metrics after implementing continuous threat exposure management.[9]"
>
> — Gartner

8. A commissioned study by Forrester Consulting on behalf of Palo Alto Networks, *The Total Economic Impact™*.
9. Gartner, *Proactive Exposure Management.*

Real-World ROI: Forrester TEI™ Study Results

In the Forrester TEI™ study, Forrester researchers interviewed organizations that transformed their exposure management approach with AI-driven platforms, achieving measurable outcomes:[10]

- **257% ROI** over three years with **less than 6 months** payback period.
- **$5.6M net present value** from operational improvements and cost savings.
- **$3.1M saved** from tool consolidation and reduced operational overhead.
- **60% improvement** in overall security posture, valued at **$2.2M** in reduced breach risk.

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 to backlogs, disconnected scanning tools, and manual remediation processes will find themselves increasingly disadvantaged.

Cortex Exposure Management goes beyond being another risk scanner to embody 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 repeatedly 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.

The business case for this transformation is also clear. As the Forrester TEI™ study points out, a composite organization based on interviewed customers that deployed unified, AI-driven exposure management platforms achieved 257% ROI over three years. They also gained measurable improvements in security posture, operational efficiency, and cost reduction. To learn more about the quantified business impact of modern exposure management, read the full Forrester Consulting Total Economic Impact™ study.

DOWNLOAD THE STUDY

About Cortex

Cortex by Palo Alto Networks has redefined solutions for security operations to help organizations deliver the modern security operation center (SOC) experience. Cortex delivers best-in-class threat detection, prevention, attack surface management, and security automation in an integrated platform powered by machine learning and Unit 42® threat intelligence. Trusted by companies around the world and recognized by leading analyst firms, Cortex XDR®, Cortex XSOAR®, Cortex Xpanse®, and Cortex XSIAM provide proven protection as standalone solutions and also work seamlessly together as a force multiplier across the SOC. To learn more about Cortex, visit www.paloaltonetworks.com/cortex.

10. A commissioned study by Forrester Consulting on behalf of Palo Alto Networks, *Total Economic Impact™*. Results are for a composite organization based on interviewed customers.

paloalto® NETWORKS

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

cortex_traditional-vulnerability-management_111125