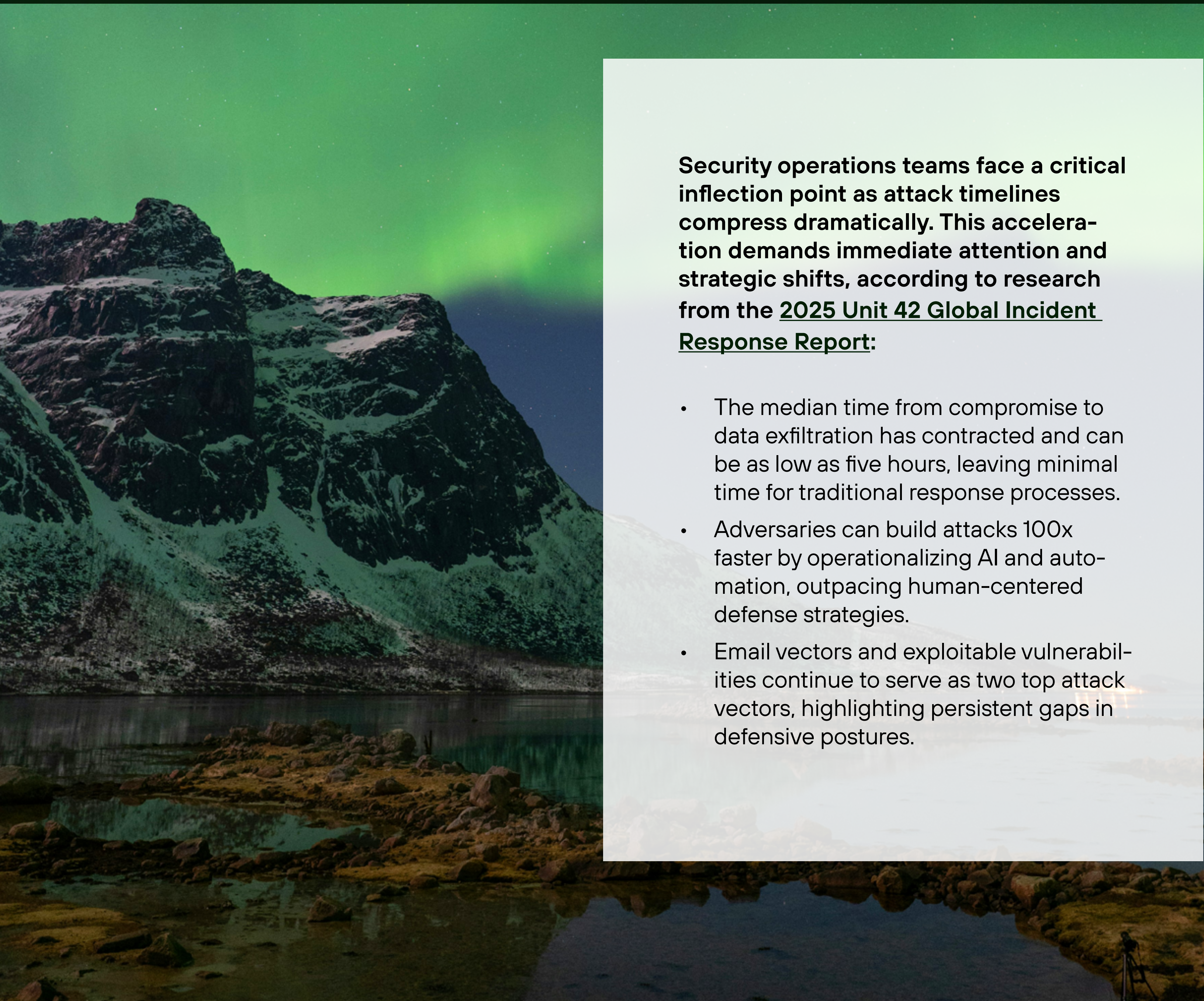
paloalto NETWORKS | CORTEX

EXECUTIVE ADVISORY

Unifying Reactive and Proactive Cybersecurity

Why Security Approaches Must Adapt Now



Security operations teams face a critical inflection point as attack timelines compress dramatically. This acceleration demands immediate attention and strategic shifts, according to research from the 2025 Unit 42 Global Incident Response Report:

- The median time from compromise to data exfiltration has contracted and can be as low as five hours, leaving minimal time for traditional response processes.
- Adversaries can build attacks 100x faster by operationalizing AI and automation, outpacing human-centered defense strategies.
- Email vectors and exploitable vulnerabilities continue to serve as two top attack vectors, highlighting persistent gaps in defensive postures.

Security professionals recognize the limitations of fragmented tools and siloed data repositories in this environment. The conventional security model—fundamentally designed as a detection and response framework—is increasingly insufficient against coordinated, multi-vector attacks that move at machine speed. Organizations that fail to adapt risk finding themselves perpetually one step behind increasingly efficient threat actors. To gain and maintain advantage, security teams must shift from merely reacting to threats after they've materialized to proactively identifying and addressing potential attack vectors before adversaries can exploit them.

Challenges Facing Security Leaders

Security executives face mounting pressures that traditional approaches cannot resolve:

Fragmented Security Architecture

Organizations have historically approached security with a fundamental divide between two distinct domains: proactive security (vulnerability management, security posture assessment, compliance) and reactive security (threat detection, incident response, SIEM/EDR/XDR). This artificial separation results in disjointed tools, teams, and processes that fail to address the reality that adversaries operate seamlessly across this divide. By treating peacetime readiness and wartime response as separate concerns, organizations miss the critical connections between exploitable vulnerabilities and active threat campaigns. This fragmentation manifests in several ways:

- **Disparate Data and Tools:** SIEM, EDR/XDR, network monitoring, cloud security, and identity management systems operate in silos, creating disconnected data repositories that limit comprehensive visibility across the attack surface.
- **Ineffective Detection:** Security teams contend with overwhelming alert volumes, high false positive rates, and significant blind spots that allow sophisticated threats to bypass detection controls.
- **Separate Cloud Security Tools:** Cloud security posture management (CSPM), cloud workload protection (CWPP), and cloud infrastructure entitlement management (CIEM) tools operate independently from on-premises security monitoring.
- **Disconnected Identity Solutions:** Identity threat detection and response (ITDR) platforms have limited integration with endpoint or network security, despite identity being a critical attack pathway.
- **Inefficient Incident Response:** Security operations rely on slow, manual, labor-intensive processes across disconnected systems, with analysts piecing together attack timelines from disparate sources and coordinating response actions across multiple interfaces.

Vulnerability Overload

The security industry faces a fundamental challenge with traditional vulnerability management approaches. Organizations are overwhelmed by an ever-growing volume of potential exposures across expanding attack surfaces, yet our research shows only less than 1% of these vulnerabilities are are weaponized and even fewer are externally facing and have no compensating controls. This extreme disparity creates an impossible prioritization problem for security teams, who find themselves buried under massive vulnerability backlogs with no clear way to identify which handful truly require immediate attention. Traditional vulnerability management tools compound the problem by generating alerts for every potential weakness rather than focusing teams on truly exploitable vulnerabilities that pose actual risk.

Email Security Integration

With nearly 5 billion email users projected by 2030, email remains the primary business communication channel—and a significant vector for initial access. A quarter of security incidents begin with email-based threats, yet traditional email security solutions typically operate in isolation from broader security operations. This separation creates visibility gaps in attack chain analysis and limits the effectiveness of both email security and broader threat detection efforts.

This tool proliferation prevents security teams from building proactive defenses by consuming resources that could be directed toward prevention. Rather than getting ahead of threats, security personnel spend their time navigating multiple systems, manually correlating alerts across disparate tools, and struggling to identify which vulnerabilities to prioritize before attackers exploit them. The inability to see connections between potentially exploitable vulnerabilities and emerging threat indicators until after an attack is underway represents a fundamental barrier to truly proactive security.

The Peacetime vs. Wartime Divide

Most concerning is the artificial division between “peacetime” security (vulnerability management, compliance, posture assessment) and “wartime” security (threat detection, incident response).

Security operations today often resemble a patchwork quilt - siloed tools that don’t communicate with each other, physically separated teams working in isolation with misaligned processes, heavy reliance on legacy systems that can’t keep pace with modern threats, and archaic practices like tracking critical vulnerabilities in spreadsheets instead of integrated platforms that enable automated remediation. This separation creates blind spots exactly where adversaries operate—at the intersection between preventable vulnerabilities and active exploitation.

Breaking Down Silos: Essential Elements of Integrated Security

In the current environment, security teams are fighting sophisticated threats with disjointed tools. They manually correlate alerts across disconnected consoles, struggle to prioritize thousands of vulnerabilities, and race against shrinking response timeframes with insufficient context. This fragmentation isn't sustainable.

Four critical elements can transform this fragmented approach into effective security operations:

1. **Unified Data:** Comprehensive security data from across the enterprise—email, endpoints, network. identity, cloud, and vulnerabilities—must form the foundation of both proactive and reactive security operations.
2. **AI-Driven Analytics:** Advanced AI and LLMs must continuously analyze this data to identify patterns, prioritize risks, and predict emerging threats before they can be exploited.
3. **End-to-End Automation:** Automated workflows must span the entire security lifecycle—from vulnerability discovery to incident response—to match the speed of today's attacks.
4. **Breaking Down the Peacetime/Wartime Divide:** Security operations must integrate proactive measures and reactive capabilities in a single platform, bringing wartime security to peacetime operations.

The Path Forward: Unifying Proactive and Reactive Security

To effectively combat today's threats, organizations must fundamentally transform their security operations model by bringing together critical capabilities that have traditionally existed in isolation:

1. A Single Source of Truth

These capabilities must operate on a unified platform that:

- Ingests relevant data once and continuously analyzes it against new attacks and capabilities
- Detects and stops attacks in real-time by correlating threats across all vectors
- Automates response actions to contain threats within minutes rather than days
- Provides continuous, real-time visibility into active threats and ongoing attacks

2. Proactive Exposure Management

Organizations need to move beyond traditional vulnerability scanning to comprehensive exposure management that:

- Provides complete visibility into assets and vulnerabilities across all environments
- Uses AI to cut through the noise, reducing vulnerability alerts by up to 99%
- Identifies which vulnerabilities have weaponized exploits and lack compensating controls
- Automatically deploys mitigating controls or patches for critical vulnerabilities
- Enables immediate remediation of critical vulnerabilities before they can be exploited

3. Integrated Email Detection & Response

Email security must evolve from standalone filtering to become an integral part of security operations:

- Correlating email threats with identity, endpoint, and network activity
- Using advanced behavioral analysis and LLMs to detect sophisticated phishing
- Automating response actions, including removing malicious emails and isolating affected endpoints
- Providing full attack chain visibility from initial email to potential impact

The Benefits of Unification: Transforming Security Operations

Organizations that successfully unify proactive and reactive security realize significant benefits:

For CISOs:

Reduced risk exposure through comprehensive visibility and control

Lower operational costs by replacing multiple point products

Better alignment between security and business objectives

Improved ability to demonstrate security effectiveness to the board

For Security Teams:

Enhanced visibility across the full attack chain

Ability to proactively address vulnerabilities before exploitation

Better prioritization of limited resources on genuine threats

Increased efficiency through automation of routine tasks

For the Business:

Reduced likelihood of business disruption from cyberattacks

Lower remediation costs through early intervention

Improved regulatory compliance through comprehensive security controls

Enhanced ability to innovate and adopt new technologies securely

Looking Ahead: The Future of AI-Driven Security Operations with XSIAM 3.0

The future belongs to organizations that can unify their security operations across the entire lifecycle—from proactive exposure management to reactive threat detection and response. This unified approach is essential for defending against today's increasingly sophisticated, AI-powered threats.

By breaking down the artificial divide between peacetime and wartime security, organizations can regain the advantage in the fight against cybercriminals. The time to make this transformation is now, before the next generation of AI-powered attacks further accelerates the threat landscape.

For the first time, security teams have the opportunity to gain a decisive advantage over adversaries. With unified security operations that span both proactive and reactive capabilities, organizations can finally eliminate their backlog of vulnerabilities, confidently defend against AI-powered email attacks, and respond to threats at machine speed. The path forward is clear: by adopting more unified, proactive, and automated security approaches, teams can transform from constantly playing catch-up to consistently staying one step ahead.

Cortex XSIAM 3.0 delivers precisely these capabilities as the world's #1 AI-driven SecOps platform. It combines Cortex Advanced Email Security and Cortex Exposure Management, evolving security operations from reactive response to proactive defense. By cutting vulnerability noise by up to 99% through AI-driven prioritization and stopping advanced email threats with LLM-powered analytics, XSIAM 3.0 provides the only comprehensive security platform you'll ever need for both proactive and reactive security.

Request a Demo of Cortex XSIAM.

LEARN MORE

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