Endpoint First: Charting the Course to AI-Driven Security Operations

1 Executive Summary

Security operations teams that rely on siloed security tools experience faster-moving cyberattacks than defenders can respond to them. These teams face the stark reality of dealing with thousands of low-context alerts, burning cycles on manual detection, and attackers flying under the radar while analysts piece together what's going on.

Securing siloed architectures demands a new, disruptive approach—a unified security operations platform anchored at the endpoint. This platform uses a high-precision endpoint agent that handles blocking and gathering comprehensive endpoint telemetry, the richest source of attack intelligence. It also expands to network, cloud, identity, and email data. With this broad context, organizations can achieve the visibility, detection, and response required to counter modern threats.

This endpoint-first transformation meets organizations wherever they are on their security maturity journey, from resource-constrained IT teams seeking simple, out-of-the-box protection to mature enterprises building AI-driven SOCs. By adopting this approach, organizations see measurable improvements in detection accuracy, response speed (minutes vs. days), and operational efficiency with adaptive defenses that evolve as threats change.

Learn how an endpoint-first architecture unifies visibility, automates detection, and enables response at machine speed. And see how it delivers measurable results for both resource-constrained teams and mature enterprises ready to build the AI-driven SOC of tomorrow.

2 | The Failing Paradigm of Siloed Security Operations

The gap between attack speed and detection capability has never been wider. Legacy security architectures built on isolated tools simply cannot provide the unified visibility and response speed required to stop today's threats.

The Modern Threat Landscape

Attacks are fast—measured in hours, not days. This speed and complexity create a significant challenge for security teams. They need data from multiple domains to see an attack unfold and make sense of it all at an exponentially faster pace.

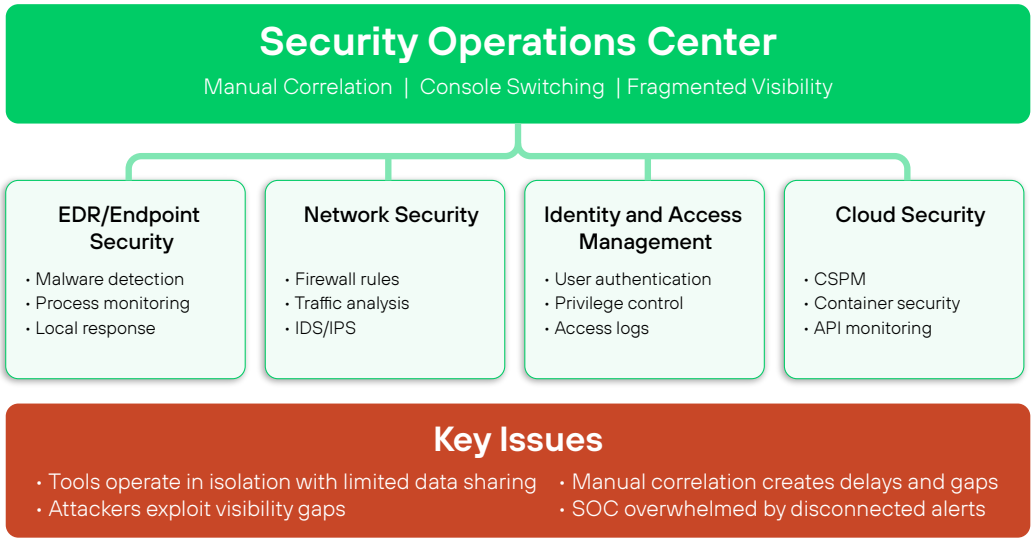

Figure 1. Traditional siloed security architecture

Weakness of an Isolated Approach

Traditional endpoint detection and response (EDR), firewalls, and cloud security tools operate in silos. Also, legacy SIEMs lack the machine-speed detection needed to keep pace with evolving threats. The results of this approach are the alert fatigue and incomplete visibility that analysts experience.

Alert Fatigue

Analysts are flooded with thousands of individual, low-context alerts from a high volume of low-fidelity sources. They struggle to distinguish the signal from the noise, making it take too long to address critical alters. The traditional SOC model was built around the human analyst, requiring security teams to pore through hundreds of alerts per day, only to spend the bulk of their time, however, on false positives.

Incomplete Visibility

An alert on the endpoint lacks context from the network or identity sources, and vice versa. Analysts must manually stitch together the story, either in the SIEM or across disparate tools, which can be slow and error-prone.

A Modern Unified Approach

To effectively counter sophisticated threats, organizations must build a security architecture on a foundation of unified data, starting at the primary point of attack—the endpoint. As data and alert volume grow, the human-led approach breaks down, requiring a fundamental shift toward AI-driven security operations.

3 The Foundation: A High-Precision Agent

Multilayered, AI-Driven Prevention

The ability to stop threats in real time is the most important function. It requires a robust set of defenses operating on the endpoint itself. Leading solutions leverage insight from tens of thousands of global customers to continuously train AI models on the latest attack behaviors. This approach enables real-time blocking of sophisticated threats. Rigorously tested capabilities work immediately upon deployment, combining efficacy with accuracy, preventing both known malware and novel attack techniques without requiring extensive tuning or baseline periods.

For example, this type of prevention proactively blocks attempts to exploit software vulnerabilities (e.g., on a web server) before malicious code can execute, effectively neutralizing zero-day threats at the initial point of entry.

Unbroken Stream of Rich Telemetry

The next equally important function is having a primary sensor for the entire security operations platform. The agent must continuously collect and stream deep endpoint activity data from process execution, network connections, file activity, registry changes, and user actions. This data is the fuel for all advanced detection, investigation, and response.

Leading solutions collect a broad range of telemetry from endpoints, building contextual intelligence that enables highly accurate security analytics to detect threats at machine speed. Additionally, leading platforms have demonstrated exceptional detection capabilities in independent evaluations, like MITRE ATT&CK® assessments, with top performers achieving perfect technique-level detection scores on their first attempt.

4 From Data to Decisions: The Power of a Unified Analytics Platform

Security teams can turn raw data from endpoints and other sources into actionable intelligence that transforms both SecOps economics and effectiveness.

Cross-Domain Data Ingestion

Endpoint telemetry serves as the starting point, but effective extended detection and response (XDR) requires fusing this data with signals from other important security domains to create holistic threat visibility. XDR platforms automatically correlate endpoint data with information from across the security infrastructure to accurately detect attacks and simplify investigations:

- **Networks**, such as firewalls, network traffic analysis, and DNS logs.
- **Identity and access management (IAM)**, such as Active Directory, cloud IAM, and authentication systems.
- **Cloud infrastructure**, such as cloud provider logs, container runtime data, and serverless environments.
- **SaaS applications**, such as productivity suites and collaboration tools.
- **Email**, such as cloud-based email services.

This data integration approach addresses one of the fundamental challenges that SOCs face—organizations often deploy dozens of security tools, yet responding to a single incident requires coordinating data and actions across many of them. By unifying these disparate data sources, XDR platforms eliminate blind spots and provide the cross-domain visibility needed to detect evasive threats that siloed endpoint, network, and cloud detection and response tools miss.

Ingesting cross-domain data enables security teams to understand the complete attack lifecycle rather than investigating isolated events, helping transform fragmented security operations into a cohesive defense strategy.

Core AI-Driven Capabilities

The unified data foundation enables comprehensive threat detection and response. Beginning with deep endpoint telemetry and extended data sources, thousands of machine learning (ML)-driven detectors continuously evaluate incoming data to uncover the full scope of advanced attacks that evade traditional signature-based defenses. This ML-first approach handles the majority of threat detection, enabling security analysts to focus on validation, advanced threat hunting, and remediation.

Intelligent Incident Management

XDR platforms leverage ML to automatically correlate related security events into unified incidents, eliminating the manual work that consumes analyst time. Every detection related to the same attack is grouped into a single case, revealing the complete, connected story. The story is made possible through shared artifacts (file hashes and IP addresses), causality chains (process A launched process B), and temporal analysis of related events. This capability shift moves security teams from reactive alert processing to proactive threat investigation.

Risk-Based Prioritization

Automated risk scoring enables security teams to focus resources on the threats that pose the greatest business risk. Incidents are scored based on the cumulative set of issues within them. Multiple factors are evaluated, including the detection of multiple alert types, activity across multiple data sources, and the statistical rarity of observed files or behaviors compared to organizational and global baselines. By considering the affected systems, user privileges, and attack sophistication, XDR ensures that high-impact threats receive immediate attention.

Operational Intelligence

Visual attack timelines and root cause analysis accelerate incident response while providing the documentation needed for compliance reporting and stakeholder communication. XDR platforms map events to standard frameworks, like MITRE ATT&CK, to provide a common language and understanding of attacker techniques. This method enables security leaders to gain clear visibility into attack progression and business impact. With predefined automation playbooks and quick actions, analysts can remediate threats in minutes rather than hours.

5 Cortex XDR: Endpoint-First Architecture in Practice

The principles of unified security operations and AI-driven detection provide the strategic framework for modern threat defense. Cortex XDR® exemplifies this endpoint-first approach, translating these foundational concepts into measurable security outcomes.

The following scenarios demonstrate how the Cortex XDR endpoint-centric security architecture handles different attack vectors and enables security teams to understand and respond to complex threats.

Scenario A: Advanced Endpoint Threat (Ransomware)

Attack Path

An attacker exploits a web server vulnerability, uses PowerShell for execution, drops a malicious script, and attempts to encrypt files.

Business Challenge

The global average cost of a data breach is $4.44 million, while ransomware attacks specifically averaged $5.08 million when disclosed by attackers.[1]

Traditional Response

Multiple disconnected alerts occur across EDR, network monitoring, and file security tools. Security teams spend 45–60 minutes correlating events while the attack progresses to often achieve successful encryption and business disruption.

Ideal Response

- **Prevention:** The Exploit Protection Module in Cortex XDR blocks the initial attack at the web server.
- **Detection and investigation:** If the module is set to detect-only mode, Cortex XDR collects data at each step. The causality view shows the entire chain: IIS process → cmd.exe → cscript.exe → ransomware.exe. Analysts can see encoded commands and identify attack vectors for future prevention with instant root cause analysis.

Business Value

Cortex XDR reduced the mean time to detect (MTTD) and mean time to respond (MTTR) from hours to minutes, preventing business disruption and eliminating recovery costs. The automated response capabilities help isolate threats before they spread across the network.

1. *Cost of a Data Breach 2025: The AI Oversight Gap*, IBM and Ponemon Institute, July 30, 2025.

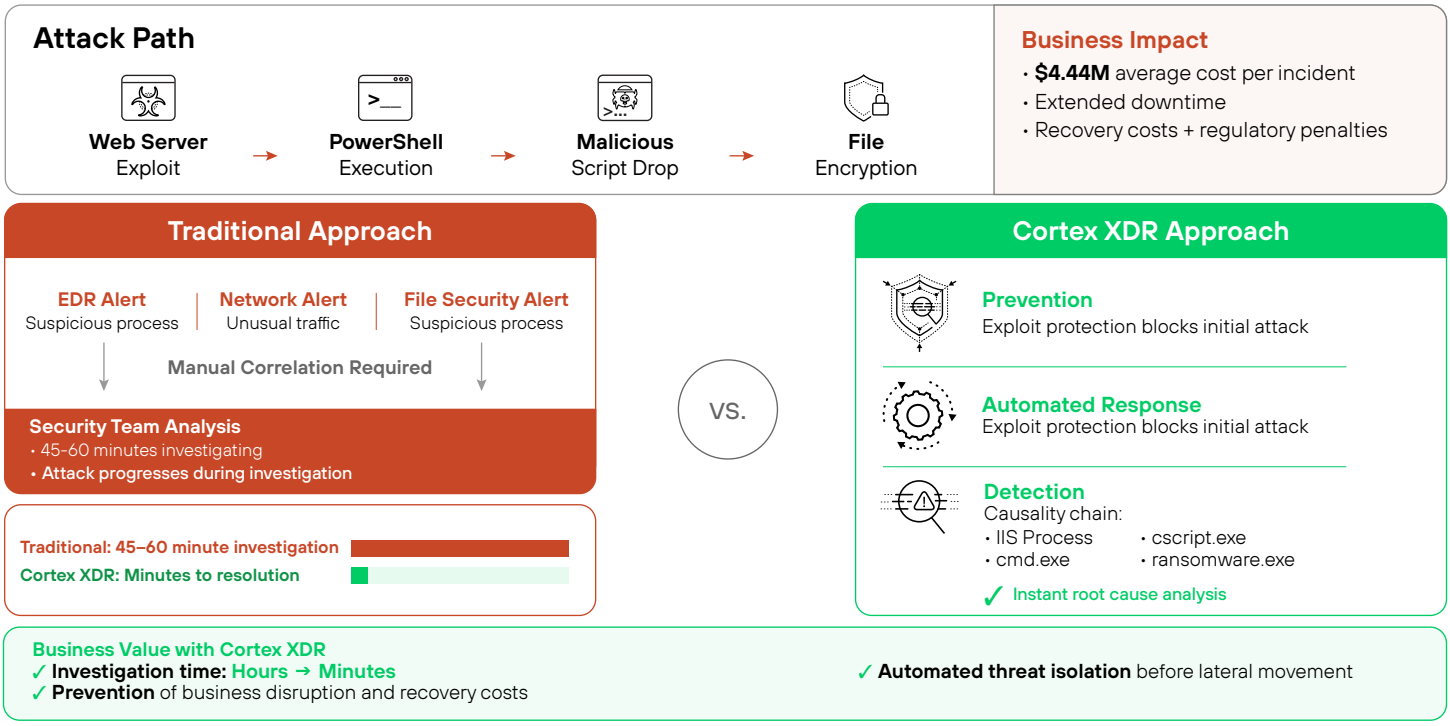

Figure 2. Scenario A: Advanced endpoint threat (ransomware)

Scenario B: Cloud-Native Breach

Attack Path

An attacker exploits a web application in a container, gains access to the cloud provider account, creates new identities for persistence, and exfiltrates data from a storage bucket.

Business Challenge

Data breaches involving multiple environments (including cloud) average $5.05 million in damages, with attackers often gaining access to multiple cloud services and data repositories.[2]

Traditional Response

Siloed alerts from container security, cloud access logs, and network monitoring create visibility gaps. Security teams struggle to connect container compromises with subsequent cloud account takeovers, allowing attackers to establish persistence and exfiltrate data.

Ideal Response

In Cortex XDR, the analyst sees a single case that shows the webshell execution, subsequent credential access using extracted container secrets, new IAM users created for persistence, and anomalous access to cloud storage buckets. Security leaders gain complete visibility into the attack scope across hybrid infrastructure.

Business Value

Faster containment reduces data exposure and regulatory compliance costs. Clear visibility into the cloud attack progression enables more effective incident response and business risk assessment.

2. IBM and Ponemon Institute, *Cost of a Data Breach Report*.

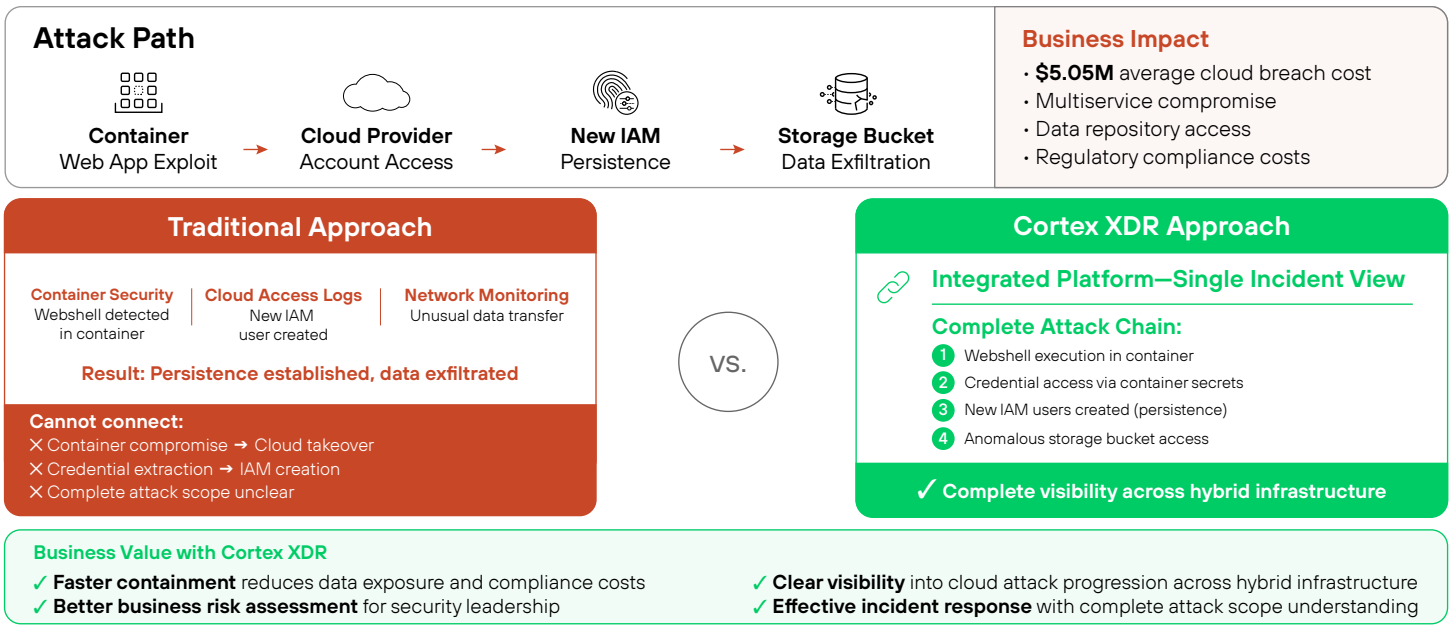

Figure 3. Scenario B: Advanced endpoint threat (Cloud-native breach)

Scenario C: Identity-Driven Compromise

Attack Path

User credentials are stolen via phishing. The attacker uses them to delete Volume Shadow Copies (VSS). They then log into the user's SaaS account from a suspicious location and configure email forwarding rules for data exfiltration.

Business Challenge

Insider threats and compromised credentials account for significant data breaches, with average costs exceeding $4.9 million per incident.[3]

Traditional Response

Identity alerts, endpoint detections, and email security warnings remain disconnected. Security teams manually investigate across multiple platforms while attackers use legitimate credentials to access sensitive data and establish persistence.

Ideal Response

Cortex XDR automatically stitches together alerts from multiple sources into one case:

- **Firewall alert:** User accessed a known phishing site.
- **Endpoint alert:** Malicious file download and attempt to delete Volume Shadow Copies (prevented).
- **Identity alert:** Impossible travel—user authenticated from a new geographic location.
- **SaaS alert:** New mail-forwarding rule created in Microsoft 365.

3. IBM and Ponemon Institute, *Cost of a Data Breach 2025*.

The ability to stitch the alerts together provides the full context that no single tool offers. It enables security leaders to respond rapidly and clearly communicate to business stakeholders about a potential incident.

Business Value

In this scenario, the reduced time to containment minimizes data exposure and potential regulatory penalties. The detailed case documentation supports compliance reporting and board-level communication about security incidents.

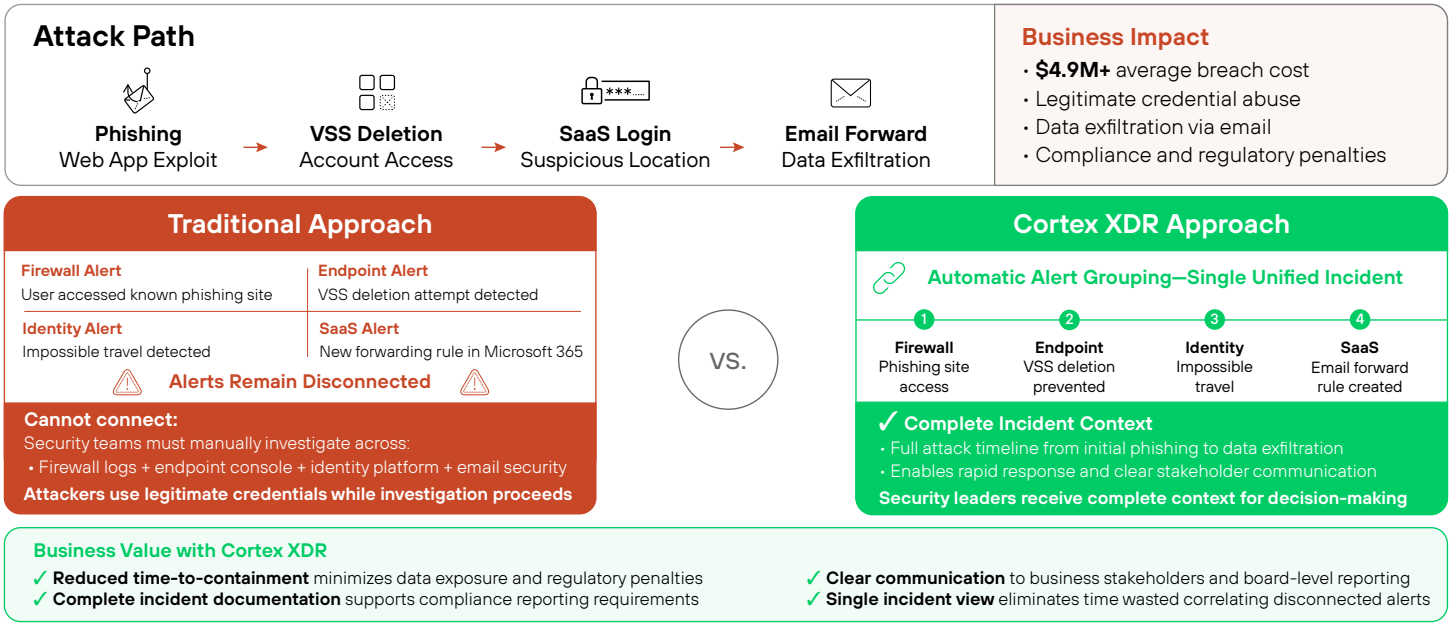

Figure 4. Scenario C: Advanced endpoint threat (Identity-driven compromise)

6 Beyond Response: Achieving SOC Transformation

The Cortex XDR endpoint-centric approach enables organizations to fundamentally transform their security operations from reactive firefighting to proactive business enablement.

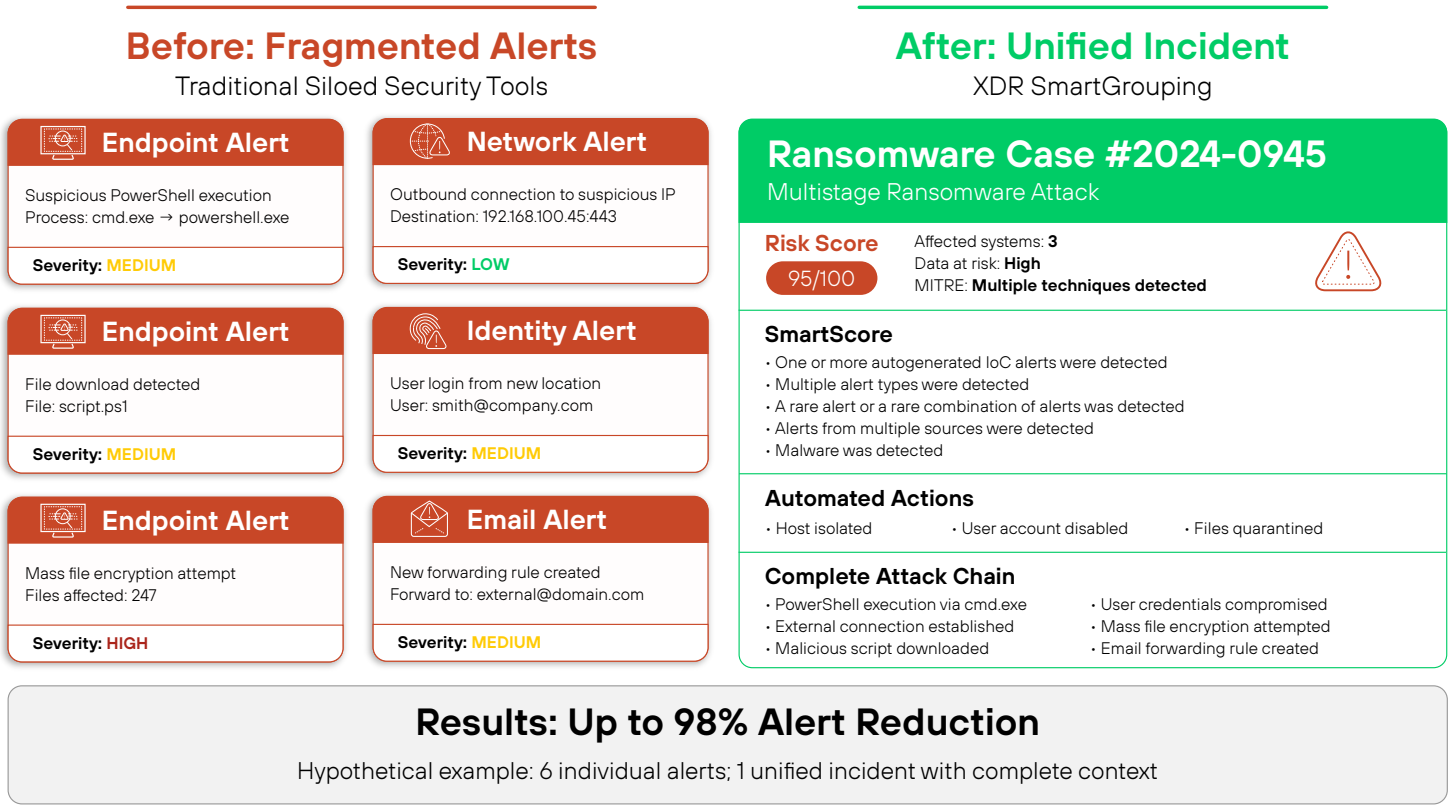

Figure 5. Traditional approach vs. Cortex XDR unified approach for alert management

The Automation Dividend

High-fidelity, contextual cases are the key to unlocking trusted automation. Cortex XDR is able to take automatic, targeted remedial actions because it understands the full attack story by using correlation and causality analysis. With natively embedded AgentiX™, Cortex XDR equips your analysts with a fleet of AI agents that continuously learn from context, orchestrate workflows, and act with precision.

For example, the Endpoint Investigation Agent in Cortex XDR responds to the identity-driven compromise scenario by:

- Performing rapid forensics collection and analysis to confirm the threat.
- Terminating the suspicious process chain on the endpoint.
- Isolating the affected host from the network.
- Disabling the compromised user account in Active Directory.
- Generating complete case documentation for compliance.

Cortex XDR autonomously handles endpoint investigation tasks, such as monitoring alert queues, initial alert triage, data enrichment, and containment actions. We estimate that these agentic team members, such as the Endpoint Investigation Agent, can help you reduce manual toil by 75%.[4]

The economic impact of automation is that organizations can progressively deploy their AI agent workforce to achieve greater autonomy in the SOC, with mature security teams substantially automating repetitive tasks over time.

Freeing Human Potential

Automation handles repetitive triage and remediation tasks, enabling security analysts to pivot to proactive, high-impact activities like threat hunting, strategic planning, and improving security posture. By leveraging automation technologies, organizations can more efficiently protect the business while creating more engaging roles for security professionals (figure 6).

SOC teams benefit by breaking away from traditional tiered approaches, instead adopting models where analysts are cross-trained across domains and supported by well-funded training programs. Moving to an autonomous model supports business continuity, provides more engaging work environments, enables greater coverage with optimized staffing, and yields more agile teams that can seamlessly pivot between responsibilities.

Figure 6. Human-first operations vs. machine-first operations

Organizations that have moved to the autonomous SOC have reported significant improvements in security analyst satisfaction with automating repetitive tasks, leading to higher retention rates in a constrained talent market. Security teams become business enablers rather than operational bottlenecks, supporting digital transformation initiatives and business growth objectives.

The Maturity Journey

This approach meets organizations where they are on their security journey. They can start by deploying Cortex XDR endpoint security with detailed telemetry collection and then using that same agent and data foundation to seamlessly grow into a fully featured, AI-driven SOC platform over time. The Cortex XDR single-agent architecture provides a seamless transition for SecOps transformation, without the disruption of rip-and-replace approaches.

Cortex XDR reduces operational overhead and lowers TCO by securing all major operating systems and cloud runtimes with a single agent architecture. This transition both consolidates endpoint security and is the first step on your SOC transformation journey. With the Cortex XDR single agent deployed and your security data already in place, you have the foundation and direct path to Cortex XSIAM®, the AI-driven platform that unifies and transforms your entire SOC.

For this implementation strategy, organizations can begin with best-in-class endpoint protection, validate detection accuracy and tune behavioral models, gradually enable automated response for high-confidence scenarios, and expand data ingestion to include network, cloud, and identity sources. This evolutionary approach protects existing investments while enabling continuous improvement and scalability as threats evolve.

4. "Playbook of the Week: Phishing for Trouble with Cortex XSOAR," Palo Alto Networks, July 1, 2022.

Security Without a SOC: The Small Enterprise Reality

While the maturity journey assumes an organization has dedicated security resources, a significant portion of the market faces a different reality. For small and midsize enterprises, the challenge is achieving effective security without a SOC.

For organizations with smaller security teams, the security challenge looks different. These companies face the same sophisticated threats as large enterprises (such as ransomware, cloud breaches, and credential theft), but without the resources to build traditional SOCs. Their reality is stark, where a small IT team of 3–7 people who wear multiple hats are responsible for everything from helpdesk tickets to infrastructure management to cybersecurity.

The Tooling Trap

Smaller organizations often inherit the same complex security architecture designed for large enterprises—multiple point solutions that each require dedicated expertise, ongoing tuning, and constant attention. A typical deployment might include separate EDR, firewall management, cloud security, and email protection tools. Each one generates its own alerts, requires its own console, and demands specialized knowledge to operate effectively.

With limited staff, however, alert fatigue becomes a massive obstacle, diverting the small team's attention and resulting in a high probability that critical threats are missed because little to no bandwidth remains for focused investigation.

Security tools operate in alert-only mode because the team might lack the confidence to enable automated responses, fearing disruption to business operations they can't quickly remediate. Maintaining and integrating a complex stack of point solutions consumes significant budget and engineering resources, slowing down the adoption of innovative security practices.

Endpoint-Centric Security Changes the Equation

For resource-constrained teams, an endpoint-centric approach built on unified data and intelligent automation is both beneficial and critical to achieving effective security at scale. Unlike free endpoint tools that provide basic protection without context or automation, or traditional managed services that add recurring costs without building internal capabilities, an endpoint-centric platform provides both immediate protection and a foundation for growth.

The Cortex XDR platform addresses this reality head-on:

- **Single-agent simplicity:** The Cortex XDR single-agent architecture enables the IT team to deploy and manage one endpoint solution instead of juggling multiple tools, dramatically reducing operational overhead.
- **Out-of-the-box efficacy:** The rigorously tested prevention capabilities work immediately, without requiring extensive tuning or specialized expertise that small teams might lack.
- **Intelligent alert reduction:** The platform transforms thousands of low-context alerts into a manageable number of high-fidelity cases that a small team can investigate. Organizations with small IT teams report reducing their security tool count from 5–7 disparate solutions to a single unified platform.[5]

5. "GuocoLand builds a unified security foundation," Palo Alto Networks, January 28, 2025.

- **Automated response capabilities:** The platform handles routine threats autonomously, freeing the IT team to focus on high-priority cases and their other responsibilities while cutting security-related operational overhead by 40%–50%.
- **Native managed detection and response (MDR):** On-demand access to expert security analysts effectively extends the internal team's capabilities without the overhead of full-time hires or the commitment of a traditional managed security service provider contract.

The Small Enterprise Reality in Action

Consider a 1,500-person manufacturing company with a 5-person IT team facing a ransomware attack at 3 p.m. on Friday. With Cortex XDR:

- The initial exploit attempt is blocked automatically at the endpoint.
- Related reconnaissance activities are correlated automatically into a single case.
- Automated response isolates the affected systems without requiring manual intervention cases.
- The IT team receives a single, prioritized case with full context Monday morning.
- The total analyst time required is 30 minutes for verification and documentation.

Without this approach, the same attack would generate over 40 disconnected alerts across multiple tools, require hours of manual correlation, and potentially succeed due to the team being unavailable over the weekend.

The Path Forward

Small enterprises need a fundamentally different approach that acknowledges their constraints while delivering uncompromised protection. By starting with the Cortex XDR endpoint-centric foundation, these organizations gain enterprise-grade security that their lean teams can operationalize.

As their needs grow—adding more sophisticated threat detection, expanding cloud infrastructure, or building dedicated security roles—the same platform and data foundation scales seamlessly. The IT team can progressively enable advanced features, integrate additional data sources, or add MDR services without requiring disruptive tool replacements or data migrations. This foundational approach makes enterprise-grade security accessible and practical for organizations that can't build traditional SOCs but still need to defend against sophisticated threats.

7 The Blueprint for a Resilient Future

Cortex XDR delivers AI-powered endpoint security with extended context from networks, cloud workloads, identities, and email in a unified platform. Organizations can transform their security operations by moving from a reactive, alert-driven posture to a proactive, threat-focused approach that automatically stitches activity across data sources, generates prioritized cases, and enables rapid investigation and response.

Unit 42® MDR seamlessly complements Cortex XDR with 24/7 expert-led monitoring, threat hunting, and coordinated response—expanding SOC capacity and accelerating containment without additional headcount.

This blueprint stops today's sophisticated breaches while building an adaptable foundation for the AI-driven SOC of tomorrow.

The Strategic Foundation

- **Cortex XDR endpoint-centric intelligence:** Provides the comprehensive visibility needed for threat detection with industry-leading MITRE ATT&CK results. Palo Alto Networks is the first and only vendor to achieve 100% technique-level detection with zero configuration changes.[6]
- **Prevention-first approach:** Stops threats before they execute behavioral analysis, machine learning, and exploit protection that blocks both known and unknown attacks at the endpoint.
- **Unified analytics platform:** Transforms fragmented alerts into coherent case narratives with up to 98% alert reduction, saving analysts hours of work every day.
- **Automated response capabilities:** Enable security teams to operate at machine speed by using automation playbooks and AI agents that drive containment and remediation across your environment in minutes.
- **Unit 42 MDR extension:** Provides experts who investigate, validate, and remediate—partnering with your team to close gaps, cut dwell time, and standardize Cortex XDR playbooks.
- **Proven industry leadership:** Palo Alto Networks is named a Leader in the 2025 Gartner® Magic Quadrant™ for Endpoint Protection Platforms and is recognized as a Customers' Choice, earning a 98% "Willingness to Recommend" score among all vendors in the Gartner® Peer Insights™ 'Voice of the Customer'" report.[7]
- **Scalable architecture:** Supports continuous evolution from endpoint protection to full SOC transformation through the direct path to Cortex XSIAM.

The Cortex XDR endpoint agent generates the richest source of attack intelligence. The destination of this transformation is a completely reimagined security operations capability that can adapt to future threats while delivering measurable improvements in detection accuracy, response speed, and operational efficiency. This approach represents the future of cybersecurity operations—platformization that transforms fragmented capabilities into unified, intelligent defense systems that can adapt to tomorrow's threats.

6. "MITRE ATT&CK Evaluations — Cortex XDR Among Elite in Endpoint Security," Palo Alto Networks, February 19, 2025.
7. "A Leader in the 2025 Gartner Magic Quadrant for EPP — 3 Years Running," Palo Alto Networks, July 17, 2025.

Take the Next Step

The endpoint-centric approach to security operations is a theoretical framework. Today's leading organizations have proven this methodology by implementing it to transform their security posture and operational efficiency.

Cortex XDR offers security leaders the opportunity to experience this evolution firsthand. With industry-leading prevention capabilities, proven detection accuracy, and the foundation for SOC evolution, Cortex XDR provides both immediate operational improvements and long-term strategic positioning.

If you prefer an expert-as-a-service model, you can pair Cortex XDR with Unit 42 MDR to extend your SOC overnight with proactive hunting, guided response, and executive-ready reporting.

See how Cortex XDR can transform your security operations.

Schedule a demo to build your proactive, AI-driven SOC today.

Can't wait to see the demo? Take the product tour now.

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.

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

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

cortex_wp_endpoint-first-charting-the-course_011426