Cortex XSIAM

Unlock Autonomous Security Operations

Stopping modern attacks requires moving faster than the adversary, every time. Security teams, however, face a never-ending onslaught of challenges while defending against these threats.

Today's siloed, human-centered SOCs stand in the way of efficient threat detection and response. What feels like nonstop alerts flood consoles, trapping analysts in repetitive tasks and swivel-chair syndrome. Endless manual work steals time that analysts don't have. Every additional tool adds complexity, slowing investigations while attackers move in seconds.

The SOC's security future requires a modern, AI-ready foundation, built for autonomous security operations, which is exactly what Cortex XSIAM® delivers. By unifying all data, automation, and agentic AI, teams can detect threats in real time and gain the speed required to stop modern threats. All this translates to more efficient operations, better decisions, less burnout, and the outcome that matters—stopping attacks.

SOC Complexity: An Attacker’s Ally

The traditional detection and response model is no longer viable. The luxury of extended dwell times, where attackers might spend 40 days unnoticed, is gone. Today’s adversaries leverage AI so they can breach defenses and achieve their objectives in mere hours.

Compounding this challenge is the escalating complexity of the security stack. Security teams are typically burdened with dozens of disparate tools. Each tool generates thousands of alerts daily, but collectively, they rarely work in concert. This fragmented approach creates overwhelming noise that obscures critical threats and severely hinders effective response. The result? The average incident response time is measured in days, not hours or minutes, leaving organizations perpetually behind the attacker’s pace.

Rethink and Transform Security Operations

Simply adding more tools is no longer enough. Organizations must move beyond fragmented solutions to a unified security experience where all data and alerts converge into a single, cohesive source of truth that’s powered by real-time AI, advanced analytics, and automation. Noise transforms into actionable insights; threats that would otherwise remain hidden are exposed; and human teams can respond to incidents in minutes, not days.

This transformation demands a fundamentally reimagined SOC architecture that features:

- Broad and automated data integration, analysis, and triage.
- Unified workflows that enable analysts to be productive.
- Embedded intelligence and automated response that can block attacks with minimal analyst assistance.

Unlike legacy security operations that are designed to maintain complexity, the modern SOC needs to unify data and lead with AI and automation to process massive datasets.

Cortex XSIAM

Cortex XSIAM harnesses the power of Cortex® AgentiX™, AI, and automation to completely transform security operations. By optimizing every stage of security operations with self-learning AI, Cortex XSIAM simplifies workflows, stops threats at scale, and puts the power of machine-speed detection and response in the hands of every analyst. Your organization can reduce risk and operational complexity by centralizing multiple products into one, AI-driven platform that’s purpose-built for security operations.

Cortex XSIAM integrates best-in-class SecOps functions, including:

- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- AI-ready security data lake
- Extended detection and response (XDR)
- Cloud detection and response (CDR)
- Network detection and response (NDR)
- Identity threat detection and response (ITDR)
- Exposure management
- Email security
- Threat intelligence platform (TIP)

A SOC transformation starts by bringing all your security data into Cortex Extended Data Lake (XDL), an extensible, AI-ready data lake for platformized SecOps. Cortex XDL acts as a single source of truth for your SOC, integrating, normalizing, and enriching your data.

Cortex XSIAM surfaces hidden threats others miss with 10,000 out-of-the-box detectors and over 2,600 ML models. It streamlines triage by automatically handling low fidelity alerts and grouping the rest into prioritized cases for rapid investigation. With over 1,000 integrations, you can orchestrate response across your security stack to eliminate threats—fast.

Easily extend the platform with advanced capabilities.

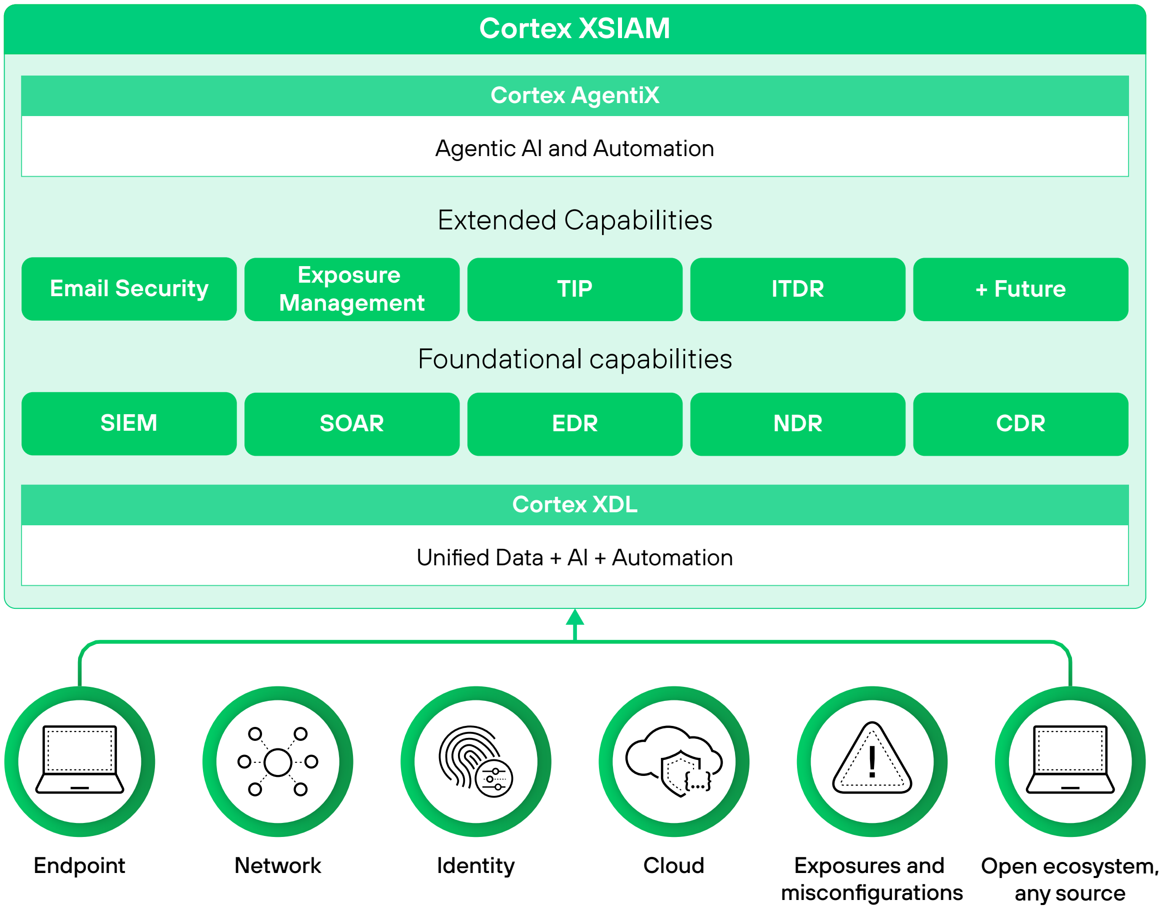


Figure 1. Cortex XSIAM core and advanced capabilities

Unified Capabilities on a Single Platform

The integration of SOC capabilities, such as SIEM, XDR, SOAR, and Exposure Management, into a single platform with a unified frontend and backend is ground-breaking for security operations. Having all capabilities in one integrated system eliminates the hassle of console switching, providing a streamlined experience.

These unified capabilities enable Cortex XSIAM to deliver broad integration support, making it easier to onboard various data sources without needing extensive engineering and infrastructure work. SOCs can seamlessly incorporate additional security-related data, enhancing their ability to analyze and detect security threats with greater precision. Moreover, the platform ensures continuous collection, stitching, and normalization of raw data, going beyond just alerts. It empowers SecOps teams with superior and simplified investigation, enabling them to identify and remediate threats faster and more effectively.

AI-Powered Protection

Ready-to-deploy AI models go beyond traditional methods. These models connect events across various data sources and offer a comprehensive overview of incidents and risks in a single location. This empowers organizations to enhance their detection, analysis, and response capabilities. Cortex XSIAM identifies threats and anomalous activity across data sources, alerting analysts to potential threats for investigation and remediation. It seamlessly connects low-confidence events, transforming them into high-confidence incidents, enabling security teams to prevent, detect, and respond more efficiently.

Automated Operations

Cortex XSIAM uses native automation and built-in integrations for seamless orchestration and execution of tasks such as incident enrichment, threat analysis, and response actions. With an AI-powered script generator and over 1,000 prebuilt playbooks in the Cortex Marketplace, teams can optimize processes and interactions across their entire security ecosystem. By automating tasks, Cortex XSIAM employs hyperscale automation to speed up investigation and response and eliminate up to 75% of manual effort in the SOC. When teams leverage agentic playbooks, they can embed LLM-powered tasks into workflows to predict, reason, and respond automatically, with optional human oversight.

Cortex Agentic Assistant

Built on Cortex AgentiX, the enterprise platform for agentic AI, the Agentic Assistant brings adaptive intelligence to SecOps. It equips your analysts with a fleet of autonomous agents that continuously learn from context, orchestrates workflows, and acts with precision—transforming security operations from manual and reactive to dynamic and machine-speed, all while keeping you firmly in control.

The AI-Driven Security Operations Platform

It all starts with the raw data. Cortex XSIAM collects and intelligently stitches data from all of your data sources—firewalls, endpoints, and cloud services—providing a clear context of security events by connecting network traffic and endpoint activities.

With this enriched data, SmartGrouping links related alerts into comprehensive incidents, offering a unified view of attack chains for SecOps teams, eliminating the need to manually piece together information.

AI-powered SmartScore enhances dynamic risk assessment by continuously analyzing incidents with machine learning (ML) and contextual rules to produce reliable risk scores. This helps SecOps teams prioritize genuine threats, reduce false positives, and improve incident response times.

By stitching logs, grouping events, and applying dynamic risk scoring, Cortex XSIAM transforms security operations, enabling more effective threat identification, prioritization, and investigation.

In legacy SOC solutions, operationalizing and optimizing the product is an exercise left to SOC teams. Cortex XSIAM benefits from continuous updates from both the Cortex Threat Research team and Palo Alto Networks Unit 42® Threat Intelligence team. Palo Alto Networks experts collect threat intelligence from more than 90,000 of our customers, update ML detection models, and automatically distribute the latest protections to Cortex XSIAM deployments. Insights from across the threat landscape help safeguard our customers from the latest advanced and fast-moving threats. By fusing leading technology with shared intelligence and research, we share the responsibility of protecting our customers' ongoing operations.

Key Integrated Capabilities

This comprehensive approach centralizes diverse security data, enabling enhanced detection and response through advanced analytics and automating incident remediation.

Cortex XSIAM combines these key SOC product capabilities into a single unified platform:

Security Information and Event Management (SIEM) includes all common SIEM functions, including log management, correlation and alerting, and compliance reporting.

Extended Detection and Response (XDR) integrates endpoint protection and detection, cloud, network, and third-party telemetry for automated detection and response.

Security Orchestration, Automation, and Response (SOAR) combines the reliability of battle-tested playbooks with the intelligence of AI agents—accessed through the Cortex Agentic Assistant—that adapt, plan, and act in real time to reduce manual work by 75%.

Centralized Management, Reporting, and Compliance simplifies operations with powerful graphical reporting capabilities that support reporting for compliance, data ingestion, incident trends, SOC performance metrics, and more.

Cortex XSIAM meets you where you are. It simplifies complex security operations, reduces alert fatigue, and streamlines workflows, all while providing the flexibility and scalability to grow alongside your evolving security needs.

Cortex Exposure Management cuts vulnerability noise by up to 99% with AI-driven prioritization and automated remediation spanning the entire enterprise.

Cortex Advanced Email Security stops sophisticated email-based attacks missed by other solutions with advanced AI and automation.

Cloud Detection and Response (CDR) includes specialty analytics designed to detect and alert on anomalies in cloud data such as cloud service provider logs and cloud security product alerts.

Identity Threat Detection and Response (ITDR) includes specialized identity analytics that use ML and behavioral analysis to profile users, machines, and entities to identify and alert on behavior that might indicate a compromised account or malicious insider.

Attack Surface Management (ASM) includes embedded capabilities that provide a holistic view of the asset inventory, including internal endpoints and vulnerability alerting for discovered internet-facing assets.

Threat Intelligence Platform (TIP) provides full TIP capabilities to manage Palo Alto Networks and third-party feeds, as well as to automatically map them to alerts and incidents.

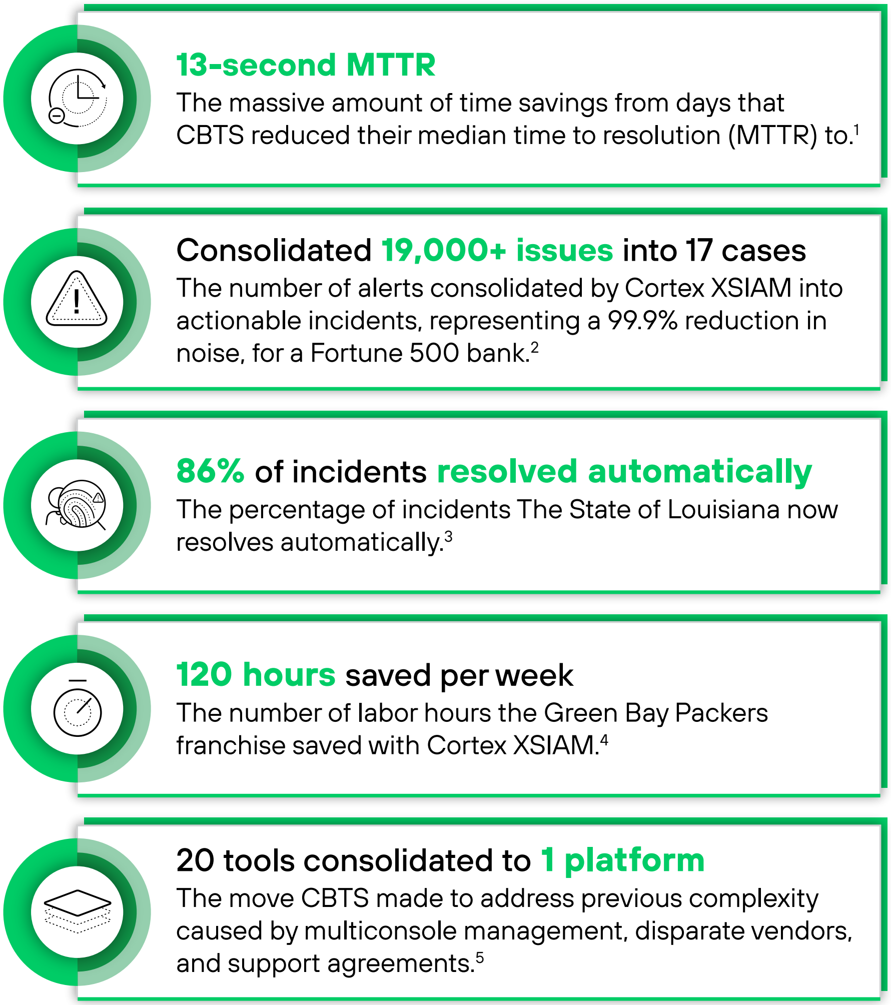
Except for CDR, these capabilities are available through additional licensing and modules.

Experience the Future of Security Operations with Cortex XSIAM

In our SOC, we process over 1 trillion events per month, distilling them into a few analyst incidents each day. Our objective is to innovate and outpace cyberthreats so our customers can confidently embrace and deploy our technology. Recent customer success metrics provide evidence that Cortex XSIAM is achieving just that.

With Cortex XSIAM, your organization gets:

- Industry-leading XDR, SIEM, SOAR, and exposure management capabilities delivered through one integrated user experience.
- A single source of truth delivered to your security team from data that was stitched together and normalized.
- Comprehensive analytics with over 10,000 prebuilt detectors and 2,600 ML models that provide real-time threat detection—without the burden of constant rule tuning.
- Industry-leading workflow automation and agentic AI that cut median time to resolution by up to 98%,[6] and reduce manual work by 75%.[7]
- A 244% ROI by improving security posture, reducing operating costs, and consolidating legacy tools.[8]



13-second MTTR
The massive amount of time savings from days that CBTS reduced their median time to resolution (MTTR) to.[1]

Consolidated 19,000+ issues into 17 cases
The number of alerts consolidated by Cortex XSIAM into actionable incidents, representing a 99.9% reduction in noise, for a Fortune 500 bank.[2]

86% of incidents resolved automatically
The percentage of incidents The State of Louisiana now resolves automatically.[3]

120 hours saved per week
The number of labor hours the Green Bay Packers franchise saved with Cortex XSIAM.[4]

20 tools consolidated to 1 platform
The move CBTS made to address previous complexity caused by multiconsole management, disparate vendors, and support agreements.[5]

Figure 2. Improved SOC efficiency and increased overall visibility for our Cortex XSIAM customers

[1] "CBTS resolves incidents in seconds with platformization, featuring Cortex XSIAM," Palo Alto Networks, March 17, 2025.

[2] "Cortex XSIAM reshapes SecOps for Fortune 500 financial giant," Palo Alto Networks, January 22, 2025.

[3] "The State of Louisiana scales security using AI-driven Cortex XSIAM," Palo Alto Networks, April 1, 2025.

[4] "Winning on defense: securing the Green Bay Packers through an AI-driven platform approach," Palo Alto Networks, July 22, 2025.

[5] Palo Alto Networks, "CBTS resolves incidents."

[6] "Boyne Resorts achieves game-changing SOC improvements with Cortex XSIAM and Unit 42 MDR," Palo Alto Networks, October 3, 2024.

[7] "Oil and gas company deploys AI-driven SOC with Cortex XSIAM," Palo Alto Networks, September 22, 2024.

[8] *The Forrester Total Economic Impact™ of Cortex XSIAM*, a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, October 15, 2025.

Enlist Elite Experts with Managed XSIAM

Organizations that adopt Cortex XSIAM might lack the in-house SOC expertise, headcount, or engineering resources to fully scale it to its potential. For example, their teams are often stretched thin or could benefit from advanced automation, SOC engineering, and threat monitoring but don't have the time and budget to hire and train staff. That's where Managed XSIAM, delivered by Unit 42, comes in. We pair our 24/7 expert-led managed detection and response (MDR) team with dedicated SOC engineering to unlock the full power of Cortex XSIAM.

Our team can manage your onboarding, custom detections, threat hunting, and automation on your behalf—driving faster attack disruption, continuous posture improvements, and executive-ready reporting. The outcome is stronger resilience with every engagement and the confidence to focus on your business growth.

Resources

- *Cortex XSIAM: The AI-Driven SecOps Platform That Goes Beyond Reactive Security* (e-book)
- Cortex XSIAM Help Center
- "CBTS resolves incidents in seconds with platformization, featuring Cortex XSIAM" (customer story)
- "Oil and gas company deploys AI-driven SOC with Cortex XSIAM" (customer story)

About Cortex XSIAM

Cortex XSIAM is the AI-driven security operations platform for the modern SOC, harnessing the power of AI to simplify security operations, stop threats at scale, and accelerate incident remediation. Reduce risk and operational complexity by centralizing multiple products into a single, coherent platform purpose-built for security operations.

Cortex XSIAM unifies best-in-class security operations functions, including EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM. Cortex XSIAM centralizes all of your security data and uses machine learning data models designed specifically for security. With Cortex XSIAM, automate data integration, analysis, and response actions, enabling analysts to focus on the incidents that matter. To learn more about Cortex XSIAM, visit www.paloaltonetworks.com/cortex/cortex-xsiam.

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