Cortex XDR

Secure Every Endpoint and Reduce Risk with an AI-Driven Approach

Cyberattacks occur three times faster now than they did just four years ago. In 20% of cases, the time from initial compromise to data exfiltration is under an hour.[1] Many existing endpoint security tools fail to be proactive, allowing too many threats to get in. They also overwhelm analysts with low-context alerts and create operational overhead that increases both cost and complexity.

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

To succeed in defending against today's cyberattacks, security operations teams need:

- **Prevention-first security** that stops threats before they gain access, to reduce the risk of a breach.
- **Rich context and advanced AI** for high-accuracy detection, investigation, and remediation.
- **A single platform** to centralize operations and lower the total cost of ownership (TCO).

Cortex XDR® delivers the world's most effective AI-driven endpoint security, proven by six years of exceptional MITRE ATT&CK® results.[2] Its unique design closes these security gaps, strengthening your posture while simplifying operations. Cortex XDR enables you to:

- **Prevent with confidence:** Stop advanced exploits, malware, and fileless attacks in real time with a unified, easy-to-deploy agent for endpoints and cloud runtime.
- **Detect evasive attacks:** Go beyond the endpoint, applying industry-leading AI across stitched endpoint, network, cloud, identity, and email data to uncover what other solutions miss.
- **Eliminate 98% of alert noise:** Dramatically reduce analyst workload by automatically grouping thousands of issues into a few prioritized cases that show the complete attack story.
- **Respond in near-real time:** Shut down attacks with best-in-class automation, AI agents, swift analyst-led actions, or our integrated 24/7 Managed Detection and Response (MDR) service.

A Proven Market Leader You Can Trust

Our market leadership is validated by the industry's most rigorous evaluations and valued by thousands of customers worldwide.

- **Historic MITRE performance:** Palo Alto Networks is the first vendor to achieve 100% technique-level detection with Cortex XDR in MITRE ATT&CK Evaluations with zero configuration changes, reflecting real-world performance.[3]
- **Flawless prevention:** Cortex XDR achieved 100% out-of-the-box prevention in the 2025 SE Labs Ransomware test,[4] with zero-prevention false positives in Round 6 of the 2024 MITRE Evaluations.[5]
- **3x recognized leader:** Palo Alto Networks, with Cortex XDR, was named a Leader in the Gartner® Magic Quadrant™ for Endpoint Protection Platforms for three consecutive years.[6]
- **Highest Willingness to Recommend:** Cortex XDR was ranked by security professionals as the highest recommended endpoint solution of all Gartner® Customers' Choice™ vendors for Endpoint Protection Platforms.[7]

How Cortex XDR Stops Sophisticated Attacks

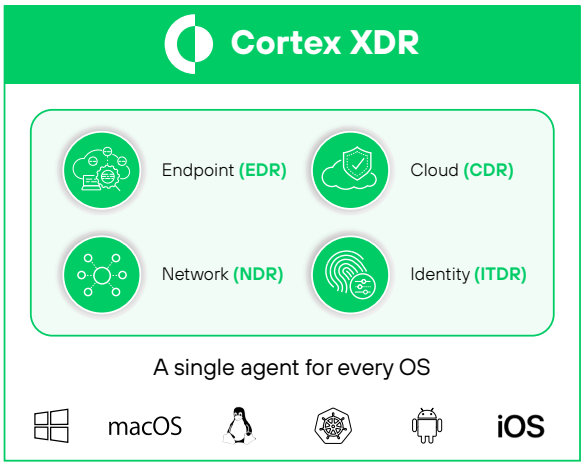
Cortex XDR delivers what security teams need from a modern endpoint defense solution, while providing the foundational platform for an AI-driven SOC transformation.

1. Reduces Risk with Industry-Leading Prevention

Our Unit 42® research experts leverage the massive scale of Palo Alto Networks—including our over 70,000 customers across every industry worldwide—to uncover the latest threat behaviors and train the AI within the Cortex XDR agent. This single, lightweight agent blocks sophisticated threats in real time with rigorously tested capabilities that work right out of the box. It uses multiple methods to block threats:

- **Behavioral threat protection:** Stops fileless threats and novel attack patterns by monitoring processes for combinations of activities that indicate malicious behavior.
- **Zero-day malware protection:** Examines over 20,000 file characteristics and uses machine learning (ML) to instantly stop unknown malware in its tracks.
- **Exploit prevention:** Monitors hundreds of endpoint processes to block the techniques used to exploit applications, regardless of whether the vulnerability has been seen before.

2. "MITRE ATT&CK Enterprise Evaluations Brings the Heat in Round 6," Palo Alto Networks, December 2024.
3. Palo Alto Networks, "MITRE ATT&CK Enterprise Evaluations."
4. "SE Labs Awards Palo Alto Networks AAA Rating and 100% Prevention Against Ransomware," Palo Alto Networks, August 5, 2025.
5. Palo Alto Networks, "MITRE ATT&CK Enterprise Evaluations."
6. "A Leader in the 2025 Gartner Magic Quadrant for EPP — 3 Years Running," Palo Alto Networks, July 17, 2025.
7. "Cortex XDR Named 2025 Gartner Customers' Choice for Endpoint Security," Palo Alto Networks, May 28, 2025.



Prevention-first approach stops threat preimpact and reduces risk.

Rich context and advanced AI enable high-accuracy detection, investigation, and remediation.

Single agent architecture on a unified data lake decreases operational overhead.

Figure 1. Cortex XDR solution overview

2. Saves Analysts Time with Unmatched Detection Accuracy

The Cortex XDR agent collects a broad range of telemetry from the endpoint and extended sources, building a rich context that enables the industry's most accurate security analytics to detect threats at machine speed. Cortex XDR set a new industry benchmark as the first endpoint solution to achieve a 100% technique-level detection score in the Round 6 MITRE Evaluations.[8]

With this foundation of context-rich data, Cortex XDR automatically groups related detections into single, prioritized cases that tell the complete attack story. It unifies visibility that provides the Cortex Agentic Assistant with the context required for autonomous, informed decision-making. By shifting from isolated events to adaptive AI analysis, you streamline investigation and reduce alert triage by up to 98%[9]—returning hours of productivity to your analysts every day.

3. Responds with Speed and Precision

With the full context of an attack, your team can respond with speed and precision. Cortex XDR has over 75 integrations to enrich endpoint security and sharpen threat detection through multisource analytics. For surgical, analyst-led actions, Live Terminal provides direct, Secure Shell access to compromised hosts to investigate and contain threats.

Trusted Automation with Transparency

Automation in Cortex XDR comes with full transparency for your team, by providing clear, understandable explanations for detection logic and automated actions. For example, when Cortex XDR generates an issue and creates a case, it provides the logic behind its risk score, enabling your team to trust the system and act decisively.

The Bottom Line: More Mature Security Operations

Our Cortex XDR approach translates directly to business value so your SOC benefits from:

- **Reduced manual toil:** Your teams spend significantly less time on correlation, alert triage, and initial investigation.
- **Faster, more accurate response:** Teams can focus on validated, prioritized threats and leverage automated remediation.
- **Empowered analysts:** Your organization can free up skilled personnel for strategic work like threat hunting and more advanced automation.

8. Palo Alto Networks, "MITRE ATT&CK Enterprise Evaluations."
9. "North Dakota IT safeguards citizens with integrated, AI-driven security operations," Palo Alto Networks, November 18, 2024.

4. Lowers TCO with the Foundation for the AI-Driven SOC

Cortex XDR reduces operational overhead and TCO by securing all major operating systems (Windows, macOS, and Linux) and cloud runtimes (e.g., Kubernetes) with a single agent architecture. In addition to consolidating endpoint security, it's the first step on your SOC transformation journey. With a single agent deployed and your security data centralized in the Cortex Extended Data Lake™ (XDL), you have a frictionless path to Cortex XSIAM®, the AI-driven platform that unifies and transforms your entire SOC.

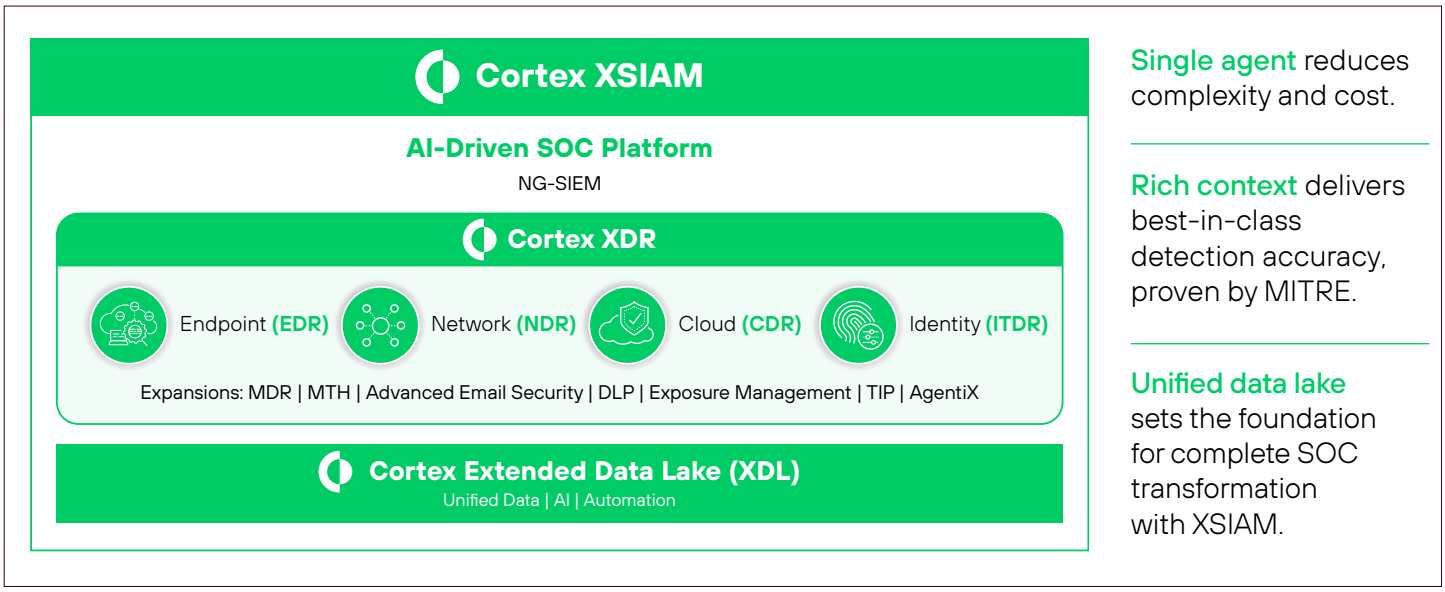


Figure 2. Single agent architecture on a unified data lake

Complete Endpoint Security and Control

Cortex XDR provides all the essential tools you need to harden and control your endpoints from a single console, using the same unified agent.

- **Device control:** Mitigate physical media risks by monitoring and managing USB and Bluetooth device access with granular policies.
- **Host firewall and disk encryption:** Centrally manage host-based firewalls for Windows and macOS, as well as enforce full-disk encryption (BitLocker or FileVault) to meet compliance mandates.
- **Mobile security:** Extend enterprise-grade threat protection and traffic control to your corporate iOS and Android devices.
- **Cortex Agentic Assistant:** A workforce of autonomous AI agents that continuously learn from context, orchestrate workflows, and act with precision.

Security Add-Ons

Extend the capabilities of Cortex XDR with powerful, integrated modules:

- **Cloud Runtime Security:** Prevent cloud attacks in real time with best-in-class protection delivered by Cortex XDR agent for VMs, containers, Kubernetes, and serverless workloads.
- **Identity Threat Detection and Response (ITDR):** Uncover identity-based threats by analyzing user and entity behavior, identifying compromised accounts, and enabling a swift response to insider threats.
- **Advanced Email Security:** Stop email attacks in real time with an AI-driven analytics engine that assesses the intent of every email.
- **Host Insights:** Proactively manage your attack surface with comprehensive vulnerability assessment and host inventory.
- **Forensics:** Accelerate deep-dive investigations with rich forensic data, including volatile memory, to determine the source and scope of a compromise.
- **Endpoint Data Loss Prevention (DLP):** Protect web and endpoint activity from data leakage, even when devices are offline.
- **Exposure Management:** Prioritize risk reduction by analyzing the full attack surface, active threats, and existing security controls.
- **Attack Surface Management (ASM):** A holistic view of the asset inventory, including internal endpoints and vulnerability alerting for discovered internet-facing assets.

Flexible Deployment and Management

Deploy quickly and augment your team with expert-led 24/7 services.

- **Cloud-native architecture:** Cortex XDR eliminates the need for on-premises log storage. The lightweight agent installs and upgrades without requiring a reboot.
- **Expert-led managed services:** For ultimate peace of mind, augment your team with our Unit 42 Managed Detection and Response. You get 24/7 monitoring, investigation, and response to shut down attacks with best-in-class mean time to respond (MTTR).

Go Beyond XDR: Evolve Your SOC with Cortex XSIAM

Cortex XSIAM—the solution to modernize your security operations—builds on the foundation of Cortex XDR. XSIAM adds industry-leading NG-SIEM, SOAR, and attack surface management into a single, AI-driven platform for the modern SOC. With Cortex, you gain the trusted foundation to evolve your security, powered by AI and automation to simplify operations, stop threats at scale, and accelerate incident remediation.

Table 1. Cortex XDR Licensing Options		
Feature	**XDR Prevent**	**XDR Pro per Endpoint**
Endpoint Threat Prevention Prevent malware, ransomware, exploits, and fileless attacks.	✓	✓
Endpoint Controls Safeguard endpoints with device control, firewall, and disk encryption.	✓	✓
Endpoint Threat Detection Uncover attacks in real time with thousands of built-in, ML-based analytic detectors.	—	✓
Unified Cases with Risk Scoring Every related detection is grouped into a single case and scored by risk.	—	✓
Automated and Analyst-Led Response Over 100 built-in playbooks and quick actions enable rapid remediation.	—	✓
Cortex Agentic Assistant A workforce of AI agents that autonomously handle workflows like triage, enrichment, and containment.	—	✓
Extended Detection Analytics (network, cloud, and identity)	—	✓
Extended Response Actions (network, cloud, and identity)	—	✓
Cloud Runtime Security	—	Add-on
Identity Threat Detection and Response	—	Add-on
Advanced Email Security	—	Add-on
Managed Threat Hunting	—	Add-on
Managed Detection and Response	—	Add-on
Extended Threat Hunting Data	—	Add-on
Host Insights	—	Add-on
Forensic Investigation	—	Add-on
Endpoint Data Loss Prevention	—	Add-on
Exposure Management	—	Add-on
Attack Surface Management	—	Add-on

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

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

© 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_ds_cortex-xdr_031626