Cortex XDR

Defining the New Category of Enterprise-Scale Prevention, Detection, and Response

Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom detection rules.
- **Reduce alerts by 50 times:** Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts.
- **Investigate eight times faster:** Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- **Stop attacks without degrading performance:** Obtain the most effective endpoint protection available with a lightweight agent.
- **Maximize ROI:** Use existing infrastructure for data collection and control to lower costs by 44%.

Security teams can't detect and stop active attacks quickly. Even though they've deployed countless security tools, they lack the enterprise-wide visibility and deep analytics needed to find threats. These siloed tools generate endless alerts and force analysts to pivot from console to console to verify threats, resulting in missed attacks and incomplete investigations. Faced with a shortage of cybersecurity professionals, teams must simplify operations.

Prevent, Detect, Investigate, and Respond to All Threats

Cortex XDR™ defines the new category for enterprise-scale prevention, detection, and response that integrates endpoint, network, and cloud data to stop sophisticated attacks. As the market's first and leading XDR category product, Cortex XDR unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency.

Block the Most Endpoint Attacks with Best-in-Class Prevention

The Cortex XDR agent safeguards endpoints from malware, exploits, and fileless attacks with industry-best, AI-driven local analysis and behavior-based protection. Organizations can stop never-before-seen threats with a single cloud-delivered agent for endpoint protection, detection, and response. The integrated Device Control module granularly manages USB access to prevent data loss and malware delivery from malicious devices. The agent shares protections across network and cloud security offerings from Palo Alto Networks to provide ironclad, consistent security across the entire enterprise.

Detect Stealthy Threats with Machine Learning and Analytics

Cortex XDR identifies evasive threats with unmatched accuracy by continuously profiling user and endpoint behavior with analytics. Machine learning models analyze data from Palo Alto Networks and third-party sources to uncover stealthy attacks targeting managed and unmanaged devices.

Investigate and Respond at Lightning Speed

Cortex XDR accelerates investigations by providing a complete picture of every threat and automatically revealing the root cause. Intelligent alert grouping and alert deduplication simplify triage and reduce the experience required at every stage of security operations. Tight integration with enforcement points lets analysts respond to threats quickly.

Get MDR Services from Our Industry-Leading Partners

Powered by Cortex XDR, our managed detection and response (MDR) partners' services relieve the day-to-day burden of security operations and provide the instant maturity of a 24/7 SOC, delivering a range of services from alert management to incident response and threat hunting. Cortex XDR enables the next generation of MDR services, allowing for comprehensive prevention, detection, and response across network, endpoint, and cloud in a unified, fully integrated technology stack. Get help with custom tuning and deployment to get up and running in weeks, not years, and immediately benefit from decades of investigations, forensics, and security operations expertise. Break through the limitations of managed services built on point products and achieve a guaranteed reduction of mean time to detect (MTTD) and mean time to respond (MTTR) to 60 minutes or less.

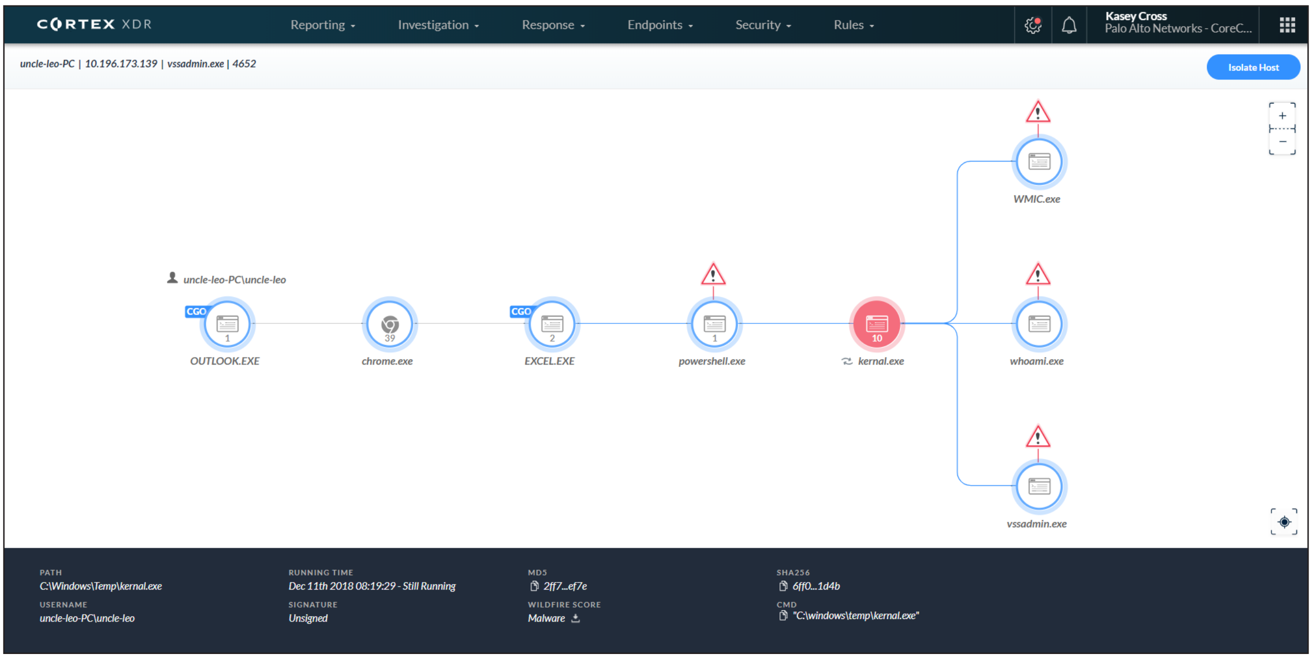

Figure 1: Cortex XDR triage and investigation view

Key Capabilities

Safeguard Your Assets with Industry-Best Endpoint Protection

Prevent threats and collect data for detection and response with a single, cloud native agent. The Cortex XDR agent offers a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptive AI-driven local analysis engine that's always learning to counter new attack techniques. A Behavioral Threat Protection engine examines the behavior of multiple, related processes to uncover attacks as they occur. Integration with the Palo Alto Networks WildFire® malware prevention service boosts security accuracy and coverage. Read more about endpoint protection.

Securely Manage USB Devices

Protect your endpoints from malware and data loss with Device Control. The Cortex XDR agent allows you to monitor and secure USB access without needing to install another agent on your hosts. You can restrict usage by vendor, type, endpoint, and Active Directory® group or user. Granular policies allow you to assign write or read-only permissions per USB device. You can easily manage USB access settings from the Cortex XDR management interface and gain peace of mind that you've mitigated USB-based threats.

Get Full Visibility Based on Good Data

Break security silos by integrating all data. Cortex XDR automatically stitches together endpoint, network, and cloud data to accurately detect attacks and simplify investigations. It collects data from Palo Alto Networks products as well as third-party logs and alerts, enabling you to broaden the scope of intelligent decisions across all network segments. Third-party alerts are dynamically integrated with endpoint data to reveal root cause and save hours of analysts' time. Cortex XDR examines logs collected from third-party firewalls with behavioral analytics, enabling you to find critical threats and eliminate any visibility blind spots.

Discover Threats with Continuous ML-based Detection

Find stealthy threats with analytics and out-of-the-box rules that deliver unmatched MITRE ATT&CK™ coverage. Cortex XDR automatically detects active attacks, allowing your team to triage and contain threats before the damage is done. Using machine learning, Cortex XDR continuously profiles user and endpoint behavior to detect anomalous activity indicative of attacks. By applying analytics to an integrated set of data, including security alerts and rich network, endpoint, and cloud logs, Cortex XDR meets and exceeds the detection capabilities of siloed network traffic analysis (NTA), endpoint detection and response (EDR), and user behavior analytics (UBA) tools. Automated detection works all day, every day, providing you peace of mind.

Investigate Eight Times Faster

Automatically reveal the root cause of every alert. With Cortex XDR, your analysts can examine alerts from any source—including third-party tools—with a single click, streamlining investigations. Cortex XDR automatically reveals the root cause, reputation, and sequence of events associated with each alert, lowering the experience level needed to verify an attack. By consolidating alerts into incidents, Cortex XDR slashes the number of individual alerts to review and alleviates alert fatigue. Each incident provides a complete picture of an attack, with key artifacts and integrated threat intelligence details, accelerating investigations.

Hunt Threats with Powerful Search Tools

Uncover hidden malware, targeted attacks, and insider threats. Your security team can search, schedule, and save queries to identify hard-to-find threats. Flexible searching capabilities let your analysts hunt threats and search for both indicators of compromise (IOCs) and behavioral indicators of compromise (BIOCs) without learning a new query language. By incorporating threat intelligence from Palo Alto Networks with a complete set of network, endpoint, and cloud data, your team can catch malware, external threats, and internal attacks whether the incidents are in progress or have occurred in the past.

Coordinate Response Across Endpoint, Network, and Cloud Enforcement Points

Stop threats with fast and accurate remediation. Cortex XDR lets your security team instantly contain endpoint, network, and cloud threats from one console. Your analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update prevention lists like bad domains through tight integration with enforcement points. The powerful Live Terminal feature lets Tier 1 analysts swiftly investigate and shut down attacks without disrupting end users by directly accessing endpoints; running Python®, PowerShell® or system commands and scripts; and managing files and processes from graphical file and task managers.

Tightly Integrate with Security Orchestration, Automation, and Response (SOAR)

Standardize and automate response processes across your security product stack. Cortex XDR integrates with Demisto®, enabling your teams to feed incident data into Demisto for automated, playbook-driven response that spans more than 300 third-party tools and promotes cross-team collaboration. Demisto playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks. You can leverage Demisto's case management to monitor and correlate Cortex XDR incidents with other alerts in your organization.

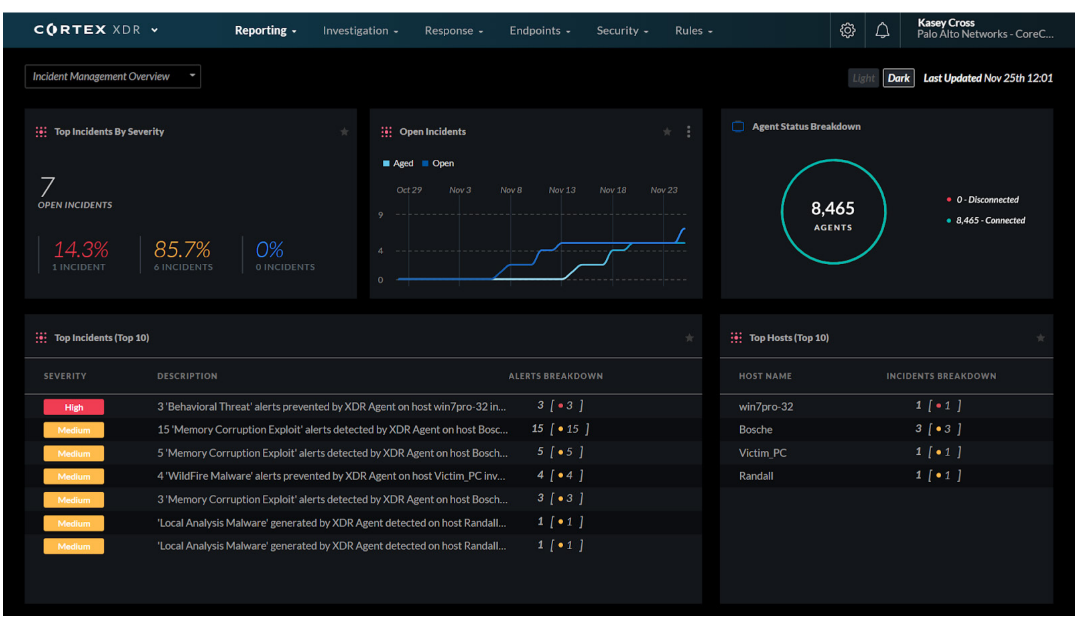

Figure 2: Customizable dashboard

Unify Management, Reporting, Triage, and Response in One Intuitive Console

Maximize productivity with a seamless platform experience. The management console offers end-to-end support for all Cortex XDR capabilities, including endpoint policy management, detection, investigation, and response. You can quickly assess the security status of your organization's or individual endpoints with customizable dashboards, and summarize incidents and security trends with graphical reports that can be scheduled or generated on demand. Public APIs extend management to third-party tools, enabling you to retrieve and update incidents, collect agent information, and contain endpoint threats from the management platform of your choice.

Ease Deployment with Cloud Delivery

Get started in minutes. The cloud native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy new on-premises network sensors or log collectors. You can use your Palo Alto Networks products or third-party firewalls to collect data, reducing the number of products you need to manage. You only need one source of data, such as Next-Generation Firewalls or Cortex XDR agents, to detect and stop threats, but additional sources can eliminate blind spots. Easily store data in Cortex Data Lake, a scalable and efficient cloud-based data repository. By integrating data from multiple sources together, automating tasks, and simplifying management, Cortex XDR delivers a 44% cost savings compared to siloed security tools.

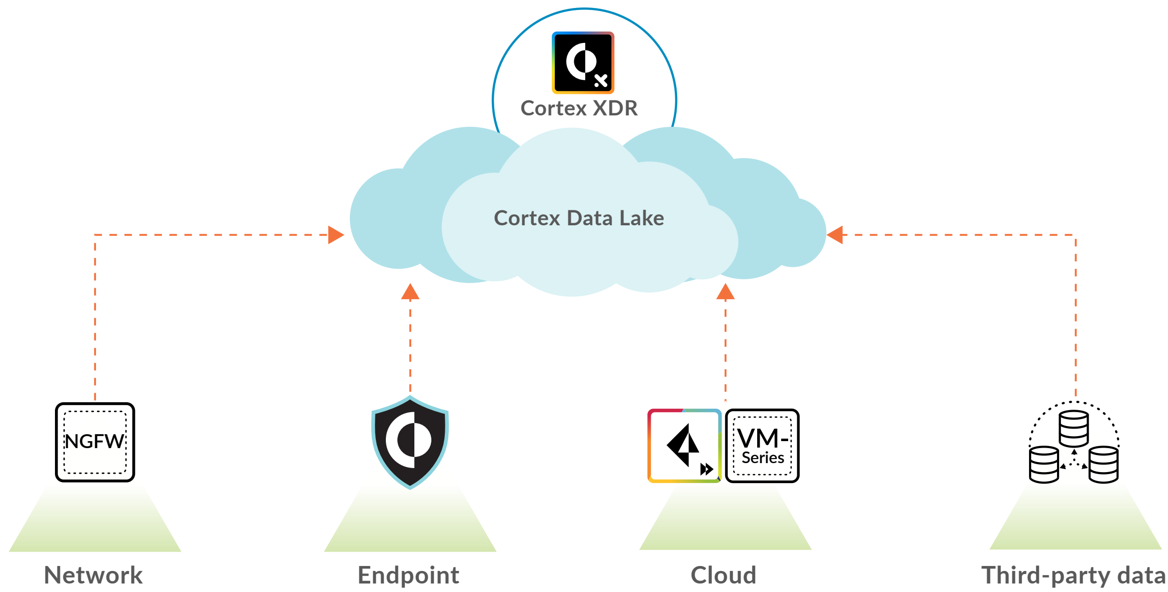

Figure 2: Analysis of data from any source for detection and response

Operational Benefits

Block known and unknown attacks with powerful endpoint protection: Leverage AI-based local analysis and Behavioral Threat Protection to stop the most malware, exploits, and fileless attacks in the industry.

Gain visibility across network, endpoint, and cloud data: Collect and correlate data from Palo Alto Networks and third-party tools to detect, triage, investigate, hunt, and respond to threats.

Automatically detect sophisticated attacks 24/7: Use always-on AI-based analytics and custom rules to detect advanced persistent threats and other covert attacks.

Avoid alert fatigue and personnel turnover: Simplify investigations with automated root cause analysis and a unified incident engine, resulting in a 50 times reduction in alerts and lowering the skill required to triage alerts.

Drastically reduce false positive alerts: Apply knowledge from every investigation to refine behavioral detection rules and speed future analysis, decreasing noise and risk.

Increase SOC productivity: Consolidate endpoint security policy management and monitoring, investigation, and response across your network, endpoint, and cloud environments in one console, increasing SOC efficiency.

Eradicate threats without business disruption: Shut down attacks with surgical precision while avoiding user or system downtime.

Eliminate advanced threats: Protect your network against malicious insiders, policy violations, external threats, ransomware, fileless and memory-only attacks, and advanced zero-day malware.

Supercharge your security team: Disrupt every stage of an attack by detecting IOCs, anomalous behavior, and malicious patterns of activity.

Continually improve your security posture: Save threat hunting searches as behavioral rules to detect similar threats in the future. Flexible informational alerts improve timeline analysis by identifying suspicious behavior and making complex events easy to understand.

Extend detection, investigation, and response to third-party data sources: Enable behavioral analytics on logs collected from third-party firewalls while integrating third-party alerts into a unified incident view and root cause analysis for faster, more effective investigations.

Table 1: Cortex XDR Features and Specifications	
Detection and Investigation Features and Capabilities	
Automated stitching of network, endpoint, and cloud data from Palo Alto Networks and third-party sources	Root cause analysis of alerts
Third-party alert and log ingestion	Timeline analysis of alerts
Machine learning-based behavioral analytics	Unified incident engine
Custom rules to detect tactics, techniques, and procedures	Threat hunting
Malware and fileless attack detection	Post-incident impact analysis
Detection of targeted attacks, malicious insiders, and risky user behavior	Dashboards and reporting
Network traffic analysis (NTA) and user behavior analytics (UBA)	Incident response and recovery
Endpoint detection and response (EDR)	IOC and threat intelligence searches
Native integration with Demisto for security orchestration, automation, and response (SOAR)	—
Endpoint Protection and Response Capabilities	
Malware, ransomware, and fileless attack prevention	Device control for USB device management
Behavioral Threat Protection	Live Terminal for direct endpoint access
AI-based local analysis engine	Network isolation, quarantine, process termination, file deletion, file blacklist
Integration with the cloud-based WildFire malware prevention service	Public APIs for response and data collection
Child process protection	Credential theft protection
Exploit prevention by exploit technique	Scheduled and on-demand malware scanning
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Guaranteed reduction of MTTD and MTTR to 60 mins or less
Investigation of every alert and incident generated by Cortex XDR	Custom tuning of Cortex XDR for enhanced prevention, visibility, and detection
Dedicated, proactive threat hunters who understand your environment	Direct access to partners' analysts and forensic experts
Guided or full threat remediation actions	Visibility and coverage across network, endpoint, and cloud assets
Technical Specifications	
Delivery model	Cloud-delivered application
Data retention	30-day to unlimited data storage
Cortex XDR Prevent subscription	Endpoint protection with Cortex XDR agents
Cortex XDR Pro per endpoint subscription	• Detection, investigation, and response across endpoint data sources • Endpoint protection with Cortex XDR agents
Cortex XDR Pro per TB subscription	Detection, investigation, and response across network and cloud data sources, including third-party data
Cortex XDR Pathfinder endpoint analysis service	Collects process information from endpoints that do not have Cortex XDR agents; included with all Cortex XDR subscriptions

Reinvent Security Operations with Cortex

Cortex XDR is part of Cortex™, the industry's most comprehensive product suite for security operations, empowering enterprises with best-in-class detection, investigation, automation, and response capabilities. The suite is built on the tightly integrated offerings of Cortex XDR and Demisto, which enables you to transform your SOC operations from a manual, reactive model that required endless resources to a lean, proactive, and automated team that reduces both MTTD and MTTR for every security use case.

Operating System Support

The Cortex XDR agent supports multiple endpoints across Windows®, macOS®, Linux, and Android® operating systems. For a complete list of system requirements and supported operating systems, please visit the Palo Alto Networks Compatibility Matrix. Cortex XDR Pathfinder minimum requirements: 2 CPU cores, 8 GB RAM, 128 GB thin-provisioned storage, VMware ESXi™ V5.1 or higher, or Microsoft Hyper-V® 6.3.96 or higher hypervisor.

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-xdr-ds-120919