Cortex XDR

Protect Your Entire Organization from Breaches with the Industry's First Extended Detection and Response Platform

Today's siloed security solutions can't keep up with evolving threats, burdening security teams with too many alerts, complex investigations, and missed attacks. Even when teams deploy dozens of tools, they still lack the enterprise-wide visibility and deep analytics they need to stop threats before damage is done. Faced with a shortage of security talent, teams need a radical new approach to eliminate threats—an approach built on good data, analytics, and AI that's always learning.

Cortex XDR Benefits

- **Stop attacks with proven, best-in-class security**. Uncover and block attacks with behavior-based and AI-powered next-generation antivirus.
- **Detect advanced threats with analytics and AI**. Uncover threats at machine speed with the solution that delivered 100% detection in the 2024 MITRE ATT&CK® Evaluations.
- **Reduce alerts by up to 98%**. Avoid alert fatigue with a game-changing incident engine that intelligently groups related alerts.
- **Cut investigation time by 88%**. Verify threats quickly by getting a complete picture of attacks with root cause analysis.
- **Maximize ROI**. Consolidate tools and simplify operations to cut SOC costs.

Prevent, Detect, and Respond to the Stealthiest Threats

You can now stop modern attacks with Cortex XDR®, the industry's first endpoint-based extended detection and response platform that integrates data from any source. Your SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and incident scoring. Cross-data insights accelerate investigations so that you can streamline incident response and recovery. Finally, by harnessing the power of AI, analytics, and rich data, Cortex XDR allows you to detect stealthy threats.

Cortex XDR delivers peace of mind with industry-leading endpoint security that achieved 100% detection with no configuration changes in the 2024 MITRE ATT&CK Evaluations. The Cortex XDR platform collects and analyzes all data so you can gain complete visibility and holistic protection to secure what's next.

In the 2024 MITRE ATT&CK Evaluations, Cortex XDR made history as the first participant ever to achieve 100% detection with technique-level detail and no configuration changes or delays.

Get Full Visibility Across Your Entire Environment

Cortex XDR automatically stitches together endpoint, network, cloud, and identity data to accurately detect attacks and simplify investigations. Third-party alerts are dynamically integrated with endpoint data to reveal root cause and save hours of analysts' time.

Discover Threats with Analytics and Machine Learning

Using machine learning, Cortex XDR continuously profiles endpoint and network behavior to detect anomalous activity indicative of attacks. It provides a 360-degree view of users, including user risk scores, for user behavior analytics (UBA).

Gain Deeper Insights with Global Analytics

Cortex XDR's Global Analytics system harnesses cross-customer insights for you to identify advanced threats, such as supply chain and zero-day attacks. By applying analytics to an integrated set of data, Cortex XDR can detect evasive threats that siloed endpoint, network, and cloud detection and response tools miss.

Investigate at Lightning Speed

Each incident within Cortex XDR provides you with a complete picture of an attack, with key artifacts and threat intelligence details. Furthermore, Cortex XDR's SmartScore identifies high-risk incidents with machine learning, empowering your team to quickly assess attack scope and impact.

Orchestrate, Automate, and Enrich with Cortex XSOAR

Cortex XDR tightly integrates with Cortex XSOAR®, enabling your teams to feed incident data for automated response based on 1,000+ product integrations. XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR. It also links insights to incidents in real time, giving you unmatched visibility into the global threat landscape and automating the distribution of your threat intelligence at scale.

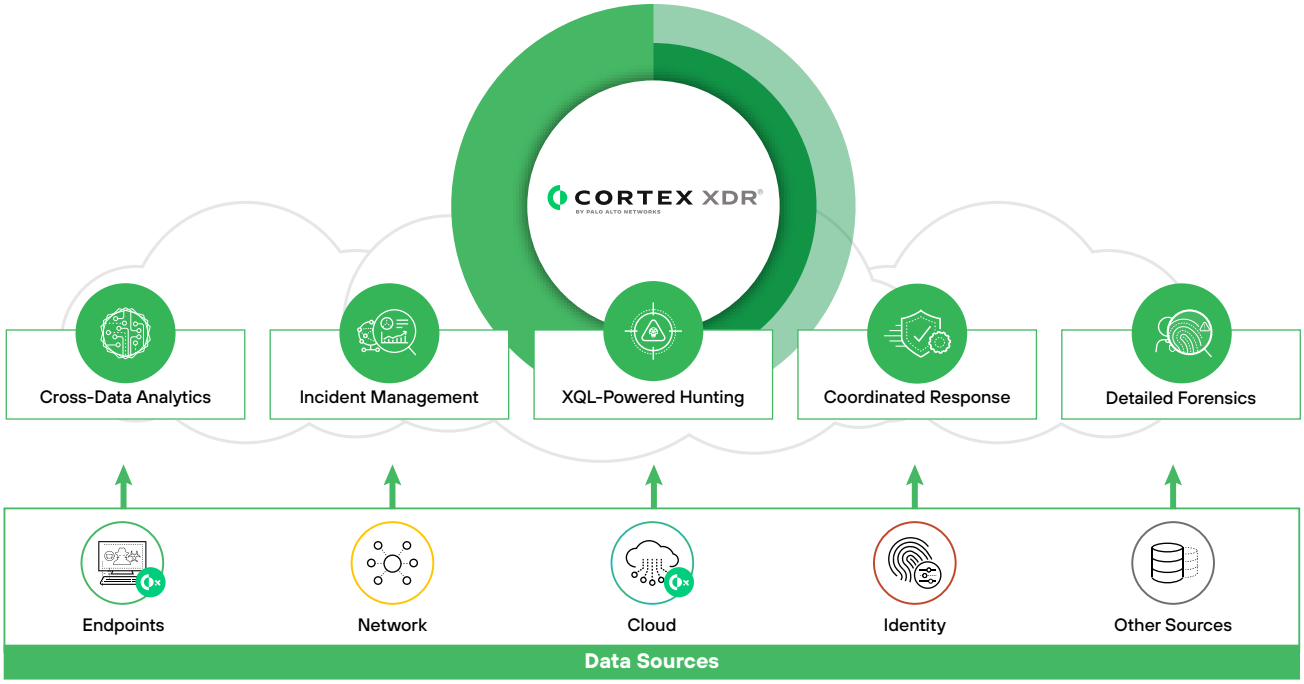

Figure 1: Analysis of data from any source for detection and response

Onboarding all your data sources into Cortex XDR enables you to broaden the scope of threat hunting and eliminate blind spots. Cortex XDR detects advanced attacks with AI, analytics, and out-of-the-box rules, allowing your team to triage and contain threats quickly. It also simplifies triage and investigations by automatically revealing the root cause, reputation, and attack sequence associated with each alert. By grouping alerts into incidents, Cortex XDR slashes the number of individual alerts to review by up to 98%, reducing alert fatigue.

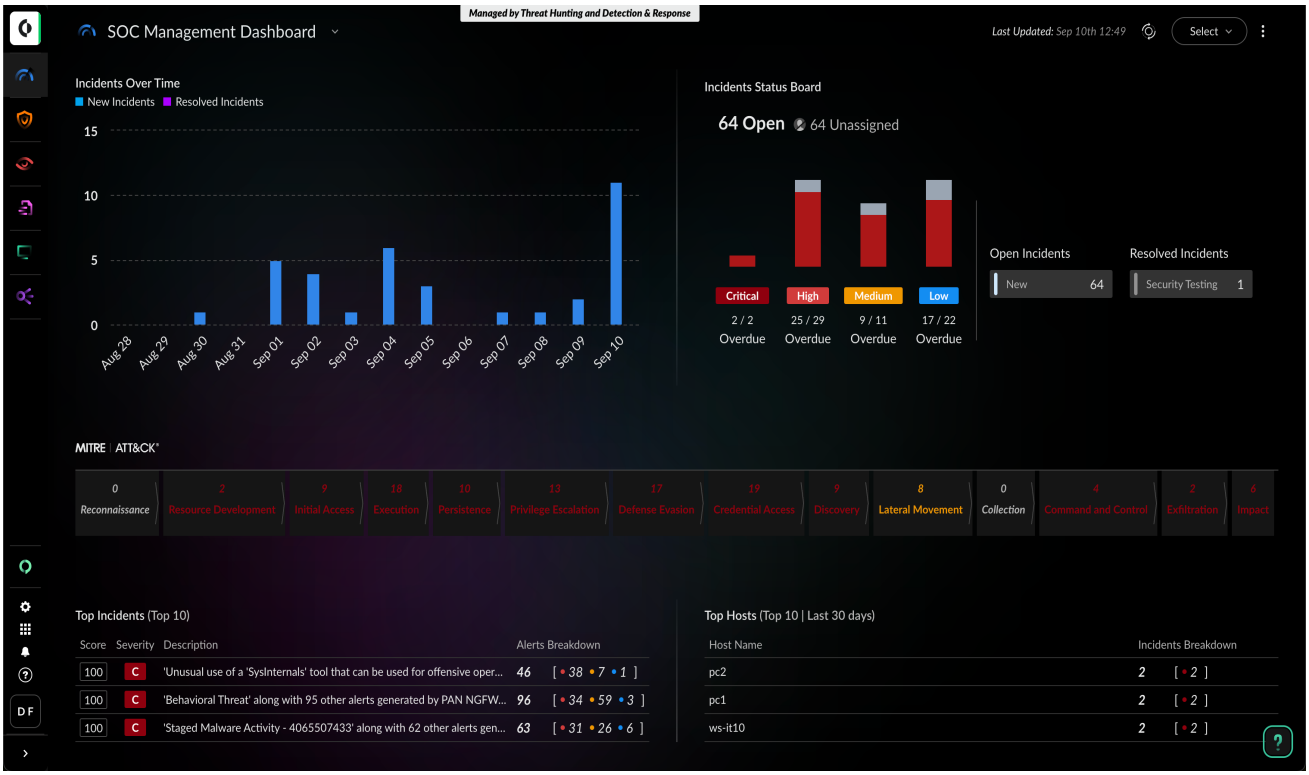

Figure 2: Customizable dashboard

Block Attacks with Best-in-Class Endpoint Detection and Response

The Cortex XDR agent offers unparalleled protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block malware infections. It enables sharp detection with AI-powered analytics and threat insights. Finally, it allows you to remediate quickly and take control of affected machines.

Securely Manage USB and Bluetooth Devices with Device Control

The Cortex XDR agent protects your endpoints from malware and data loss by monitoring and managing USB access. You can restrict usage by vendor, type, endpoint, and Active Directory group or user without needing to install another agent on your hosts. Granular policies allow you to assign write or read-only permissions per USB device.

Bluetooth devices are also a potential vector for data loss from endpoints. Bluetooth Device Control now gives analysts control over Bluetooth devices connecting to endpoints, covering both Bluetooth Classic and Bluetooth Low Energy devices. Admins can set granular policies, like allowing specific Bluetooth devices for productivity, while blocking everything else and stopping potential data loss. This device control capability for Bluetooth further hardens endpoint security posture and prevents unwanted data sharing over Bluetooth channels.

Protect Endpoints with Host Firewall and Disk Encryption

With host firewall and disk encryption capabilities, you can lower your security risks as well as address regulatory requirements. The Cortex XDR host firewall enables you to control inbound and outbound communications on your Windows and macOS endpoints. Additionally, with disk encryption, you can create rules and policies and apply BitLocker or FileVault encryption on your endpoints. Host firewall and disk encryption capabilities and policies can be centrally configured from the Cortex XDR management console.

Extend Enterprise Security to Mobile Devices

With Cortex XDR, you can extend security to your mobile devices on both the iOS and Android platforms. For iOS devices, utilize URL filtering to analyze, block, or report malicious URLs and manage custom URLs. You can also report and block spam calls and messages, and leverage the Safari browser security module to gate suspicious sites and inform users about site safety. Additionally, the network and EDR security module allows you to exercise granular control and monitoring of network traffic on supervised iOS devices.

For Android, Cortex XDR enables you to examine APK files to prevent malicious applications from running on your endpoints. Cortex XDR delivers robust mobile protection, securing your devices and safeguarding your organization's data.

Superior Detection Coverage with Analytics and Malware Analysis

Cortex XDR examines every file with its AI-driven local analysis engine—always learning and preparing to counter new attack techniques. The 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 analysis service boosts security accuracy and coverage.

Stop Threats Quickly with Flexible Response Options

Cortex XDR lets your security team instantly contain endpoint, network, and cloud threats from one console. 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 analysts swiftly verify and contain attacks without disrupting end users by running Python, PowerShell, or system commands and scripts directly on endpoints. Analysts of all experience levels can manage files and processes from graphical file and task managers.

eXtended Threat Hunting Data Module

Data collection is crucial for effective threat hunting. It enables the identification and analysis of potential threats by providing valuable insights into system behavior, network traffic, and user activity. Comprehensive data empowers threat hunters to swiftly detect and respond to cyberattacks, preventing or minimizing damage to organizations' security posture. Cortex XDR's eXtended Threat Hunting Data Module enhances XDR Pro by onboarding additional event types and boosting XDR's analytics capabilities, allowing you to sharpen your detection and strengthen threat hunting operations.

The XDR Advantage

Cortex XDR
The industry's first extended detection and response solution

Host Insights
Better identify threats and vulnerabilities and contain them

Identity Analytics
Leverage identity and access context and behavioral analysis

Forensics
Makes triage and forensic analysis easy and more powerful

Identity Threat Detection and Response
Manage risk from identity threats and malicious insiders

eXtended Threat Hunting Data Module (XTH)
Gain deeper visibility, enable threat hunting, and unlock advanced analytics

Gain Unprecedented Visibility and Response with Host Insights

Host Insights, an add-on module for Cortex XDR, offers a holistic approach to endpoint visibility and attack containment, reducing your exposure to threats so you can avoid breaches. Host Insights helps you swiftly find and eradicate threats by delivering vulnerability assessment, host inventory, and Search and Destroy.

Accelerate Incident Response with Forensics

Cortex XDR Forensics is a triage and investigation module letting you review evidence, hunt for threats, simplify investigations, and perform compromise assessments from one console. With its deep data collection, it provides you with instant access to a wealth of forensics data and artifacts—including volatile memory—so you can determine the source and scope of an attack. See the data-sheet for more information.

Furthermore, with Cortex XDR Pro's dissolvable agent, you can collect forensics data without the need to maintain the complete agent on your endpoint. Instead, you deploy it just once. The dissolvable agent can be installed on the affected device, performs a one-time data collection, and then uninstalls itself.

Manage Insider and Identity Risk with Identity Analytics and ITDR

With Cortex XDR's Identity Analytics, you can use advanced data collection and analytics to identify abnormal user and entity activity to defend against compromised user accounts and malicious insiders. Identity Analytics allows you to gain visibility by ingesting user activity data feeds (from endpoints, agents, firewalls, Active Directory, and more). It also applies machine learning and behavioral analytics built into analytic detectors that are continuously updated and created by Cortex threat researchers and data sciences experts.

By combining advanced detection capabilities as part of Identity Analytics with the Identity Threat Detection and Response (ITDR) Module that protects against identity threats later on along the attack lifecycle, you can swiftly identify and investigate identity-related threats, assess impact through scoring, visualize trends and profiles, and reduce the risk of data breaches.

Hunt for Hidden Malware, Targeted Attacks, and Insiders

Powerful searching capabilities in Cortex XDR let your analysts unearth threats using an intuitive Query Builder as well as construct advanced queries and visualize results with XQL Search. Your team can search, schedule, and save queries to unearth hard-to-find threats. By integrating threat intelligence with an extensive set of security data, your team can catch malware, external threats, and malicious insiders. The Asset Management feature reveals potential threats and streamlines network management by showing you all the devices in your environment, including managed, unmanaged, and rogue devices.

Enlist Experts for Managed Detection and Response

With the Palo Alto Networks Unit 42® Managed Detection and Response (Unit 42 MDR) service, a team of world-class analysts, hunters, and researchers work for you to investigate and respond to attacks, allowing your team to scale fast and focus on more strategic tasks. The Unit 42 team applies years of experience protecting businesses and governments around the globe to monitor your environment 24/7 and hunt for suspicious activity. Armed with industry-leading threat intelligence from over 10 years of malware analysis, augmented every day by over 30 million new malware samples and 500 billion events, our Unit 42 experts ensure you stay ahead of emerging threats.

With Cortex XDR, you can choose MDR services from Unit 42 as well as our extensive ecosystem of XMDR partners.

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

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 as well as 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.

Cortex XDR was named a Leader in The Forrester Wave™: Extended Detection And Response Platforms, Q2 2024.

Ease Deployment with Cloud Delivery

The cloud-native Cortex XDR platform revolutionizes security deployment by eliminating the need for new on-premises log storage or network sensors. At its core is a lightweight agent that can be installed and upgraded without system reboots, minimizing operational disruption. This cloud-first approach provides a scalable and efficient data repository, allowing organizations to easily store and manage security information from multiple sources.

Protecting the Cloud

Cortex XDR extends its robust protection to cloud environments, supporting both private and public cloud platforms including AWS, Google Cloud, and Microsoft Azure. This versatility ensures consistent security practices across an organization's entire IT ecosystem, regardless of where assets are hosted. Threats in the cloud are prevented at runtime, detected with analytics tuned for cloud-specific data, and are remediated with cloud-specific response actions. The platform also offers seamless integration with Kubernetes, simplifying deployment to containerized environments and protecting modern, cloud-native applications.

By safeguarding cloud workloads alongside on-premises assets, Cortex XDR provides comprehensive visibility across an organization's entire IT landscape. This unified view bridges the gap between traditional and cloud infrastructures, offering invaluable insights for security teams defending complex, hybrid environments.

Table 1: Cortex XDR License Capabilities			
	XDR Prevent	XDR Pro per Endpoint	XDR Pro per Gigabyte
Next-Generation Antivirus Block malware, ransomware, exploits, and fileless attacks	✓	✓	
Endpoint Protection Safeguard endpoints with device control, firewall, and disk encryption	✓	✓	
Detection and Response Pinpoint attacks with AI-driven analytics and coordinate response		✓	✓
Managed Detection and Response Let Unit 42 experts work for you 24/7 to detect and respond to threats		✓	✓
Managed Threat Hunting Let Unit 42 experts work for you 24/7 to discover advanced threats		✓	✓
Host Insights Find vulnerabilities and sweep across endpoints to eradicate threats		✓	
Forensics Investigation Investigate incidents swiftly with comprehensive forensics evidence collection		✓	
Third-Party Security Events Send security events from other data sources		✓	✓
Third-Party Security Logs Send raw logs from other data sources			✓
Network Traffic Analysis Syslog, Kafka, DB, CSV file, FTP, NetFlow, Windows events, Pathfinder			✓
Prisma® and Palo Alto Networks IoT Security Unify cloud and/or control system environments with XDR			✓
Integrations Threat intelligence solutions, Slack, send syslog	✓	✓	✓
Security Analytics Apply machine learning and UEBA detections to security data		✓	✓
Identity Threat Detection and Response (ITDR Module) Uncover hard-to-detect threats like insiders, lateral movement, credential compromise (includes XTHD when paired with XDR Pro per Endpoint)			✓
eXtended Threat Hunting Data (XTHD Module) Collect rich data at the endpoint to support deep threat hunting operations in an environment		✓	

Resources

Cortex XDR At a Glance

Cortex XDR Help Center

Customer Service Portal

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

cortex_ds_cortex-xdr_012425