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.

Business 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.** Find more attacks with the solution that achieved the highest number of technique detections in the 2022 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

Cortex XDR is the industry's first extended detection and response platform that stops modern attacks by integrating data from any source. With Cortex XDR, you can harness the power of AI, analytics, and rich data to detect stealthy threats. 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.

Cortex XDR delivers peace of mind with industry-leading endpoint security that achieved the highest combined protection and detection scores in the 2022 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.

Block Attacks with Best-in-Class Endpoint Protection

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.

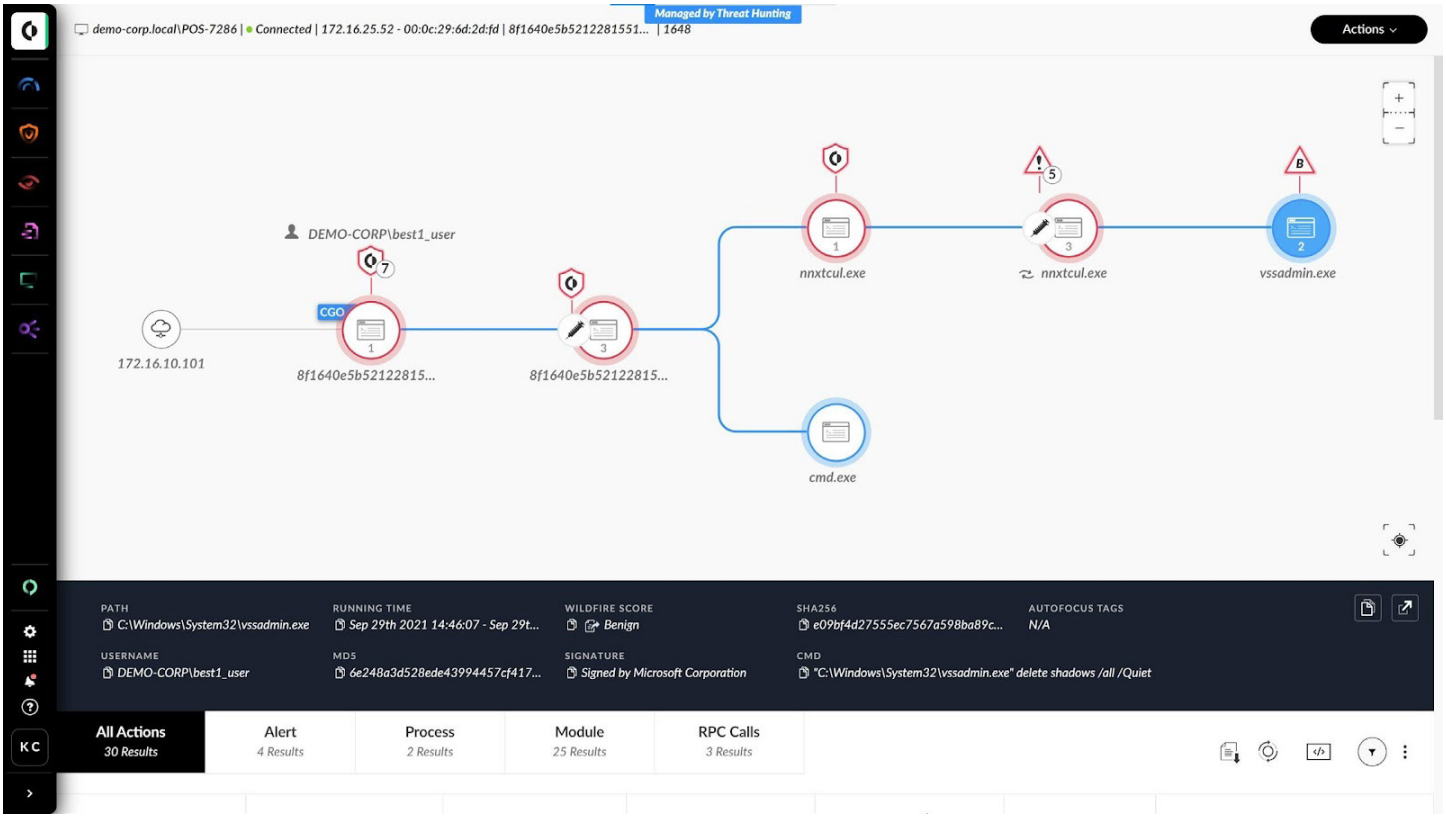

Figure 1: Cortex XDR triage and investigation view

Securely Manage USB 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.

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, you can apply BitLocker or FileVault encryption on your endpoints by creating disk encryption rules and policies. Cortex XDR provides full visibility into endpoints that were encrypted and lists all encrypted drives. Host firewall and disk encryption capabilities let you centrally configure your endpoint security policies from the Cortex XDR management console.

In the 2022 MITRE ATT&CK evaluations, Cortex XDR delivered 100% protection and 100% detection across all 19 detection steps.

Get Full Visibility Across Your Entire Environment

Cortex XDR gathers data from any source, enabling you to broaden the scope of threat hunting across all data. It 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. Cortex XDR examines logs with behavioral analytics, enabling you to find critical threats and eliminate blind spots.

Discover Threats with Analytics and Machine Learning

Cortex XDR detects advanced attacks with AI, analytics, and out-of-the-box rules, allowing your team to triage and contain threats quickly. 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). A Global Analytics feature harnesses cross-customer insights 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

Cortex XDR 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. Each incident provides a complete picture of an attack, with key artifacts and threat intelligence details, empowering your team to quickly assess the scope and impact. SmartScore incident scoring lets you focus on the threats that matter most by identifying high-risk incidents with machine learning.

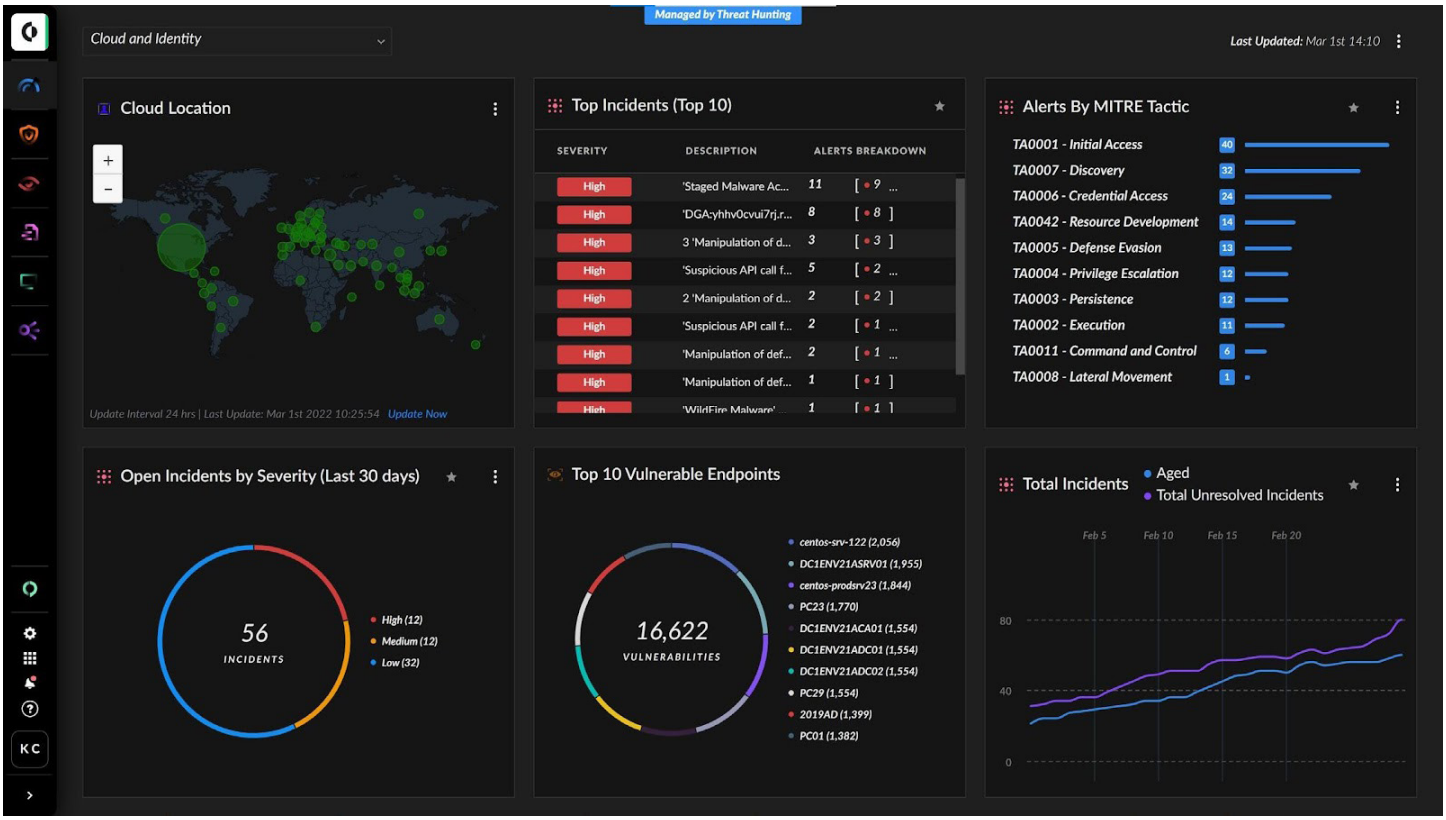

Figure 2: Customizable dashboard

Hunt for Hidden Malware, Targeted Attacks, and Insider Threats

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. An asset inventory feature reveals potential threats and streamlines network management by showing you all the devices in your environment, including managed, unmanaged, and rogue devices.

Stop Threats Quickly with Flexible Response Options

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 analysts swiftly verify and contain attacks without disrupting end users by directly accessing endpoints and running Python, PowerShell, or system commands and scripts. Analysts of all experience levels can manage files and processes from graphical file and task managers.

Gain Unprecedented Visibility and Response with Host Insights

Host Insights helps you swiftly find and eradicate threats by delivering vulnerability assessment, host inventory, and Search and Destroy. Vulnerability assessment provides you with real-time visibility into vulnerability exposure and current patch levels across your endpoints. Host inventory presents detailed information about your host applications and settings, while Search and Destroy lets you swiftly find

and eliminate threats across all endpoints. 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.

Accelerate Incident Response with Forensics

Cortex XDR Forensics is a powerful triage and investigation solution that lets you review evidence, hunt for threats, and perform compromise assessments from one console. With its deep data collection, Cortex XDR Forensics provides you with instant access to a wealth of forensics data and artifacts—including volatile memory—so you can determine the source of an attack and what, if any, data was accessed. Designed by incident responders for incident responders, it simplifies investigations, so you can trace every move an adversary made and swiftly contain threats from the Cortex XDR console.

Orchestrate, Automate, and Enrich with Cortex XSOAR

Cortex XDR tightly integrates with Cortex XSOAR, the industry's top security orchestration, automation, and response (SOAR) platform, enabling your teams to feed incident data into Cortex XSOAR for automated playbook-driven response that spans more than 800+ product integrations and promotes cross-team collaboration. Cortex XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks. It also unlocks the power of your threat intelligence by giving you unmatched visibility into the global threat landscape, linking threat information to incidents in real time and automating the distribution of your threat intelligence at scale.

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 endpoints with customizable dashboards as well as summarize incidents and security trends with reports. 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: Endpoint Security Software As A Service, 2021

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 30M new malware samples and 500B 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.

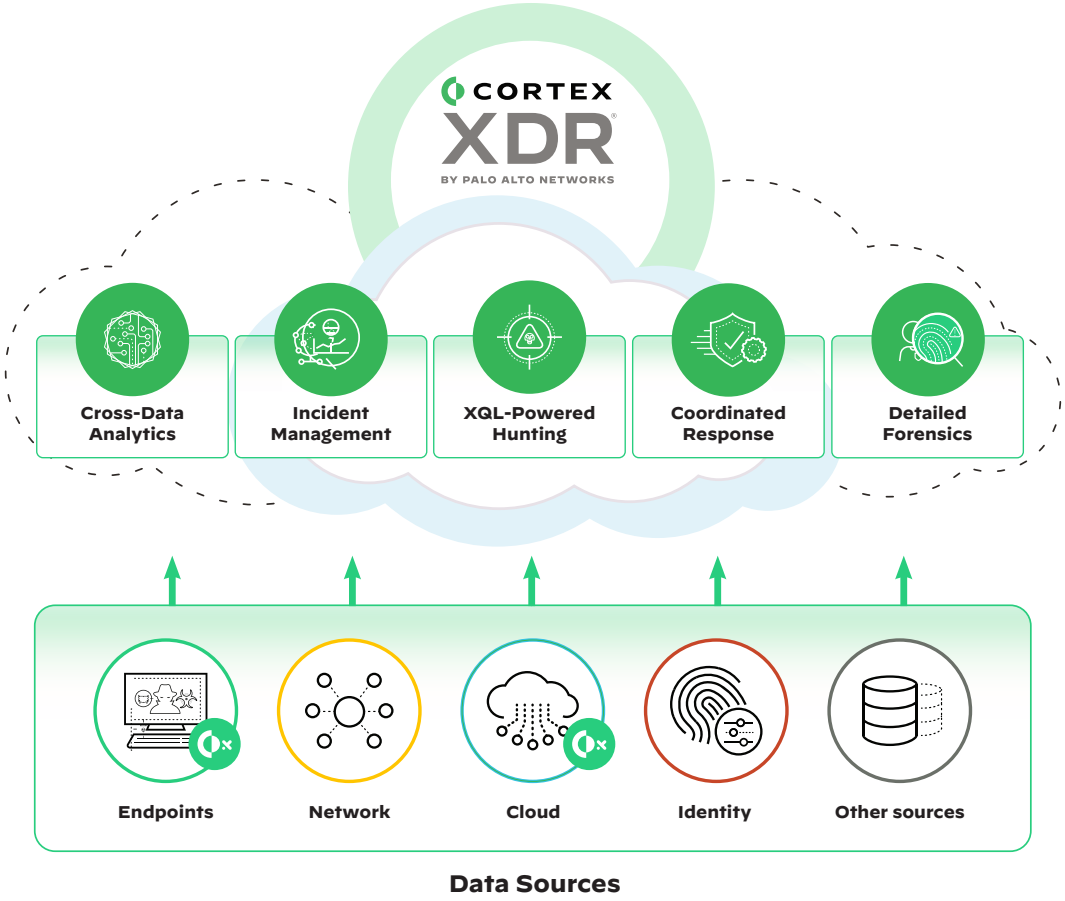

Figure 3: Analysis of data from any source for detection and response

Table 1: Cortex XDR Benefits	
Block known and unknown attacks with powerful endpoint protection.	Prevent exploits, malware, ransomware, and fileless attacks with AI-based local analysis and Behavioral Threat Protection.
Stop breaches and eliminate blind spots with full visibility.	Gather data from any source, including third-party firewalls, identity providers, cloud providers, ATM devices, HR applications, DNS servers, and more for 360-degree visibility.
Automatically integrate data for cross-data insights.	Uncover advanced attacks and gain additional context for investigations by automatically stitching together endpoint, network, cloud, and identity data. Accelerate investigations by instantly viewing the endpoint events associated with network or cloud alerts.
Uncover advanced attacks with cross-data analytics and ML.	Detect nation-state attacks, insider threats, and other covert activity by profiling behavior and identifying adversary tactics.
Avoid alert fatigue and analyst burnout.	Simplify investigations with automated root cause analysis and intelligent alert grouping, drastically reducing the number of individual alerts to review by up to 98% and lowering the skill required to triage alerts.
Increase SOC productivity.	Consolidate triage, investigation, orchestration, and response across all data in one console, and display the root cause of alerts with one click, improving SOC efficiency.
Force multiply your security team.	Disrupt every stage of an attack by detecting indicators of compromise (IoCs) and anomalous behavior as well as prioritizing analysis with SmartScore incident scoring.
Eradicate threats without business disruption.	Shut down attacks with surgical precision while avoiding user or system downtime with Live Terminal.
Restore hosts to a clean state.	Rapidly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys using remediation suggestions.

Table 1: Cortex XDR Benefits (continued)	
Extend detection, monitoring, and investigation into cloud environments.	Integrate cloud data, including host data, traffic logs, audit logs, and Prisma Cloud logs, with endpoint and network data. The Cortex XDR agent provides built-in, host-level support for Linux Kubernetes containers across Google Kubernetes (GKE), Amazon Elastic Kubernetes Service (EKS), and Azure Kubernetes Service (AKS).
Improve the ROI of your SOC.	Lower your total cost of ownership (TCO) and improve your security posture by eliminating siloed, on-premises tools, cutting SIEM expenses, and automating SecOps tasks.

Ease Deployment with Cloud Delivery

The cloud-native Cortex XDR platform offers streamlined deployment, eliminating the need to deploy new on-premises log storage or network sensors. You can install and upgrade the lightweight Cortex XDR agent without rebooting your endpoints. To protect cloud workloads, you can install the Cortex XDR agent in private and public cloud environments, including AWS, Google Cloud, and Microsoft Azure. Kubernetes integration eases deployment to containers.

While Cortex XDR only needs one source of data to stop threats, additional data sources eliminate blind spots and reduce response time with cross-data insights. You can easily store data in a scalable and efficient cloud-based data repository. By integrating data from multiple sources together, automating tasks, and simplifying management, Cortex XDR increases SOC efficiency and lowers costs compared to siloed security tools.

Cortex XDR Features

Detection Capabilities

- Behavioral analytics powered by machine learning
- Custom and hundreds of out-of-the-box rules to detect attacker tactics, techniques, and procedures
- Global Analytics powered by cross-customer data
- Identity Analytics for user behavior analytics (UBA)
- Full endpoint detection and response (EDR), network detection and response (NDR), and cloud detection and response (CDR)

Investigation, Forensics, and Risk Management Capabilities

- Root cause analysis and timeline analysis of alerts
- Incident management with intelligent alert grouping
- SmartScore incident scoring powered by machine learning
- MITRE ATT&CK visualization
- Endpoint, endpoint group, and data source tagging
- Cross-data insights that link network, identity, and cloud alerts to endpoint data
- Asset inventory and rogue device discovery
- Optional vulnerability assessment and host inventory with a Host Insights add-on
- Optional forensics capabilities for incident response with a Forensics add-on

Threat Hunting Capabilities

- XQL Search for advanced threat hunting and querying, including filtering, visualization, and aggregation
- WildFire malware prevention service for incident artifacts
- VirusTotal threat intelligence integration
- Optional high-fidelity Unit 42 threat intelligence feed for enrichment, hunting, and investigations with Cortex XSOAR
- Optional Unit 42 Managed Threat Hunting and Unit 42 MDR services

Response Capabilities

- Network isolation of endpoints
- Endpoint script execution using Python scripts

- Blocking, quarantine, or removal of files
- Host restore with one to two clicks using remediation suggestions
- Process termination
- Optional Search and Destroy to swiftly find and delete malware by indexing files with Host Insights
- Live Terminal for direct endpoint access, task management, and file management
- Public APIs for protection, response, and data collection
- Firewall integration using external dynamic lists to block network traffic

Endpoint Protection Capabilities

- Behavioral Threat Protection
- AI-based local analysis engine
- Deep network inspection engine to block network intrusions and worms
- WildFire integration for cloud-based malware analysis
- Kernel protection
- Ransomware protection module
- Credential theft protection
- Exploit prevention by technique
- Child process protection
- Behavior-based web shell protection
- Customizable prevention rules
- Device control for USB device management
- Host firewall
- Disk encryption with BitLocker and FileVault

Data Collection and Processing

- Data ingestion from virtually any source
- Automated stitching of endpoint, network, cloud, and identity data
- Data normalization and data aggregation
- Custom parsing rules
- Flexible data collection methods, including HTTP collector, XDR Connector agent, Cortex XDR agent, Google Cloud, Amazon Web Services (AWS), plus Broker VM collection of syslog, CSV, FTP, Kafka, Database, Files and Folders, and more

Management and Log Storage Capabilities

- Intuitive web user interface
- Role-based access control and scope-based access control
- Graphical reports and widget-driven dashboards
- Email, Slack, and syslog log forwarding and notifications
- Multi-factor authentication and single sign-on for administration
- Management audit logs
- Automatic or manual cloud-delivered agent upgrades
- Automatic security content updates
- Scheduled and on-demand malware scanning
- Optional event forwarding of telemetry
- Optional Hot Storage and Cold Storage

Managed Detection and Response Capabilities

- 24/7/365 monitoring, triage, and investigation of Cortex XDR alerts and incidents
- Guided or full threat remediation actions

Table 2: Cortex XDR Subscription Offerings			
	XDR Prevent	XDR Pro per Endpoint	XDR Pro per TB
Subscription Model	Per User	Per User	Per TB
Delivery Model	Cloud-delivered service	Cloud-delivered service	Cloud-delivered service
Incident Management	✓	✓	✓
Endpoint Threat Prevention	✓	✓	—
Threat Detection and Investigation	—	Endpoint Data	Network, cloud, third-party data
Response	✓	✓	✓
Host Insights	—	Optional	—
Forensics	—	Optional	—
Alert Forwarding	✓	✓	✓
Event Forwarding of Telemetry	—	Optional	Optional
Data Retention	30 days standard	30 days standard; Hot and Cold Storage options	30 days standard; Hot and Cold Storage options
Unit 42 Managed Threat Hunting	—	Optional	Optional
Unit 42 Managed Detection and Response	—	Optional	Optional

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