Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom detection rules.
- **Reduce alerts by 98%:** 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%.

Cortex XDR

Safeguard Your Entire Organization with the Industry's First Extended Detection and Response Platform

Security teams are inundated with inaccurate, incomplete alerts. Today's siloed security tools force analysts to pivot from console to console to piece together investigative clues, resulting in painfully slow investigations and missed attacks. Even though they've deployed countless tools, teams still lack the enterprise-wide visibility and deep analytics needed to find threats. Faced with a shortage of security professionals, teams must simplify operations.

Prevent, Detect, Investigate, and Respond to All Threats

Cortex XDR™ is the world's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. Combined with our Managed Threat Hunting service, Cortex XDR gives you round-the-clock protection and industry-leading coverage of MITRE ATT&CK® techniques.

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 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.

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. Visit us online to read more about endpoint protection.

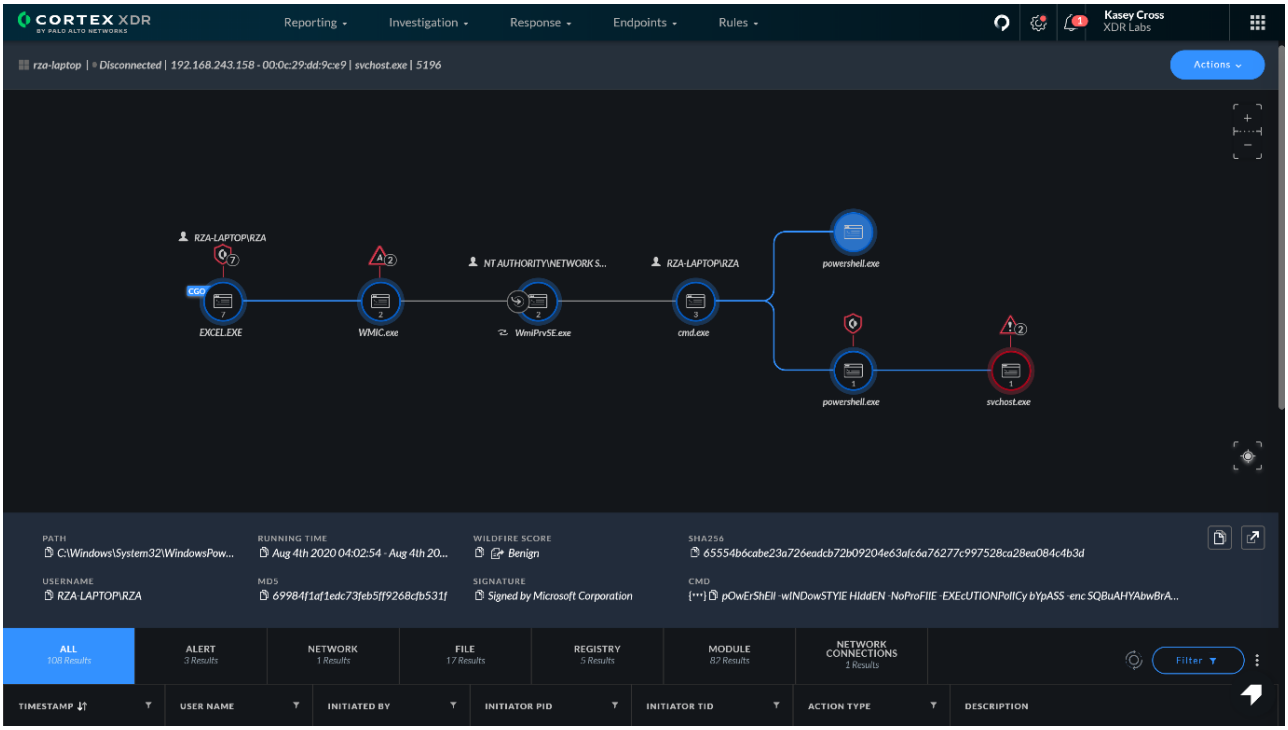

Figure 1: Cortex XDR triage and investigation view

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.

Protect Endpoint Data with Host Firewall and Disk Encryption

Reduce the attack surface of your endpoints. 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.

Get Full Visibility with Comprehensive 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 Threat 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.

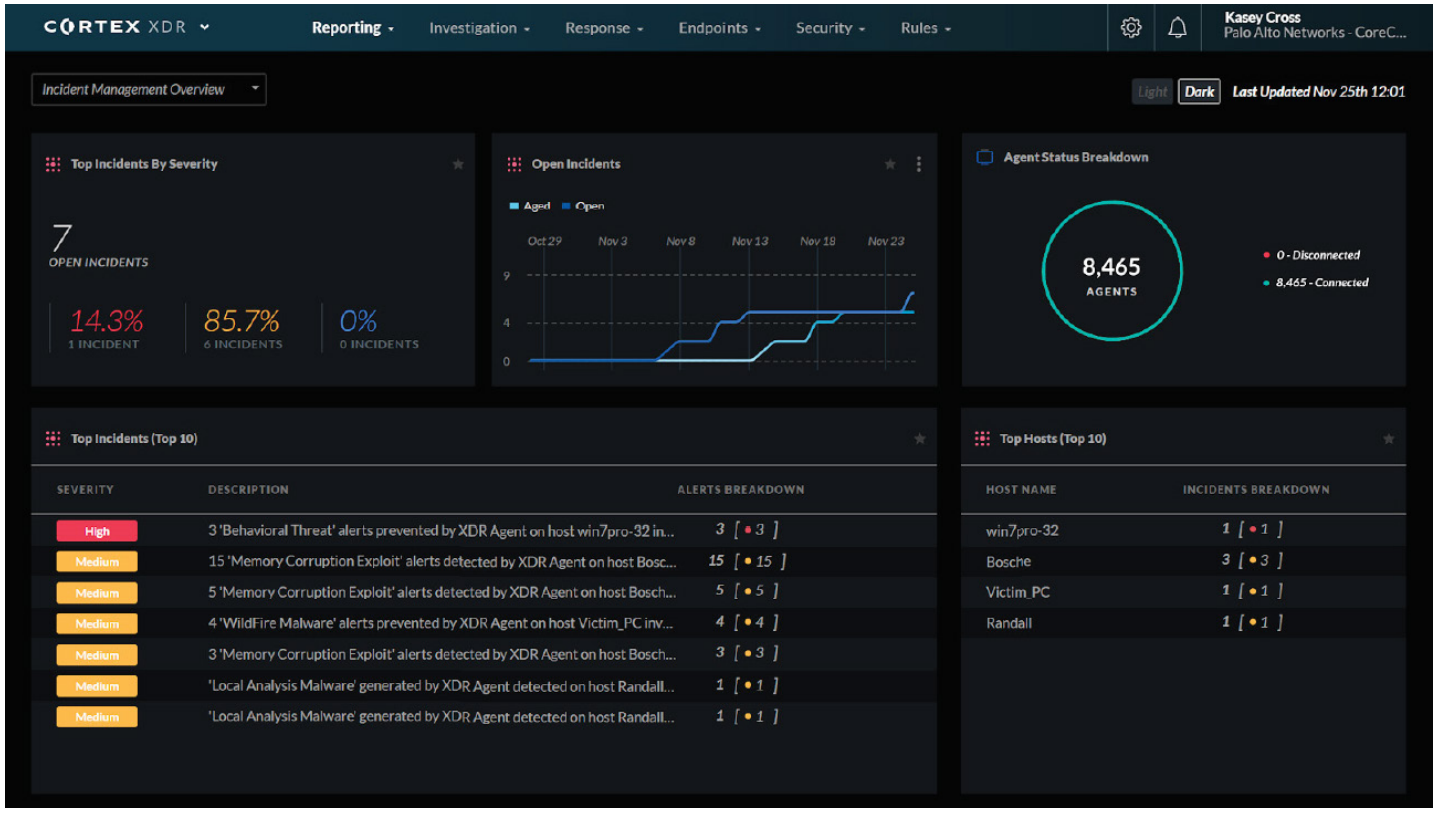

Figure 2: Customizable dashboard

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 for 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 unearth threats using an intuitive Query Builder as well as construct advanced queries and visualize results with XQL Search. By integrating threat intelligence with an extensive set of security data, your team can catch malware, external threats, and malicious insiders. An Asset Management feature streamlines network management and reveals potential threats by showing you all the devices in your environment, including managed and unmanaged devices.

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.

Get Unprecedented Visibility and Swift Response with Host Insights

Understand your risks and contain threats quickly before they can spread. Host Insights, an add-on module for Cortex XDR, combines vulnerability management, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Vulnerability Management provides you 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 eradicate threats across all endpoints. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breaches.

24/7 Threat Hunting Powered by Cortex XDR and Unit 42 Experts

Augment your team with the industry's first threat hunting service operating across endpoint, network, and cloud data. Cortex XDR Managed Threat Hunting offers round-the-clock monitoring from world-class threat hunters to discover attacks anywhere in your environment. Our Unit 42 experts work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware. To detect adversaries hiding in your organization, our hunters comb through comprehensive data from Palo Networks and third-party security solutions. Detailed Threat Reports reveal the tools, steps, and scope of attacks so you can root out adversaries quickly, while Impact Reports help you stay ahead of emerging threats.

Natively Integrate with Cortex XSOAR for Security Orchestration and Automation

Standardize and automate response processes across your security product stack. Cortex XDR integrates with Cortex™ XSOAR, our security orchestration, automation, and response platform, enabling your teams to feed incident data into Cortex XSOAR for automated, playbook-driven response that spans more than 450 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.

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 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.

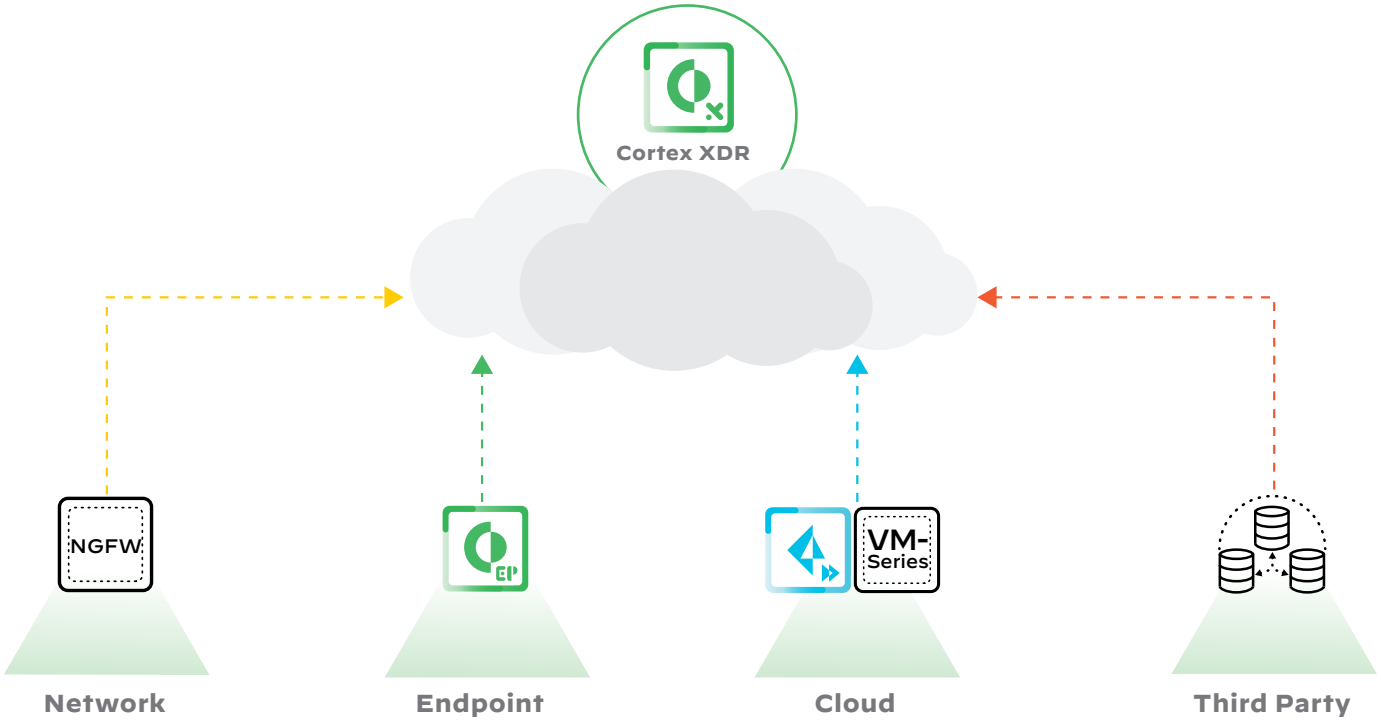

Figure 3: Analysis of data from any source for detection and response

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 98% reduction in alerts and lowering the skill required to triage alerts.

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 indicators of compromise (IOCs), anomalous behavior, and malicious patterns of activity.

Restore hosts to a clean state: Simplify response with recommended next steps for remediation. You can rapidly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys.

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.

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.

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	Machine learning-based behavioral analytics
Third-party alert and log ingestion from any source with required network information	Custom rules to detect tactics, techniques, and procedures
Third-party log data from Check Point, Fortinet, Cisco ASA firewalls, Okta, PingOne, Azure Active Directory, Google Cloud, and Windows Event Collector	Root cause analysis of alerts
Host Insights add-on module, providing Vulnerability Management, Search and Destroy, and Host Inventory	Asset management
Cortex XDR Managed Threat Hunting service	Timeline analysis of alerts
Malware and fileless attack detection	Unified incident engine
Detection of targeted attacks, malicious insiders, and risky user behavior	Post-incident impact analysis
Network detection and response (NDR) and user behavior analytics (UBA)	Dashboards and reporting
Endpoint detection and response (EDR)	Threat intelligence integration
Native integration with Cortex XSOAR for orchestration, automation, and response	Threat hunting
Incident management	Incident response and recovery
Endpoint Protection Capabilities	
Malware, ransomware, and fileless attack prevention	Customizable prevention rules (available with Cortex XDR Pro)
Behavioral Threat Protection	Endpoint script execution (available with Cortex XDR Pro)
AI-based local analysis engine	Network isolation, quarantine, process termination, file deletion, file block list
Cloud-based malware prevention with WildFire	Live Terminal for direct endpoint access
Child process protection	Remediation suggestions for host restore (available with Cortex XDR Pro)
Exploit prevention by exploit technique	Public APIs for response and data collection
Device control for USB device management	Credential theft protection
Host firewall	Scheduled and on-demand malware scanning
Disk encryption with BitLocker and FileVault	Optional automatic agent upgrades
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Reduction of MTTD and MTTR
Investigation of every alert and incident generated by Cortex XDR	Custom tuning of Cortex XDR for enhanced prevention, visibility, and detection
Guided or full threat remediation actions	Direct access to partners' analysts and forensic experts

Table 1: Cortex XDR Features and Specifications (continued)	
Specification	**Cortex XDR**
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 Managed Threat Hunting subscription	24/7 threat hunting powered by Cortex XDR and Unit 42 experts
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 Cortex XSOAR, enabling 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, Chrome® OS, 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.

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

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.
cortex-xdr-ds-110920