Cortex XDR

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

Security teams face too many alerts, too many tools, and too many missed attacks; today's siloed security solutions can't keep up with evolving threats. Even when security teams deploy dozens of tools, they still lack the enterprise-wide visibility and deep analytics they need to stop attacks. Faced with a shortage of security talent, teams need a radical new approach to detection and response.

Business Benefits

- **Detect advanced attacks with analytics:** Uncover threats with AI, behavioral analytics, and custom correlation 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.
- **Improve endpoint performance:** Block advanced malware, exploits, and fileless attacks with one lightweight agent.
- **Maximize ROI:** Consolidate tools and simplify operations to lower SOC costs by 44%.

Prevent, Detect, and Respond to All Threats

Cortex® XDR™ is the world's first extended detection and response platform that gathers and integrates all security data to stop sophisticated attacks. It unifies prevention, detection, investigation, and response in one platform for unrivaled security and operational efficiency. With the highest combined detection and protection scores in the MITRE ATT&CK® round 3 evaluation, Cortex XDR lets you rest easy knowing your data is safe.

Block 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.

Detect Stealthy Threats with 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.

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 Endpoints 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.

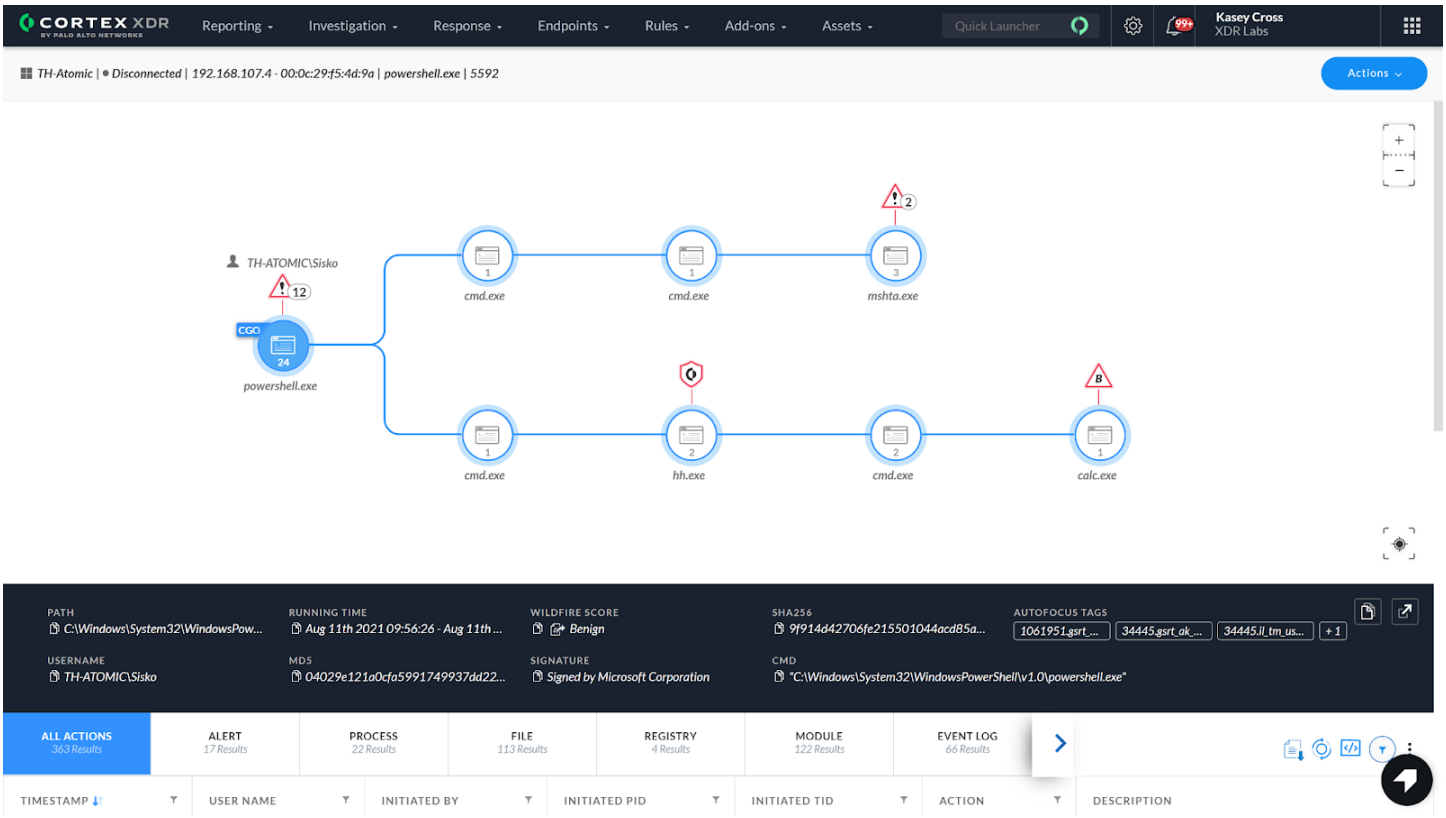

Figure 1: Cortex XDR triage and investigation view

Get Full Visibility with Comprehensive Data

Break security silos by integrating all data. Cortex XDR gathers data from any source, enabling you to broaden the scope of threat hunting across your entire environment. 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 any visibility blind spots.

Discover Threats with Analytics and Machine Learning

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. An Identity Analytics feature provides a 360-degree view of users, including user risk scores. By applying analytics to an integrated set of data, Cortex XDR meets and exceeds the detection capabilities of siloed network detection and response (NDR), endpoint detection and response (EDR), and user behavior analytics (UBA) tools.

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.

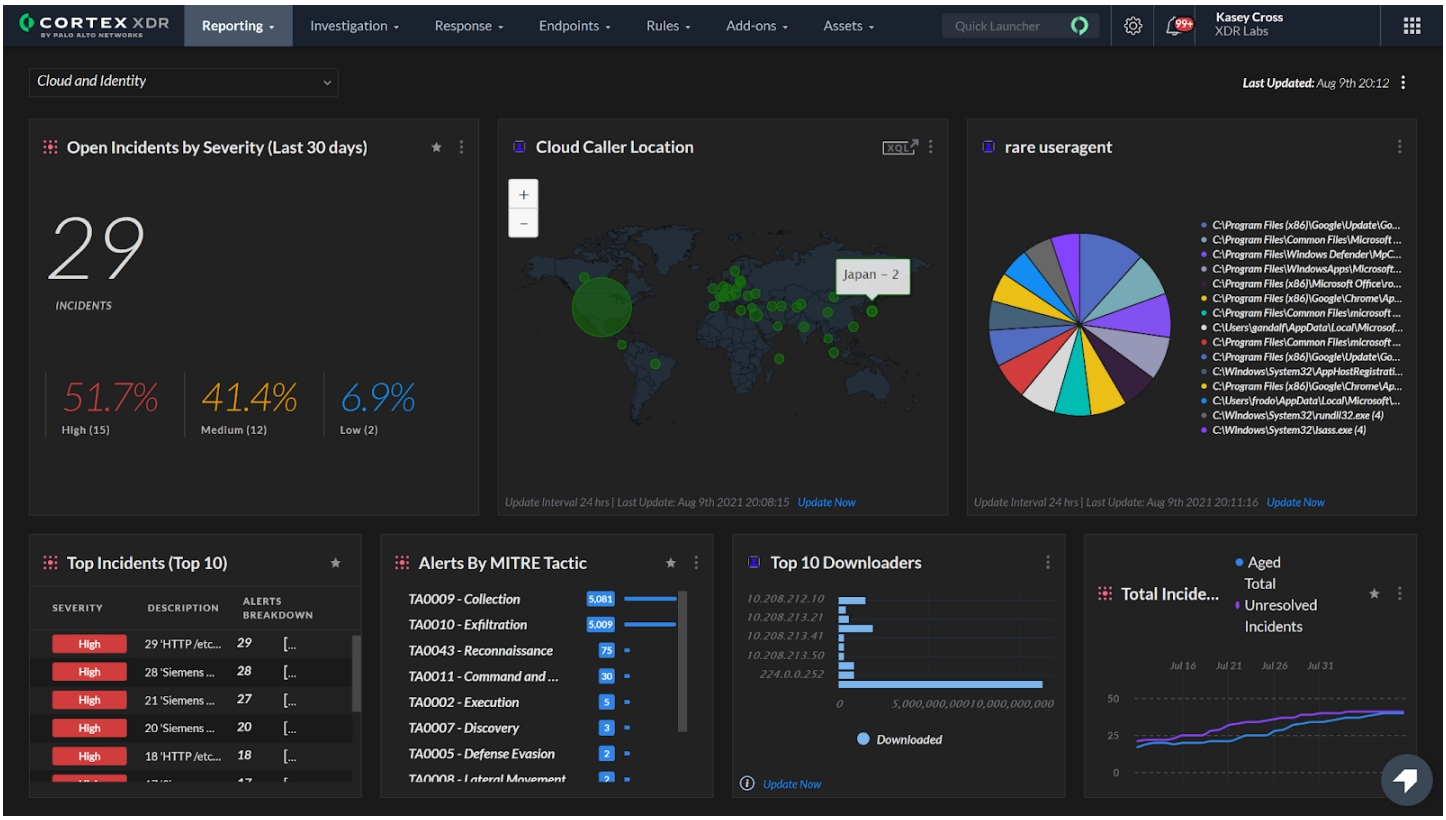

Figure 2: Customizable dashboard

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 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.

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 assessment, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Vulnerability Assessment 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.

Benefit from 24/7 Managed Threat Hunting

Augment your team with the industry's first threat hunting service operating across all 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. 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.

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. The Cortex XDR Forensics add-on module, with its deep data collection, provides you instant access to a wealth of forensics artifacts and enables you to 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.

Integrate with Cortex XSOAR for Security Orchestration and Automation

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 700+ 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.

FORRESTER® WAVE LEADER 2021 Endpoint Security Software As A Service

Cortex XDR was named a Leader in the 2021 Forrester Wave: Endpoint Security Software As A Service

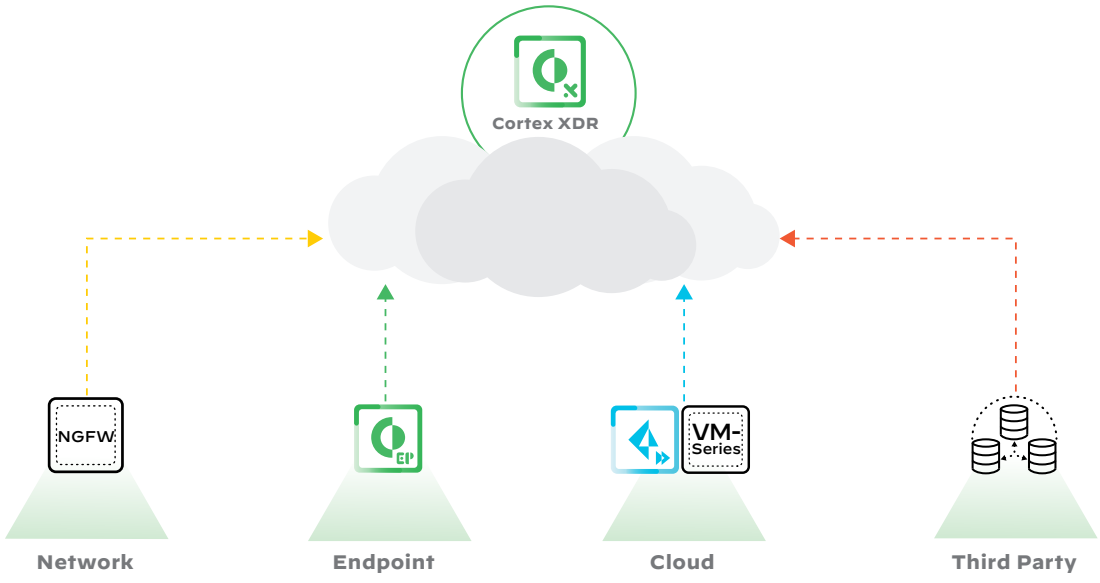

Figure 3: Analysis of data from any source for detection and response

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.

Extend detection, investigation, and threat hunting to all data: Gather data from any source, including third-party firewalls, identity providers, cloud providers, ATM devices, HR applications, DNS servers, and even access card readers for 360-degree visibility.

Extend detection, monitoring, and investigation into cloud environments: Integrate cloud host data, traffic logs, audit logs, data from Palo Alto Networks' industry-leading Prisma Cloud product, and third-party cloud security data with non-cloud endpoint and network data sources. 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).

Automatically detect sophisticated attacks 24/7: Use AI-based analytics and custom correlation 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 monitoring, investigation, and response across all your data in one console, and display the root cause of any alert with one click, improving SOC efficiency.

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

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

Supercharge your security team: Disrupt every stage of an attack by detecting indicators of compromise (IOCs) and anomalous behavior as well as prioritizing analysis with incident scoring.

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.

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 log storage or network sensors. You can install the Cortex XDR agent without rebooting your endpoints. To protect cloud workloads, you can install the Cortex XDR agent in AWS, Google Cloud, and Microsoft Azure cloud platforms. Kubernetes integration eases deployment to containers.

You only need one source of data 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

Endpoint Protection Capabilities	
Behavioral Threat Protection to block malicious actions or combinations of behavior	Device control for USB device management
AI-based local analysis engine	Host firewall
Deep network inspection engine to block network intrusions	Disk encryption with BitLocker and FileVault
WildFire integration for cloud-based malware analysis	Kernel protection
Ransomware protection module	Credential theft protection
Exploit prevention by exploit technique	Child process protection

Table 1: Cortex XDR Features and Specifications (continued)	
Response Capabilities	
Live Terminal for direct endpoint access	Customizable prevention rules (available with Cortex XDR Pro)
Network isolation	Endpoint script execution (available with Cortex XDR Pro)
File quarantine and file removal	Host restore (available with Cortex XDR Pro)
Process termination	Native integration with Cortex XSOAR for orchestration, automation, and response
File block list	Public APIs for protection, response, and data collection
Detection and Investigation Capabilities	
Data ingestion from any source for threat hunting and detection	Behavioral analytics powered by machine learning
Automated stitching of endpoint, network, cloud, and identity data	Custom rules and correlation rules to detect attacker tactics and techniques
Endpoint detection and response (EDR)	Root cause analysis and timeline analysis of alerts
Network detection and response (NDR)	Incident management and incident scoring
Identity Analytics for user behavior analytics	MITRE ATT&CK visualization
Forensics add-on module for incident response	Threat hunting with XQL Search
Host Insights add-on module for vulnerability assessment, host inventory, and Search and Destroy	Threat intelligence integration
Cortex XDR Managed Threat Hunting service	Asset management and rogue device discovery
Management Capabilities	
Intuitive web user interface	Role-Based Access Control and Scope-Based Access Control
Graphical reports and custom dashboards	Email, Slack, and syslog log forwarding and notifications
Multi-factor authentication for administration	Management audit logs
Optional automatic agent upgrades	Scheduled and on-demand malware scanning
Partner-Delivered MDR Service Benefits	
24/7 year-round monitoring and alert management	Reduction of MTTD and MTTR
Investigation of alerts and incidents 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 2: Cortex XDR Technical Specifications	
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	• Endpoint protection with Cortex XDR agents • Detection, investigation, and response across endpoint data sources
Cortex XDR Pro per TB subscription	• Detection, investigation, and response across network, cloud, and third-party data sources
Cortex XDR Managed Threat Hunting subscription	• 24/7 threat hunting powered by Cortex XDR and Unit 42 experts

Table 2: Cortex XDR Technical Specifications (continued)	
Specification	**Cortex XDR**
Cortex XDR agent operating system and virtual application support	• Windows • macOS • Linux • Chrome® OS • Android® • Citrix Virtual Apps and Desktops • Citrix App Layering • VMware AppVolumes • VMware Horizon View • VMware ThinApp • Windows Virtual PC • Virtual machines (VMs) and containers For a complete list of system requirements and supported operating systems, please visit the Palo Alto Networks Compatibility Matrix.
Cortex XDR Pathfinder endpoint analysis service	• Collects process information from endpoints that do not have Cortex XDR agents; included with all Cortex XDR subscriptions • Cortex XDR Pathfinder minimum requirements: 2 CPU cores, 8 GB RAM, 128 GB thin-provisioned storage, VMware ESXi TM V5.1 or higher, or Microsoft Hyper-V® 6.3.96 or higher hypervisor

paloalto® NETWORKS | Cybersecurity Partner of Choice

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087