CORTEX XDR

Hunt down and stop stealthy attacks by unifying network, endpoint, and cloud data

Business Benefits

- **Automatically uncover stealthy attacks:** Continuously detect threats with machine learning, behavioral analytics, and custom detection rules.
- **Stop alert fatigue and attrition:** Validate security alerts in seconds, improving analyst productivity and morale by reducing the backlog.
- **Reduce mean time to identify (MTTI):** Combine precise attack detection with rapid alert triage to drastically cut dwell time.
- **Reduce mean time to contain (MTTC):** Investigate and accurately respond to external attacks and insider threats, without years of experience.
- **Increase ROI from current investments with Cortex:** Solve all your security needs through an ecosystem of trusted apps, while using existing infrastructure as sensors and enforcement points.

Break Down Silos to Simplify Your Investigations

Security teams often lack the visibility and automation required to stop attacks. Siloed tools like endpoint detection and response (EDR) and network traffic analysis (NTA) collect large amounts of data, but they also force analysts to pivot from console to console to verify threats, increasing complexity and slowing down investigations. Faced with a shortage of cybersecurity professionals, teams must simplify their operations, or they will struggle to investigate and stop attacks.

Quickly Detect, Investigate, and Respond to Threats

Cortex XDR detection and response natively integrates network, endpoint and cloud data to stop sophisticated attacks. Leveraging behavioral analytics, it identifies unknown and highly evasive threats targeting your network with behavioral analytics. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

Cortex XDR speeds alert triage and incident response by providing a complete picture of each threat and revealing the root cause automatically. By stitching different types of data together and simplifying investigations, Cortex XDR reduces the time and experience required at every stage of security operations, from triage to threat hunting. Tight integration with enforcement points lets you respond to threats quickly as well as apply the knowledge gained from investigations to detect similar attacks in the future.

Protect Against Known and Unknown Threats with Traps

Great security starts with ironclad prevention. Traps™ endpoint protection and response, included with Cortex XDR, uses multiple methods of prevention to safeguard endpoints from malware, ransomware, and exploits. Together, Traps and Cortex XDR deliver consistent prevention, detection, and response across all your digital assets. Native integration with cloud-based threat intelligence ensures prevention is coordinated across your network, endpoint, and cloud security products.

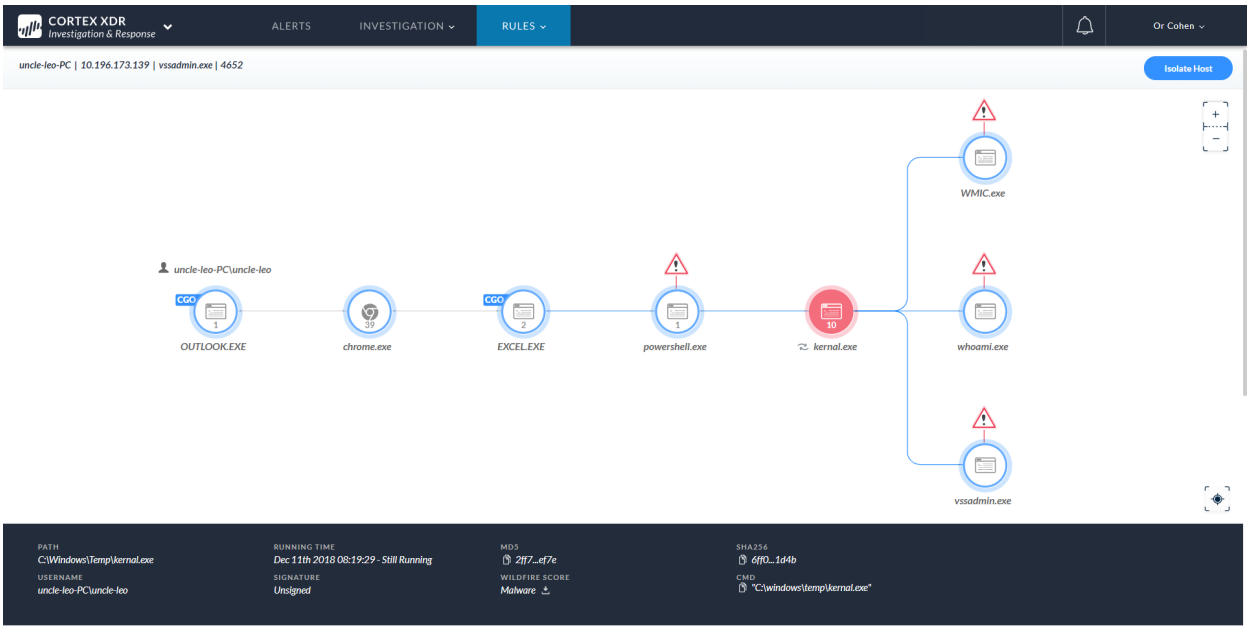

Figure 1: Cortex XDR dashboard

Key Capabilities

Gain Complete Visibility

Correlate network, endpoint, and cloud data to streamline detection and response. Cortex XDR saves hours of manual analysis by automatically correlating data collected from your network, endpoints, and cloud assets. It stitches disparate data types together within the Cortex Data Lake, a scalable and efficient cloud-based data store, to accurately detect attacks and simplify investigations.

Automate Attack Detection with AI

Find stealthy threats with behavioral analytics. Cortex XDR automatically pinpoints active attacks, allowing your team to triage and contain threats before the damage is done. Using machine learning, Cortex XDR continuously profiles user and device behavior to detect anomalous activity indicative of attacks. By examining rich data built expressly for analytics, Cortex XDR can detect attacks such as credential theft and tunneled DNS threats, which are nearly impossible to identify from standard threat logs or high-level network flow data. Automated detection works all day, every day, providing you peace of mind.

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 indicators of compromise (IoCs) 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 occured in the past.

Instantly Investigate Events

Automatically reveal the root cause of every alert. With Cortex XDR, your analysts can analyze alerts from any source 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 needed for accurate validation. A forensic timeline of all attack activity provides actionable detail for incident investigations, allowing analysts to determine the scope, damage, and next steps in seconds.

Coordinate Response Across Enforcement Points

Stop threats with fast and accurate remediation. Cortex XDR lets your security team instantly contain network, endpoint, and cloud threats from one console. Your analysts can quickly stop the spread of malware, restrict network activity to and from devices, and update threat prevention lists like bad domains through tight integration with enforcement points. With Cortex XDR, you can swiftly shut down advanced attacks while gaining more value from your existing investments.

Adapt Your Defenses to Stop Future Attacks

Detect attackers' tactics, techniques, and procedures with behavioral rules. With Cortex XDR, your team can apply knowledge from each investigation to reduce your attack surface and streamline future investigations, shifting your security posture from reactive to proactive. Your analysts can also create granular behavioral rules that detect malicious activity unique to your network. Flexible informational alerts improve timeline analysis by identifying suspicious behavior and making complex events easy to understand.

Get Industry-Leading Endpoint Protection

Use a single agent for endpoint threat prevention and data collection. Your Cortex XDR subscription includes unlimited Traps agents, offering the best endpoint protection available. Traps lets you stop known and unknown malware, exploits, and ransomware by blocking malicious behavior and techniques. Integrated, cloud-based malware analysis with Palo Alto Networks WildFire® malware prevention service improves accuracy and coverage. The Traps agent records all endpoint activity, forwards it to the Cortex Data Lake for analysis, and orchestrates response.

Ease Deployment with Cloud Delivery

Get started in minutes. As a cloud-based app, Cortex XDR offers simple, zero-touch deployment, eliminating the need to deploy new on-premises log collectors or sensors. It uses your existing Palo Alto Networks products as sensors and enforcement points, reducing the number of products you need to manage. If you're a new customer, you only need to deploy one type of sensor, such as next-generation firewalls or Traps, to detect and stop threats with Cortex XDR. Cortex XDR is built on Cortex, the industry's only open AI-based continuous SOC platform. It delivers new levels of simplicity in security operations and significantly improved security outcomes through automation and unprecedented accuracy.

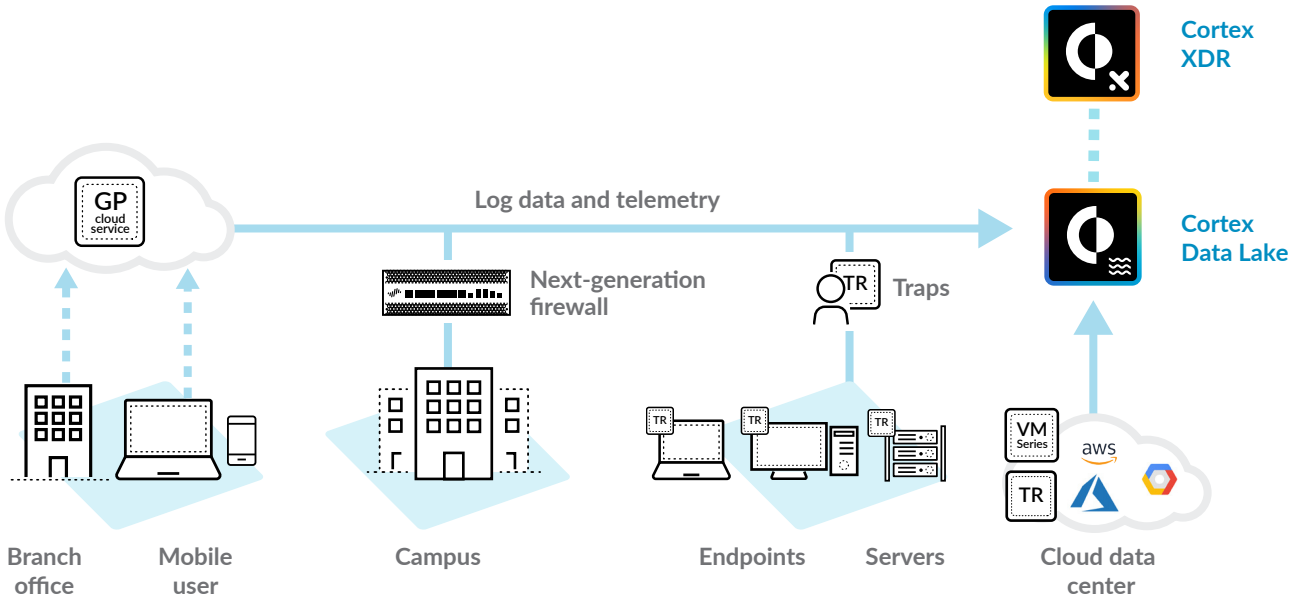

Figure 2: Analysis of data from any source for cross-environment detection and response

Operational Benefits

Achieve visibility across network, endpoint, and cloud data: Collect and correlate network, endpoint, and cloud data at scale for use in detection, triage, investigation, response, and hunting.

Automatically detect sophisticated attacks 24/7: Use always-on machine learning and custom rules to detect advanced persistent threats and other sophisticated attacks.

Eliminate the alert backlog: Simplify investigations with automated root cause analysis and timeline views, lowering the skill required to evaluate and analyze 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: Streamline operational processes to a single console by consolidating alert triage, investigation, and response across your network, endpoint, and cloud environments.

Remediate without business impact: 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.

Cortex XDR Features	
Automated alert investigation	Custom behavior-based detection
Root cause analysis	Supervised and unsupervised machine learning
Incident response	Malware and fileless attack detection
Incident containment and recovery	Targeted attack detection
Post-incident impact analysis	Insider threat detection
Threat hunting	Risky user behavior analysis
IoC and threat intelligence searches	Malware, ransomware, and exploit prevention with Traps

Technical Specifications	
Delivery model	Cloud-delivered application
Data retention	30-day to unlimited data storage

Operating System Support

Traps supports multiple endpoints across Windows®, macOS®, and Linux operating systems. For a complete list of system requirements and supported operating systems, please visit the Traps 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.

Cortex XDR licensing includes:

- Cortex XDR – Analytics app
- Cortex XDR – Investigation and Response app
- Traps endpoint protection and response
- Cortex XDR – Pathfinder endpoint analysis service (agentless alternative to Traps)

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-022219