paloalto NETWORKS

CORTEX™
BY PALO ALTO NETWORKS

Bolster Your Endpoint Security: Upgrade to Cortex XDR

Reasons to Upgrade

With Cortex XDR, you can:

- Stop malware with AI-based local analysis and Behavioral Threat Protection
- Reduce risks with disk encryption, device control, and host firewall
- Simplify operations with cloud native management
- Get optional detection and response across network, endpoint, and cloud assets
- Enjoy industry-leading coverage of attack techniques, according to MITRE ATT&CK® testing.

MITRE | ATT&CK®

Cortex XDR™ gives you everything you need to secure your endpoints, with best-in-class endpoint protection, device control, disk encryption, and host firewall in one lightweight endpoint agent.

If you already have Traps™ advanced endpoint protection, you're entitled to upgrade to Cortex XDR Prevent at no additional cost. Cortex XDR eliminates malware, exploits, and fileless attacks with all-new endpoint defenses, including a rebuilt AI-driven local analysis engine and cloud-backed Behavioral Threat Protection. The Cortex XDR agent integrates with the WildFire® malware prevention service for coordinated malware prevention across your network, endpoint, and cloud security.

Take Your Security to the Next Level with Powerful Endpoint Protection

Cortex XDR provides the most comprehensive prevention available, unifying multiple complementary engines to stop every step of an endpoint attack. The Cortex XDR agent includes a broad set of exploit protection modules 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 analyzes the behavior of multiple, related processes to uncover attacks as they occur. WildFire integration boosts security accuracy and coverage.

Scheduled and on-demand malware scanning reveals dormant malware, satisfying compliance requirements for malware protection.

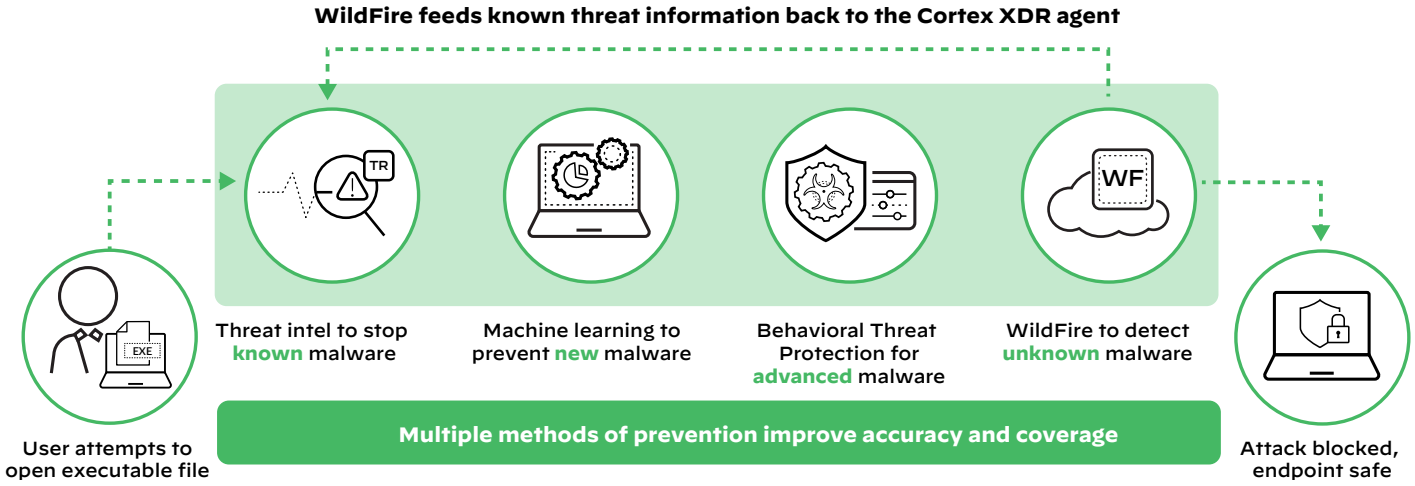

Figure 1: Multiple security engines to block advanced, never-before-seen malware

Securely Manage USB Devices

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

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® endpoints. Additionally, you can apply BitLocker® encryption or decryption on your endpoints by creating disk encryption rules and policies. Host firewall and disk encryption capabilities let you centrally configure your endpoint security policies from the Cortex XDR management console.

Table 1: Cortex XDR Tiers—Feature Comparison

Feature	Traps 4.2 Agent	Cortex XDR Prevent
Prevention		
Malware, exploit, and fileless attack prevention	√	√
Cloud-based malware analysis with WildFire	√	√
Behavioral Threat Protection	—	√
Device control to manage USB access	—	√
Host firewall	—	√
Disk encryption	—	√
Public APIs for data collection and response	—	√

Table 1: Cortex XDR Tiers—Feature Comparison (continued)		
Feature	**Traps 4.2 Agent**	**Cortex XDR Prevent**
Detection and Investigation		
Security alerts	√	√
Incident management to group related alerts together	—	√
Comprehensive endpoint data collection, including process, registry, file, and network activity	—	Requires Cortex XDR Pro
Root cause analysis of network and endpoint alerts	—	Requires Cortex XDR Pro
Threat hunting with IOC- and behavior-based queries	—	Requires Cortex XDR Pro
Response		
File quarantine	√	√
Blocking of future file executions	√	√
Endpoint-based isolation	—	√
Live Terminal to terminate processes and more	—	√
Endpoint script execution	—	Requires Cortex XDR Pro
Management		
Cloud native deployment and management	—	√
Optional automated agent upgrade	—	√
Scheduled and on-demand endpoint malware scanning	—	√

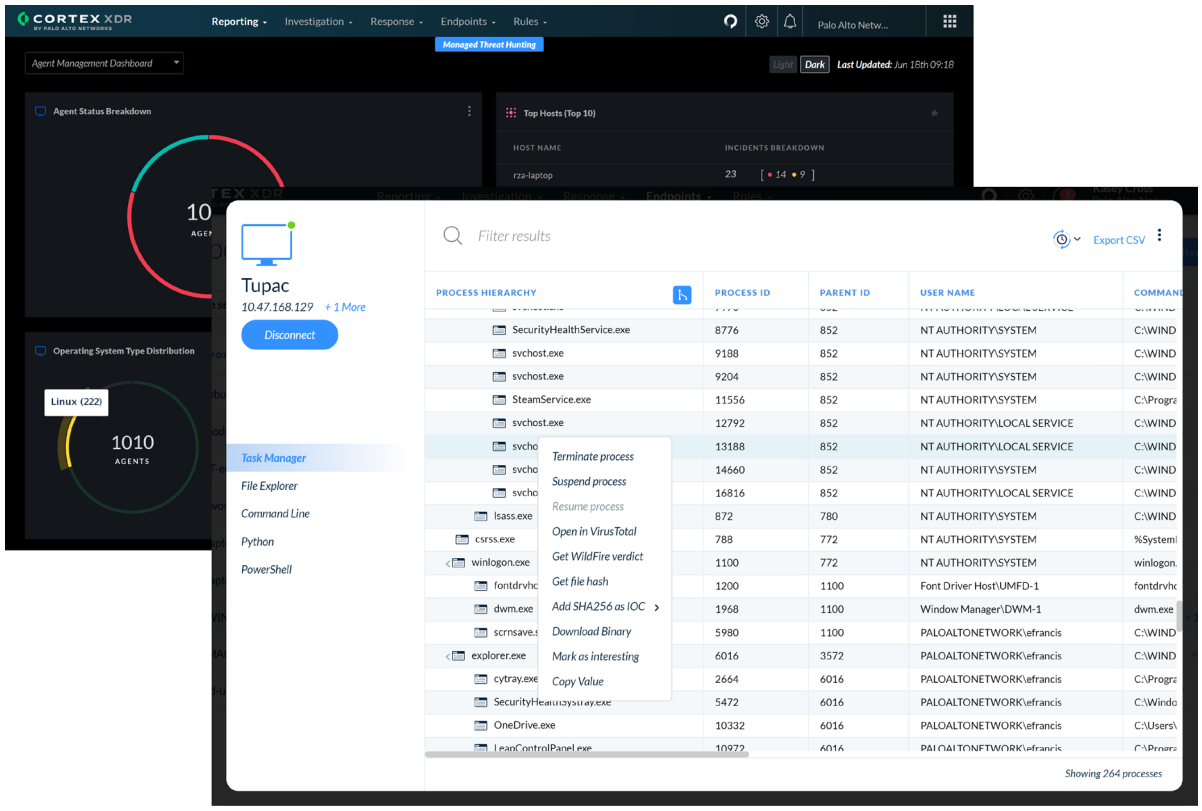

Figure 2: Agent status dashboard; Live Terminal for direct access to endpoints for investigation and response

Extend Your Investment to Detection and Response

With a Cortex XDR Pro subscription, you can transform your Cortex XDR agents into sensors and enforcement points for detection and response. Cortex XDR Pro offers the world's first extended detection and response platform that integrates network, endpoint, and cloud data to stop sophisticated attacks.

Cortex XDR stitches together different types of data to reveal the root cause and timeline of attacks, allowing analysts of all experience levels to investigate incidents. Tight integration with enforcement points—including your Cortex XDR agents—lets you contain threats quickly. Additional features, such as vulnerability assessment, script execution, and powerful searching capabilities, empower you to prioritize risks as well as hunt down and eliminate attacks anywhere in your enterprise.

Take Advantage of Secure, Cloud Native Endpoint Protection

As a cloud-delivered service, deployment of your Cortex XDR agents is a snap. You can avoid cumbersome on-premises management and stay ahead of attackers by leveraging the power of cloud analytics.

Security is our top priority at Palo Alto Networks. We apply industry-standard best practices for security and confidentiality, including application, system, network, and physical security, to safeguard the Cortex XDR service. Log data sent from Cortex XDR agents to the Cortex XDR management console is encrypted in transmission and at rest. Furthermore, Cortex XDR has achieved SOC 2 Type II Plus compliance and reached the "In Process" milestone for FedRAMP certification. Learn more about our security in the Cortex XDR Privacy datasheet.

On-Premises Broker for Restricted Networks

The on-premises Broker Service extends Cortex XDR agents to devices that cannot directly connect to the internet. Agents can use the Broker Service as a communication proxy to the Cortex XDR management service, receive the latest security console, and send content to Cortex™ Data Lake and WildFire without having to directly access the internet.

Easily Upgrade from Traps to Cortex XDR Prevent

To simplify your migration from Traps Endpoint Security Manager (ESM) to Cortex XDR, our detailed instructions will walk you through each step of the upgrade process. If you prefer hands-on assistance, consider a Professional Services engagement to help you deploy new agents as well as migrate your security policies, allow lists, exclusions, and more. Our experts will also provide upgrade documentation and verify successful deployment.

Cortex XDR is your secret weapon for eradicating elusive threats anywhere in your organization by applying multiple layers of defense. If you already have Traps advanced endpoint protection, you should upgrade to Cortex XDR to bolster your endpoint security even further.

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