Cortex XDR Endpoint Protection Solution Guide

Safeguard Your Endpoints from Never-Before-Seen Attacks with a Single, Cloud-Delivered Agent for Endpoint Protection, Detection, and Response

The Cortex XDR agent combines industry-best behavioral protection and AI-based analysis to block malware, exploits, and fileless attacks.

Benefits

- Stop malware with AI-based local analysis and Behavioral Threat Protection.
- Block the exploits that lead to breaches.
- Prevent unauthorized access and data loss with disk encryption, device control, and host firewall.
- Simplify operations with cloud-native deployment and management.
- Get industry-leading security with the solution that delivered 100% protection and 100% detection across all 19 steps in the 2022 MITRE ATT&CK evaluations.

Advanced malware and script-based attacks can bypass traditional antivirus with ease and potentially wreak havoc on your business. To protect your endpoints, you need a solution that provides superior prevention and uses AI to continuously adapt to rapidly changing threats and outpace adversaries.

The Cortex XDR agent provides everything you need to secure your endpoints. By analyzing files before and after they execute them, it identifies the telltale signs of attacks, including zero-day malware, fileless attacks, and script-based attacks. You can quickly deploy the unified, cloud-delivered agent to your endpoints to instantly start blocking advanced attacks and collecting data for detection and response.

Eliminate Zero-Day Malware, Ransomware, and Fileless Attacks

The Cortex XDR agent provides a complete endpoint threat prevention stack, thwarting every possible attack vector with a single agent by unifying multiple complementary engines:

- **AI-based local analysis** blocks malware before it can execute, using a local machine learning model powered by a comprehensive data set from global sources. The model is built on a unique agile framework, enabling continuous updates to ensure the latest local prevention is always available.
- **Integration with cloud-based WildFire** malware prevention service brings deep inspection of unknown files, with intelligence automatically shared across your Palo Alto Networks endpoint agents, Next-Generation Firewalls, and cloud infrastructure.
- **Behavioral Threat Protection** blocks the stealthiest threats by recognizing the sequence of events associated with malware and fileless attacks. This engine examines the behavior of multiple related processes to uncover attacks, even if individual actions do not definitively signal malicious activity.
- **Behavior-based ransomware protection** safeguards your endpoints against ransomware by detecting processes attempting to modify or encrypt files, providing another layer of defense against covert ransomware.
- **Credential gathering protection** prevents tools like Mimikatz from accessing system passwords, ensuring that adversaries and malicious insiders cannot misuse credentials or escalate privileges.

You can uncover dormant malware and address compliance requirements with scheduled and on-demand malware scanning. Malware scanning discovers malicious executable files, DLLs, and Office macros, to mitigate risks even if the files have not been opened or executed.

Block Exploits by Technique to Shut Down Attacks Early

Adversaries often exploit system and application vulnerabilities to gain control of endpoints and install malware. To stay ahead of continually evolving exploits, the Cortex XDR agent identifies exploit techniques and methods rather than simply detecting exploits with signatures. By foiling each step of an exploit, it breaks the attack lifecycle and renders threats ineffective.

The Cortex XDR agents prevent exploits through multiple methods:

- **Preexploit protection** blocks reconnaissance and vulnerability-profiling techniques before adversaries launch exploits, effectively preventing attacks.
- **Technique-based exploit prevention** prevents known and zero-day exploits, without any prior knowledge of the threats, by blocking exploit techniques such as buffer overflow or DLL hijacking.
- **Kernel exploit prevention** blocks exploits that take advantage of vulnerabilities in the operating system kernel to create processes with escalated, system-level privileges. The Cortex XDR agent also thwarts injection techniques used to load and run malicious code from the kernel.
- **Java deserialization exploit protection** blocks exploits like Log4Shell and SpringShell by detecting attacks such as the modification of server attributes from a malicious source.

Maximize Accuracy of Behavioral Threat Protection with Silent Rules

Behavioral Threat Protection provides accurate and timely protection by tightly coupling threat research, visibility into active threats in customer's networks, and telemetry on silent rules to ensure effective security—all with rapid global updates to all agents. Every new rule starts in silent mode, allowing Cortex XDR researchers to quickly roll out new rules with an exceptionally low rate of false positives.

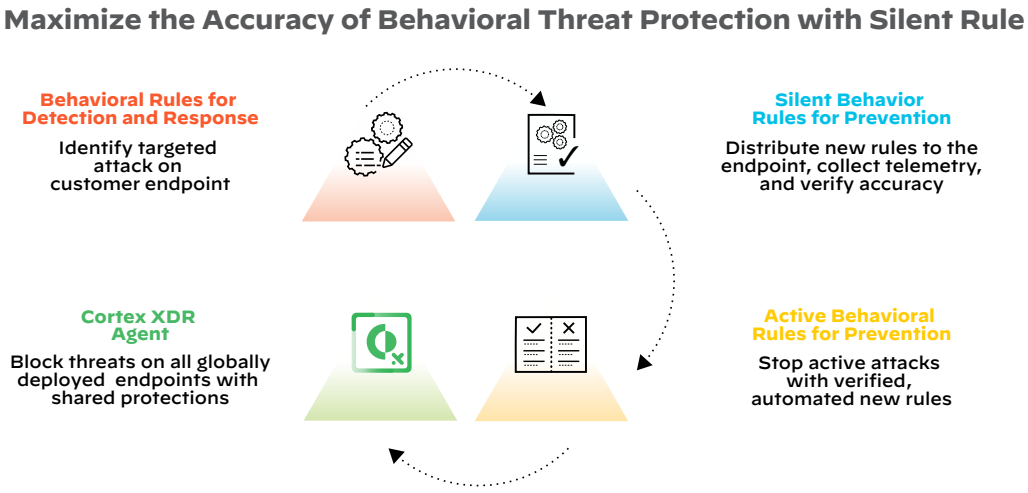

Figure 1: How silent Behavioral Threat Protection rules evolve into active rules

Quickly Discover and Investigate Threats with Cortex XDR

The Cortex XDR agent proactively blocks attacks and collects rich endpoint data for Cortex XDR, the industry's first extended detection and response platform that spans all data sources to stop modern attacks. A unified user interface facilitates management of alerts and incidents for detection and response as well as policies for the Cortex XDR agent.

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 and apply the knowledge gained from investigations to detect similar attacks in the future.

Instantly Respond to Attacks

The Cortex XDR agent provides an array of response options to quickly contain threats while allowing analysts to further their investigations and collect additional endpoint information.

To resolve threats, analysts and administrators can:

- **Isolate endpoints** by disabling all network access on compromised endpoints except for traffic to the Cortex XDR management console, preventing these endpoints from communicating with and potentially infecting other endpoints.
- **Terminate processes** to stop any running malware from continuing to perform malicious activity on the endpoint.
- **Block additional executions** of a given file by block listing it in the policy.
- **Quarantine malicious files** and remove them from their working directories if the Cortex XDR agent has not already quarantined the files.
- **Retrieve specific files** from endpoints under investigation for further analysis.

- **Directly access endpoints with Live Terminal**, gaining the most flexible response actions in the industry to run Python, PowerShell, or system commands or scripts; review and manage active processes; and view, delete, move, or download files.
- **Orchestrate response with open APIs** that allow third-party tools to apply enforcement policies and collect agent information from any location.
- **Automate response through Cortex XSOAR integration**. Your team can share incident data with Cortex XSOAR for automated, playbook-driven response across hundreds of third-party tools. Cortex XSOAR playbooks can automatically ingest Cortex XDR incidents, retrieve related alerts, and update incident fields in Cortex XDR as playbook tasks.
- **Execute any Python-based script** from the Cortex XDR management console or orchestration tools such as Cortex XSOAR. Out-of-the-box scripts make it easy for your team to take advantage of this powerful feature.
- **Swiftly find and delete files** across your organization with Search and Destroy, which indexes endpoint files.
- **Restore hosts to a clean state** based on remediation suggestions. You can rapidly recover from an attack by removing malicious files and registry keys, as well as restoring damaged files and registry keys—without re-imaging or building custom scripts.

Apply Consistent, Coordinated Policies Across Endpoint, Network, and Cloud Security

The Cortex XDR agent tightly integrates with WildFire, Next-Generation Firewalls, and Prisma Access to consistently protect your entire enterprise environment. This integration enables continual improvement of your security posture, including coordinated prevention of zero-day attacks. Whenever Palo Alto Networks products observe unknown malware, the offending files are sent to WildFire for analysis. If suspected malware is deemed malicious, new protection is automatically distributed in minutes to all Next-Generation Firewalls, endpoint agents, and users protected by Prisma Access.

Securely Manage USB Devices

USB devices offer a variety of functions, but they also introduce risk. When users unwittingly connect malware-laden flash drives to their computers or copy confidential data to backup disk drives, they expose their organizations to attack and data loss. Advanced attackers can even infect seemingly innocuous USB devices such as keyboards and web cameras with malware. The powerful device control module included with Cortex XDR allows you to monitor and secure USB access without needing to install another endpoint agent on all your hosts. You can assign policies based on the Active Directory group and the organizational unit, restrict usage by device type, and assign read-only or read/write policy exceptions by vendor, product, and serial number. The device control module allows you to easily manage USB access and gain peace of mind that you've mitigated USB-based threats.

Protect Endpoint Data with Host Firewall and Disk Encryption

With integrated host firewall and disk encryption capabilities, you can lower your security risks and 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. Cortex XDR provides full visibility into Windows endpoints that were encrypted using BitLocker and lists all the encrypted drives. With host firewall and disk encryption, you can centrally manage your endpoint security policies from Cortex XDR.

Deploy Effortlessly from the Cloud

Operations teams can quickly install agents across all their endpoints from the cloud-native management service. The Cortex XDR agent speeds up time-to-protection and simplifies operations by eliminating the need for on-premises logging and management servers. End users will experience better performance and less disruption than burdensome and bloated legacy antivirus.

On-Premises Broker for Restricted Networks

The on-premises Broker Service extends Cortex XDR agents to devices that cannot directly connect to the internet. Now, 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 the cloud-based Cortex XDR service and WildFire without directly accessing the internet.

Protect All Your Endpoints with Comprehensive Operating System Support

The Cortex XDR agent protects endpoints running all major operating systems—Windows, macOS, Linux, and Android—by stopping known and unknown attacks before they compromise systems. In contrast, native OS security features only protect their respective endpoints, which creates fragmented protection, leaves endpoints vulnerable to attacks, and slows down incident response. For a complete list of supported operating systems, please see the Palo Alto Networks Compatibility Matrix.

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