Endpoint protection (Cortex XDR)

Adversary strategies have evolved from simple malware distribution to a broad set of automated, targeted, and sophisticated attacks that can bypass traditional endpoint protection. This evolution has forced organizations to deploy multiple products from different vendors to protect against, detect, and respond to these threats. Cortex XDR brings powerful endpoint protection together with endpoint detection and response (EDR) in a single agent. You can replace all your traditional antivirus agents with one lightweight agent that shields your endpoints from the most advanced adversaries by understanding and blocking all elements of attacks.

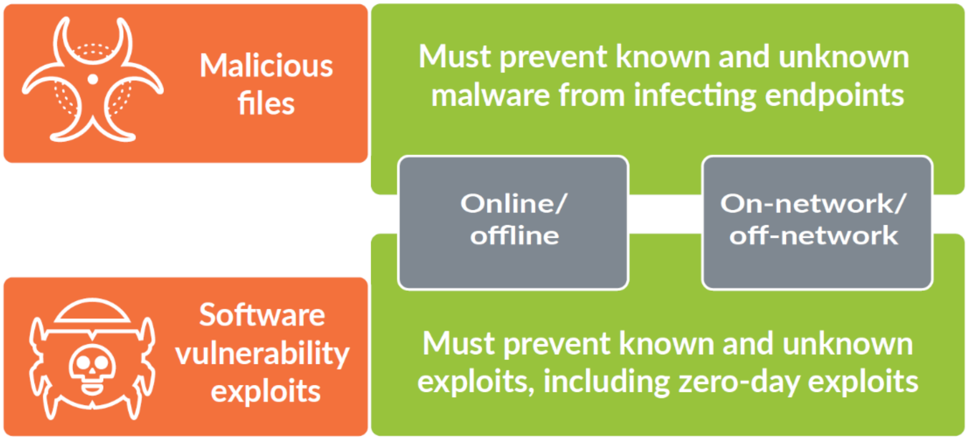
Although attacks have become more sophisticated and complex, they still use basic building blocks to compromise endpoints. The primary attack methods continue to exploit known and unknown application vulnerabilities as well as deploy malicious files, including ransomware. These attack methods can be used individually or in various combinations, but they are fundamentally different in nature:

- Exploits are the results of techniques used against a system that are designed to gain access through vulnerabilities in the code of an operating system or application.
- Malware is a file or code that infects, explores, steals, or conducts virtually any behavior an attacker wants.
- Ransomware is a form of malware that holds valuable files, data, or information for ransom, often by encrypting data, with the attacker holding the decryption key.

Due to the fundamental differences between malware and exploits, effective prevention must protect against both. The Cortex XDR agent combines multiple methods of prevention at critical phases within the attack lifecycle to halt the execution of malicious programs and stop the exploitation of legitimate applications, regardless of operating system, the endpoint’s online or offline status, and whether the endpoint is connected to an organization’s network or roaming.

Palo Alto Networks Cybersecurity Academy

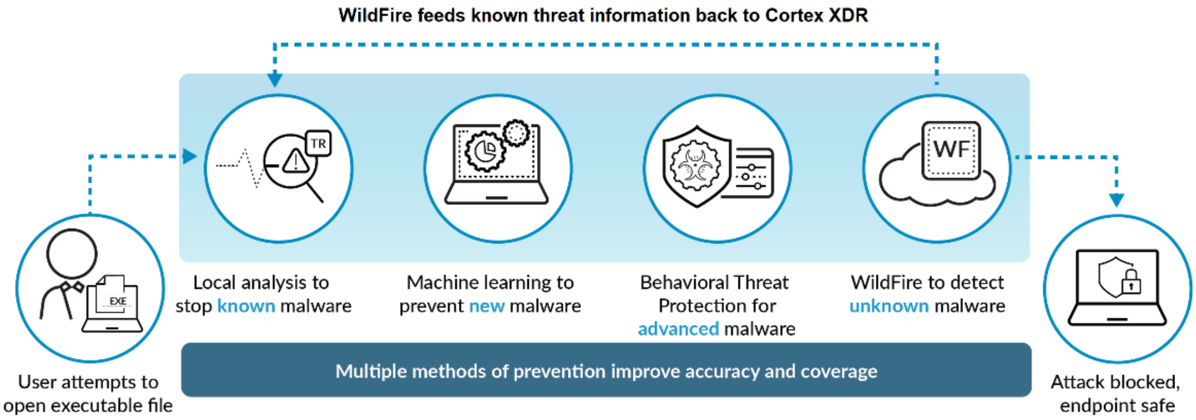
Malicious files vs. exploits


Malicious files
Must prevent known and unknown malware from infecting endpoints
Online/ offline
On-network/ off-network
Software vulnerability exploits
Must prevent known and unknown exploits, including zero-day exploits

Stop malware and ransomware

The Cortex XDR agent prevents the execution of malicious files with an approach tailored to combating both traditional and modern attacks. Additionally, administrators can use periodic scanning to identify dormant threats, comply with regulatory requirements, and accelerate incident response with endpoint context. The Cortex XDR agent also performs scheduled or on-demand scans for dormant malware in malicious Office files with macros, executable files, and DLLs, to remediate these without the malicious files being opened. Known and unknown malware, including ransomware, is subject to multiple preventive technologies.

Cortex XDR leverages multiple technologies and techniques to protect endpoints from known and unknown malware.


WildFire feeds known threat information back to Cortex XDR
TR
EXE
WF
Local analysis to stop known malware
Machine learning to prevent new malware
Behavioral Threat Protection for advanced malware
WildFire to detect unknown malware
User attempts to open executable file
Multiple methods of prevention improve accuracy and coverage
Attack blocked, endpoint safe

WildFire threat intelligence

In addition to third-party feeds, Cortex XDR uses the intelligence obtained from tens of thousands of subscribers to the Palo Alto Networks WildFire malware prevention service to continuously aggregate threat data and maintain the collective immunity of all users across endpoints, networks, and cloud applications:

1. Before a file runs, the Cortex XDR agent queries WildFire with the hash of any Windows, macOS, or Linux executable file, as well as any dynamic link library (DLL) or Office macro, to assess its standing within the global threat community. WildFire returns a near-instantaneous verdict on whether a file is malicious or benign.

2. If a file is unknown, the Cortex XDR agent proceeds with additional prevention techniques to determine whether it is a threat that should be blocked.

3. If a file is deemed malicious, the Cortex XDR agent automatically terminates the process and (optionally) quarantines the file.

Local analysis and machine learning

If a file remains unknown after the initial hash lookup, the Cortex XDR agent uses local analysis via machine learning on the endpoint – trained by the rich threat intelligence from global sources, including WildFire – to determine whether the file can run. By examining thousands of file characteristics in real time, local analysis can determine whether a file is likely malicious or benign without relying on signatures, scanning, or behavioral analysis. The model is built on a unique agile framework, enabling continuous updates to ensure that the latest local prevention is always available.

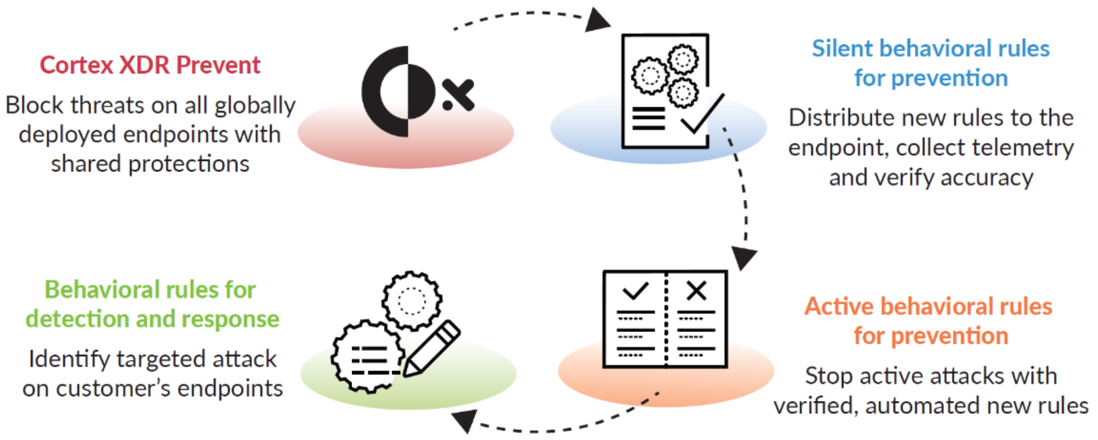
Behavioral threat protection

Sophisticated attacks that use multiple legitimate applications and processes for malicious operations have become more common, are hard to detect, and require deeper visibility to correlate malicious behavior. For behavior-based protection to be effective, including identification of malicious activity occurring within legitimate processes, it's critical to understand everything happening on the endpoint. The Cortex XDR agent enacts behavior-based protection in a few different ways.

Endpoint attacks often comprise multiple events that occur in the system. By itself, each event appears benign as attackers use legitimate applications and operating system functions to achieve their goal. Strung together, however, they may represent a malicious event flow. With behavioral threat protection, the Cortex XDR agent can detect and act on malicious chains of events that target multiple operations on an endpoint, such as network, process, file, and registry activity. When the Cortex XDR agent detects a match, it executes a policy-based action, such as "block" or "alert." In addition, it reports the behavior of the entire event chain up to the console and identifies the actor that caused the activity chain. The Cortex XDR agent can also quarantine files that were involved in malicious flows. Behavioral threat protection is ideal for protecting against script-based and file-less attacks.

Palo Alto Networks Cybersecurity Academy

Behavioral threat protection with Cortex XDR


Cortex XDR Prevent
Block threats on all globally deployed endpoints with shared protections
Silent behavioral rules for prevention
Distribute new rules to the endpoint, collect telemetry and verify accuracy
Active behavioral rules for prevention
Stop active attacks with verified, automated new rules
Behavioral rules for detection and response
Identify targeted attack on customer's endpoints

The granular *child process* protection module prevents script-based attacks used to deliver malware by blocking known targeted processes from launching child processes that are commonly used to bypass traditional security approaches. The Cortex XDR agent prevents script-based and file-less attacks by default with out-of-the-box, fine-grained controls over the launching of legitimate applications, such as script engines and command shells, and continues to expand these controls through regular content updates. Administrators have additional flexibility and control with the ability to whitelist or blacklist child processes, along with command-line comparisons, to increase detection without negatively affecting process performance or shutting processes down.

The behavior-based ransomware protection module protects against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before any data loss occurs. To combat these attacks, Cortex XDR employs decoy files to attract the ransomware. When the ransomware attempts to write to, rename, move, delete, or encrypt the decoy files, the Cortex XDR agent analyzes the behavior and prevents the ransomware from encrypting and holding files hostage. When configured to operate in prevention mode, the Cortex XDR agent blocks the process attempting to manipulate the decoy files. When you configure this module in notification mode, the agent logs a security event.

Key Terms

In multitasking operating systems, a *child process* is a subprocess created by a parent process that is currently running on the system.

Palo Alto Networks Cybersecurity Academy

WildFire inspection and analysis

In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware. WildFire brings together the benefits of independent detection techniques for high-fidelity and evasion-resistant discovery that goes beyond legacy approaches. Among these techniques:

- Static analysis is a powerful form of analysis, based in the cloud, that detects known threats by analyzing the characteristics of samples before execution.
- Dynamic analysis (sandboxing) detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior.
- Bare-metal analysis uses a hardware-based analysis environment specifically designed for advanced threats that exhibit highly evasive characteristics and can detect virtual analysis.

If WildFire determines a file to be a threat, it automatically creates and shares a new prevention control with the Cortex XDR agent and other Palo Alto Networks products in minutes to ensure that the threat is immediately classified as malicious and blocked if it is encountered again.

Block exploits and file-less threats

Rather than relying on signatures or behavior-based detection to identify exploit-based attacks, the Cortex XDR agent takes the unique approach of targeting the limited set of techniques, or tools, any exploit-based attack must use to manipulate a software vulnerability. By preventing the use of these techniques – instead of identifying each individual attack – the Cortex XDR agent uses multiple methods to prevent zero-day exploits as well as protect unpatched systems, shadow IT (or applications IT is unaware of), and unsupported legacy systems.

Pre-exploit protection

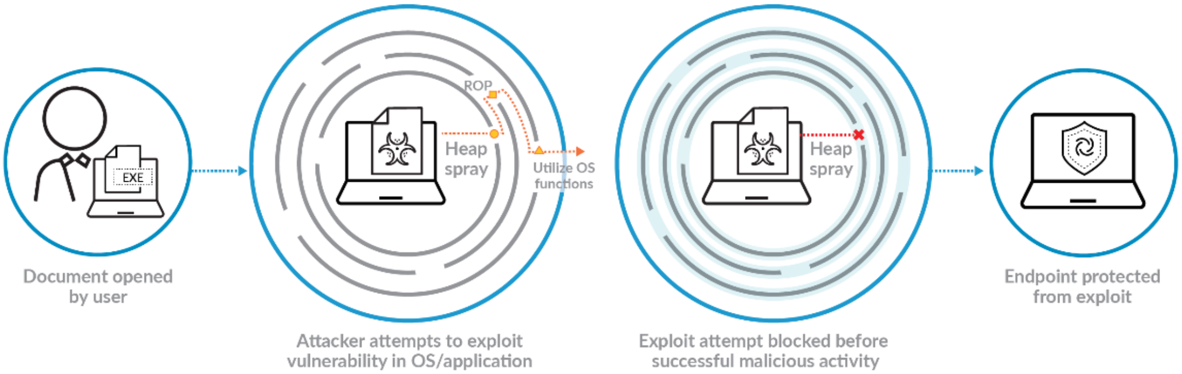
The Cortex XDR agent prevents the vulnerability-profiling techniques exploit kits use before launching attacks. By blocking these techniques, the agent prevents attackers from targeting vulnerable endpoints and applications, effectively stopping the attacks before they begin.

Technique-based exploit prevention

The Cortex XDR agent prevents known, zero-day, and unpatched vulnerabilities by blocking the exploitation techniques attackers use to manipulate applications. Although there are thousands of exploits, they typically rely on a small set of exploitation techniques that change infrequently. By blocking these, Cortex XDR prevents exploitation attempts before endpoints can be compromised.

Palo Alto Networks Cybersecurity Academy

Cortex XDR focuses on exploit techniques rather than on the exploits themselves.


EXE
Document opened by user
ROP
Heap spray
Utilize OS functions
Attacker attempts to exploit vulnerability in OS/application
Heap spray
Exploit attempt blocked before successful malicious activity
Endpoint protected from exploit

Kernel exploit prevention

The Cortex XDR agent prevents exploits that use vulnerabilities in the operating system kernel to create processes with escalated, system-level privileges. It also protects against new exploit techniques used to execute malicious payloads, such as those seen in the 2017 WannaCry and NotPetya attacks. By blocking processes from accessing the injected malicious code from the kernel, the Cortex XDR agent can stop an attack early in the attack lifecycle without affecting legitimate processes. This capability enables the agent to block advanced attacks that target or stem from the operating system itself.

By blocking the techniques common to exploit-based attacks, the Cortex XDR agent allows customers to:

- **Protect applications that can’t be patched and shadow IT applications.** The Cortex XDR agent enables organizations to run any applications – including those developed in house, no longer receiving updates or security support, or running in the environment without IT’s awareness – without opening the network to the threat of exploit-based attacks.

- **Prevent successful zero-day exploits.** Because the Cortex XDR agent blocks the limited set of exploitation techniques that zero-day exploits typically use, it protects organizations against attacks that utilize zero-day exploits.

- **Eliminate the need to urgently patch applications.** Organizations using the Cortex XDR agent can apply security patches when it is best for the business and after sufficient testing. It prevents the exploitation of application vulnerabilities regardless of when an organization applies security patches issued by application vendors.

Credential theft protection

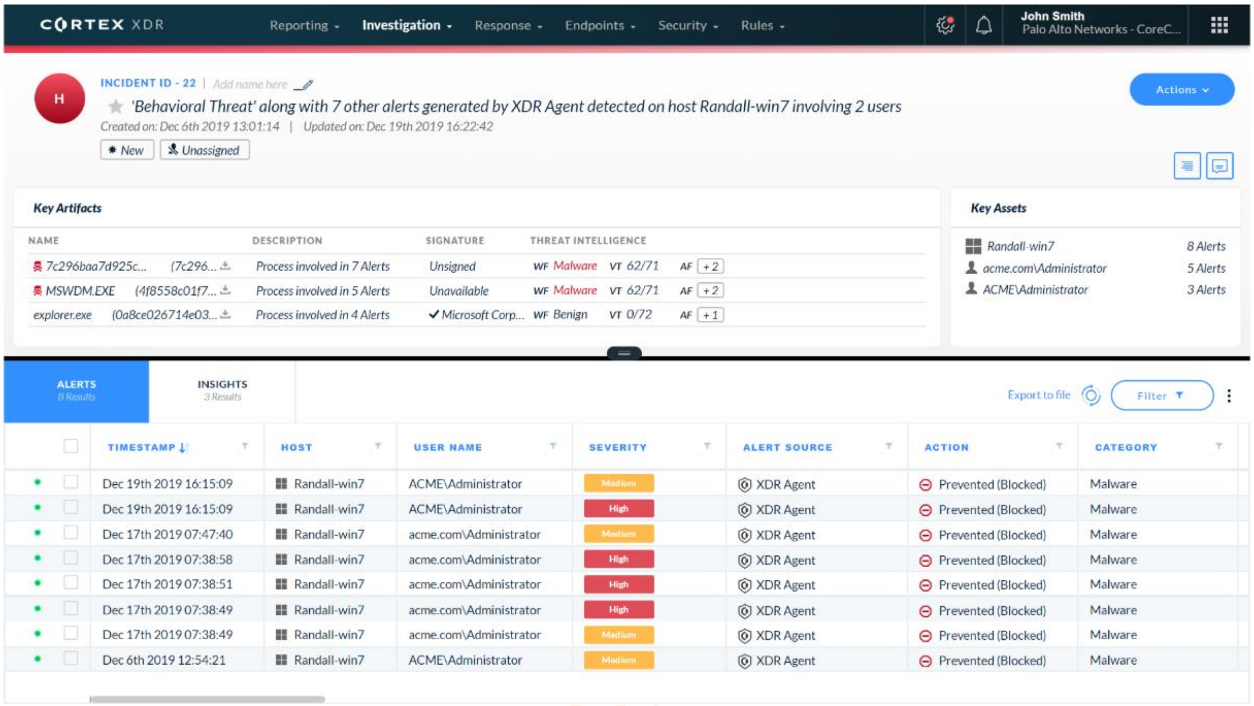
Attackers steal credentials to impersonate valid users, move uninterrupted through targeted organizations’ networks, and find and exfiltrate valuable data. The Cortex XDR agent prevents credential theft tools like Mimikatz from accessing system passwords, ensuring that adversaries and malicious insiders cannot misuse credentials or escalate privileges. For additional credential theft protection, Cortex XDR can collect endpoint events, profile behavior, and detect credential-based attacks to eliminate hard-to-find attacks.

Palo Alto Networks Cybersecurity Acad

Investigate and respond to attacks

To facilitate faster investigation and response, Cortex XDR offers administrators and incident response teams multiple means to further their investigations, collect necessary information, and make any necessary changes to the endpoint in question.

Investigate and respond to attacks.



INCIDENT ID - 22 | Add name here

'Behavioral Threat' along with 7 other alerts generated by XDR Agent detected on host Randall-win7 involving 2 users

Created on: Dec 6th 2019 13:01:14 | Updated on: Dec 19th 2019 16:22:42

Key Artifacts

NAME		DESCRIPTION	SIGNATURE	THREAT INTELLIGENCE		
7c296baa7d925c...	(7c296...	Process involved in 7 Alerts	Unsigned	WF Malware	VT 62/71	AF +2
MSWDM.EXE	(4f8558c01f7...	Process involved in 5 Alerts	Unavailable	WF Malware	VT 62/71	AF +2
explorer.exe	(0a8ce026714e03...	Process involved in 4 Alerts	✓ Microsoft Corp...	WF Benign	VT 0/72	AF +1

Key Assets

Randall-win7	8 Alerts
acme.com\Administrator	5 Alerts
ACME\Administrator	3 Alerts

	TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY
● □	Dec 19th 2019 16:15:09	Randall-win7	ACME\Administrator	Medium	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 19th 2019 16:15:09	Randall-win7	ACME\Administrator	High	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 17th 2019 07:47:40	Randall-win7	acme.com\Administrator	Medium	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 17th 2019 07:38:58	Randall-win7	acme.com\Administrator	High	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 17th 2019 07:38:51	Randall-win7	acme.com\Administrator	High	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 17th 2019 07:38:49	Randall-win7	acme.com\Administrator	High	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 17th 2019 07:38:49	Randall-win7	acme.com\Administrator	Medium	XDR Agent	Prevented (Blocked)	Malware
● □	Dec 6th 2019 12:54:21	Randall-win7	ACME\Administrator	Medium	XDR Agent	Prevented (Blocked)	Malware

When remediation on the endpoint is needed following an alert or investigation, administrators have the option to take the following actions:

- **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 blacklisting 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.

Palo Alto Networks C

Extending prevention beyond Windows environments

Although native security has grown among major operating system vendors, such security remains focused on its own OS, creating fragmented protection, policies, enforcement, and visibility. Organizations need to be able to apply security rules across a mixed environment from a single screen as well as protect against a range of threats, from basic to advanced.

Through the Cortex XDR console, organizations can control default and custom security policies across Windows, macOS, Linux, and Android endpoints with confidence that multiple methods of protection are keeping their systems safe from attack.

Cortex XDR for macOS

Cortex XDR secures macOS systems against malware and exploits with more than just “check box” security. The Cortex XDR agent uses multiple methods – such as local analysis, WildFire inspection and analysis, Gatekeeper enhancements, trusted publisher identification, and administrator override policies – to block malware. To prevent exploits, the agent blocks kernel privilege escalation and exploitation techniques, including *JIT* and *ROP* as well as *dylib hijacking*.

The Cortex XDR agent prevents attackers from bypassing the macOS digital signature verification mechanism, Gatekeeper. This mechanism allows or blocks the execution of applications based on their digital signatures, which are ranked in three signature levels: Apple System, Mac App Store, and Developers. It extends Gatekeeper functionality to enable customers to specify whether to block all child processes or to allow only those with signature levels that match or exceed those of their parent processes.

Cortex XDR for Android

The Cortex XDR agent prevents known malware and unknown *Android Package Kit* (APK) files from running on Android endpoints. It enforces your organization’s security policy as defined in the Cortex XDR console. The security policy determines whether to block known malware and unknown files, upload unknown files for in-depth inspection and analysis, treat malware as grayware, or perform local analysis to determine the likelihood that unknown files are malware. You can also whitelist trusted signers to enable unknown, signed apps to run before the Cortex XDR agent receives an official verdict for the app.

Key Terms

An *Android Package Kit* (APK) file is an app created for the Android mobile operating system.

Cortex XDR for Linux

The Cortex XDR agent protects Linux servers by preventing attackers from executing malicious ELF files or exploiting known or unknown Linux vulnerabilities to compromise endpoints. The agent also extends protection to processes that run in Linux containers. The Cortex XDR agent enforces your organization’s security policy as defined in the Cortex XDR console. When a security event occurs on your Linux server, it collects forensic information that you can use to analyze the incident further. The Cortex XDR agent on Linux operates transparently in the background as a system process.

Palo Alto Networks Cybersecurity Academy

When you install it on a Linux server, it automatically protects any new or existing containerized processes regardless of how the container is deployed and managed.

Device control for secure USB access

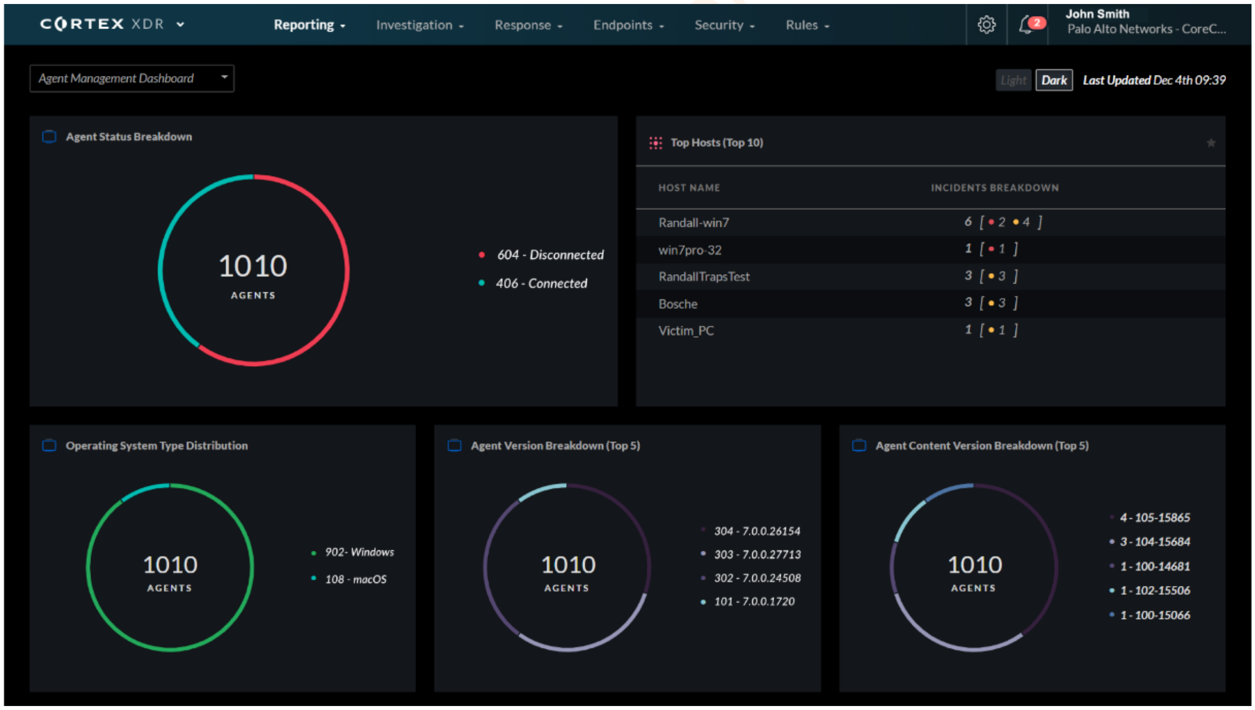
USB devices offer a variety of benefits, but they also introduce risk. When users unwittingly connect malware-laden flash drives to their computers or copy confidential data to backup disk drives, they expose their organizations to attack and data loss. Advanced attackers can even infect seemingly innocuous USB devices such as keyboards and webcams 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 Active Directory group and 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.

Cybersecurity Academy

Simple endpoint security management

With an intuitive, web-based user interface, Cortex XDR helps administrators quickly coordinate and protect your organization with out-of-the-box, day-one capabilities, without sacrificing your complex environment's need for control and customization.

The Cortex XDR dashboard



HOST NAME	INCIDENTS BREAKDOWN
Randall-win7	6 [• 2 • 4]
win7pro-32	1 [• 1]
RandallTrapsTest	3 [• 3]
Bosche	3 [• 3]
Victim_PC	1 [• 1]

Cloud-based management

The multiregion, cloud-based Cortex XDR service saves you from investing in building out your own global security infrastructure and ties in to the suite of Palo Alto Networks products for additional integration and value. The service is simple to deploy and requires no server licenses, databases, or other infrastructure to get started, enabling your organization to protect hundreds or millions of endpoints without incurring additional operating costs.

Intuitive interface

Cortex XDR was designed to address security teams' growing responsibilities with an interface that makes it easy to manage policies and events as well as accelerate incident response. By combining endpoint policy management, detection, investigation, and response in one web-based management console, Cortex XDR provides a seamless platform experience. You can quickly assess security status with customizable dashboards and summarize incidents and security trends with graphical reports that can be scheduled or generated on demand. You can also deploy and upgrade Cortex XDR agents easily from a central location.

Elements include:

- **Multiple grouping methods**, including static groups or dynamic groups. Dynamic grouping can be based on endpoint characteristics such as a partial hostname or alias, full or partial domain or workgroup name, IP address, range or subnet, installation type such as VDI, agent version, endpoint type, or operating system version.

- **Security profiles and simplified, rule-based policies** to protect endpoints out of the box while enabling granular customization for sensitive departments or individuals and easy reuse of settings across different endpoint groups.

- **Incident management** to help identify high-priority events and enable teams to communicate on status, progress, and other useful information. Integrated WildFire analysis displays information such as hash values, targeted users, applications, processes, and URLs involved in delivery or phone-home activities for incident response.

Benefits of a connected platform

By tightly integrating with the Palo Alto Networks suite of products, the Cortex XDR agent continuously exchanges threat information and data with WildFire – and endpoint incident and event logs with Cortex Data Lake, a cloud-based data collection, storage, and analysis service – to help your organization coordinate and automate enforcement across your entire security ecosystem, including endpoints, networks, and clouds.

Native integration for fast investigation and response

The data collected from the Cortex XDR agent is stored in Cortex Data Lake, which delivers efficient log storage that scales to handle the large volume of data needed for analytics, detection, and response. You can quickly deploy Cortex XDR and Cortex Data Lake, avoiding the time-consuming process of setting up new equipment.

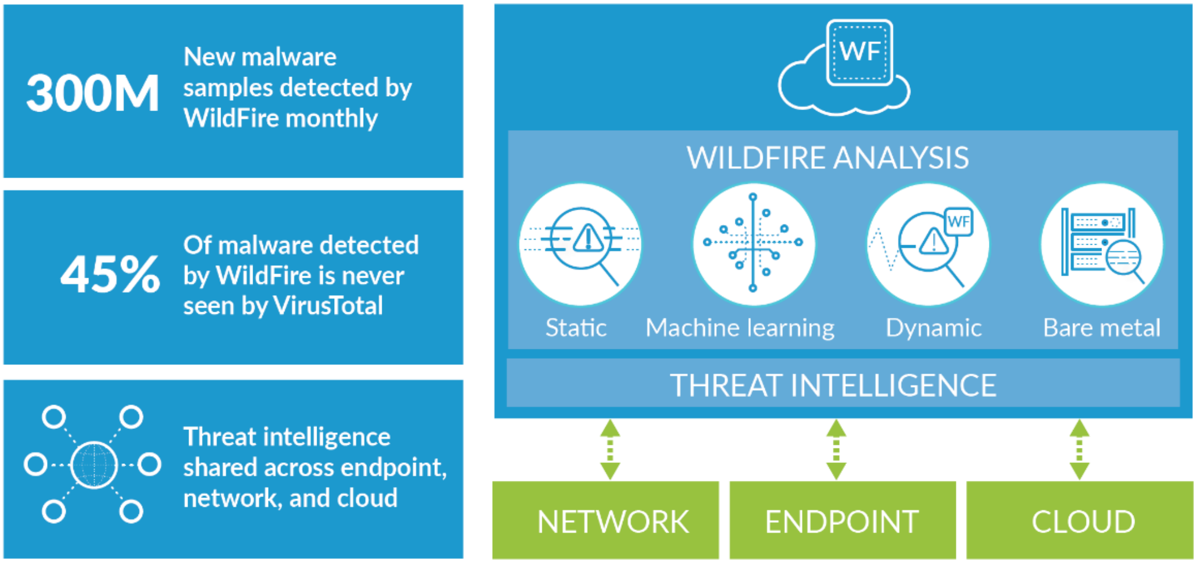
By eliminating on-premises log storage and additional sensors and enforcement points, Cortex XDR can reduce total cost of ownership by 44 percent on average. Cortex XDR also boosts the productivity of your security operations team by automatically detecting attacks and accelerating investigations.

Cortex XDR is the world's first detection and response app that breaks silos by natively integrating endpoint, cloud, and network apps to stop sophisticated attacks. Cortex supports data from Palo Alto Networks next-generation firewalls, Prisma Access, and Cortex XDR agents, in addition to third-party

Palo Alto Networks Cybersecurity Academy

alerts and logs. It speeds alert triage and incident response by providing a complete picture of an attack, including root cause, and stitching together the sequence of events to simplify investigations. Intelligent alert grouping and deduplication reduce the number of individual alerts to review by 98 percent, alleviating alert fatigue.

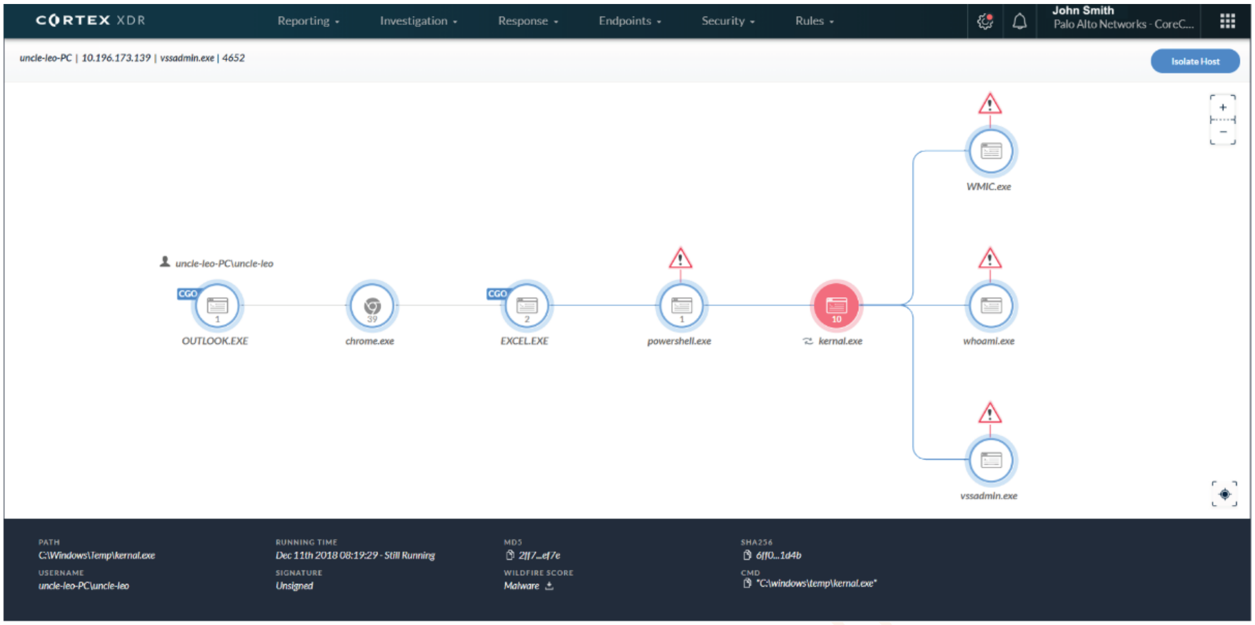
Native integration with network, endpoint, and cloud apps as well as WildFire threat intelligence


300M
New malware samples detected by WildFire monthly
45%
Of malware detected by WildFire is never seen by VirusTotal
Threat intelligence shared across endpoint, network, and cloud
WF
WILDFIRE ANALYSIS
Static
Machine learning
WF
Dynamic
Bare metal
THREAT INTELLIGENCE
NETWORK
ENDPOINT
CLOUD

Cortex XDR reduces the time and experience required at every stage of security operations, from triage to threat hunting. Through tight integration with enforcement points like the Cortex XDR agent, it detects and contains threats quickly, and applies the knowledge gained to continually improve your security.

Palo Alto Networks Cybersecurity Academy

Cortex XDR speeds alert triage and incident response.



uncle-leo-PC | 10.196.173.139 | vssadmin.exe | 4652

PATH: C:\Windows\Temp\kernal.exe
USERNAME: uncle-leo-PC\uncle-leo
RUNNING TIME: Dec 11th 2018 08:19:29 - Still Running
SIGNATURE: Unsigned
MD5: 2ff7...ef7e
WILDFIRE SCORE: Malware
SHA256: 6ff0...1d4b
CMD: "C:\windows\temp\kernal.exe"

Coordinated enforcement

The integrated suite of Palo Alto Networks products delivers greater security value than isolated components. Whenever a next-generation firewall sees a new piece of malware, or whenever an endpoint sees a new threat, protections are made available in minutes to all other next-generation firewalls and endpoints running the Cortex XDR agent, requiring no administrative effort, whether it happens at 1 a.m. or 3 p.m. Tight integration between your network, endpoints, and clouds enables a continually improving security posture and provides coordinated enforcement to protect you from zero-day attacks.

Centralized logging across the platform

To surface evasive threats and prevent attacks, your organization must be able to perform advanced analytics as well as detection and response on all available data. Security applications that perform such analytics need access to scalable storage capacity and processing power.

Cortex Data Lake is a cloud-based storage offering for the context-rich, enhanced network and endpoint logs Palo Alto Networks security products generate, including next-generation firewalls, Prisma Access, and the Cortex XDR agent. The cloud-based nature of Cortex Data Lake allows you to collect ever-expanding volumes of data without needing to plan for local compute and storage.

Cortex XDR uses Cortex Data Lake to store all event and incident data it captures, ensuring a clean handoff to other Palo Alto Networks products and services, such as AutoFocus contextual threat intelligence, for further investigation and incident response with endpoint context.

Palo Alto Networks Cybersecurity

Cortex XDR technical architecture

The architecture of Cortex XDR is optimized for maximum availability, flexibility, and scalability to manage millions of endpoints. It comprises the following components:

Cortex XDR endpoint agent. The endpoint agent consists of various drivers and services, but it requires only minimal memory and CPU usage – 512MB of RAM and 200MB of disk space – to ensure a non-disruptive user experience. After it's deployed on your endpoints, your administrators have complete control over all Cortex XDR agents in your environment through the Cortex XDR console.

Cortex XDR management console. Cortex XDR is a cloud-based application designed to minimize the operational challenges associated with protecting your endpoints. From the web-based Cortex XDR console, you can manage endpoint security policy, review security events as they occur, identify threat information, and perform additional analysis of associated logs.

WildFire malware prevention service. Cortex XDR can send unknown malware to WildFire. Based on the properties, behaviors, and activities that a sample displays during analysis and execution in the WildFire sandbox, WildFire determines a verdict for the sample: benign, grayware, or malicious. WildFire then generates signatures and makes these globally available every five minutes, allowing other Palo Alto Networks products to recognize the newly discovered malware.

Cortex Data Lake. Cortex Data Lake is a scalable, cloud-based log repository that stores context-rich logs generated by Palo Alto Networks security products, including next-generation firewalls, Prisma Access, and Cortex XDR agents. The cloud-based nature of Cortex Data Lake allows you to collect ever-expanding volumes of data without needing to plan for local compute and storage.

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 Cortex Data Lake and WildFire without having to directly access the internet.

Palo Alto Networks Cybersecurity Academy