Take Your Endpoint Security to the Next Level

Replace Your Antivirus with Cortex XDR

Protecting your endpoints requires a much more holistic approach than simply blocking known malware. Adversaries today create countless variants of malware and use obfuscation techniques to evade signature detection. They can turn your own resources against you, converting legitimate endpoint applications into attack tools. They can even compromise unmanaged and internet of things (IoT) devices to infiltrate your network and take over your managed endpoints.

Against this backdrop of threats, your security team must think beyond static signature-based antivirus. You need a solution that can automatically block known and zero-day attacks as well as provide the visibility your analysts require for detection and response. This paper describes today's top risks and operational challenges. It then proposes a framework to mitigate these risks with Cortex XDR™.

State-sponsored attackers perfected the art of infiltrating victims' networks years ago, using cyberwarfare tactics such as reconnaissance, lateral movement, and privilege escalation. To avoid raising alarms, these adversaries even targeted unusual systems like routers, industrial control systems, Wi-Fi networks, and mobile phone SIM cards.

Today, many advanced attack methods once isolated to cyberwarfare activities have become commonplace in cybercrime and industrial espionage. Less-resourced threat actors have borrowed techniques from their more advanced peers to conduct targeted attacks that can bypass traditional endpoint protection. The criminals behind WastedLocker, SamSa, Maze, EKANS, and other ransomware families have demonstrated that the attack methods used to steal government secrets can be applied to with equal success to ransomware attacks.

The rising prevalence of attacks reveals the shortcomings of traditional security tools like antivirus. By examining effective attack techniques and the failures of legacy security solutions, we can decide what alternatives to put in place.

The Good, the Bad, and Everything in Between

Since the advent of malware, endpoint security vendors have focused on technologies that block known "bad" files, domains, and IP addresses using attack signatures and threat intelligence information. Unfortunately, a sophisticated attacker with enough motivation can find ways to elude static, signature-based defenses.

Therefore, to better fight endpoint threats, you should look for a robust endpoint security solution that can detect and block every stage of an attack, from the initial exploit to malware installation and ultimately to the malicious actions executed by running malware. Every layer of defense must be intelligent enough to resist evasion techniques and continuously adapt to catch the latest threats. You should also reduce your attack surface and shield sensitive data with endpoint protection features such as host firewall, device control, and disk encryption.

Increasingly, even run-of-the-mill adversaries are copying the advanced cyberwarfare techniques of more well-resourced attackers in order to camouflage their activity. They are shunning traditional malware and instead abusing legitimate applications like PowerShell® as part of living-off-the-land attacks.

Once they've compromised a host, these adversaries steal credentials and move laterally until they achieve their objectives. These post-intrusion, seemingly legitimate activities are difficult to block because attackers are using "good" applications and user credentials for underhanded purposes. Attackers are also compromising "good" devices like IoT, printers, or medical devices to conduct attacks. Malicious insiders, likewise, can hide in plain sight by using their existing privileges to steal or manipulate data.

While well-designed next-generation antivirus can automatically block (making it 99%+) of all threats, the novel and evasive threats that do succeed can wreak havoc. To stop stealthy attacks before the damage is done, you need proactive endpoint protection as well as detection and response. By collecting rich data, you can perform analytics and machine learning to unearth threats. You also build the foundation for threat hunting, investigations, and incident response.

To stop stealthy threats before the damage is done, you need proactive endpoint protection as well as detection and response.

Thinking Beyond the Endpoint

Most detection and response strategies focus only on the endpoint. However, many organizations' networks today have more unmanaged devices than managed when considering all IP-connected hosts across all network segments. Besides network data, security teams should consider other valuable data sources like cloud and authentication data, which—when integrated together—can provide a complete view of an organization and help reveal hidden threats.

Up until now, when security teams pursued a more holistic approach to detection and response, they had to deploy siloed tools for endpoint, network, and user-based detection and response. Teams that provisioned siloed tools were burdened with the costs of deploying and maintaining new network sensors and endpoint agents everywhere.

Siloed security tools also slow down investigations. With separate detection and response tools for endpoint, network, cloud, and user data, analysts are forced to pivot from console to console and manually piece together data to get a clear understanding of an attack. To investigate a network alert, for example, an analyst may need to perform painstaking analysis and correlation to identify the endpoint, network activity, and user associated with each incident. With today's complex and siloed tools, only specialized experts can navigate the labyrinth required for investigations.

What Is Needed

A new approach is required to solve today's security operations challenges—one that will ease every stage of security operations, from detection and threat hunting to triage, investigation, and response. This new approach requires the following three integrated capabilities, working together to lower risk and simplify operations:

- **Great endpoint threat prevention:** Highly effective prevention allows you to stop everything you can—the more than 99% of attacks that can be blocked automatically in real or near-real time—without manual verification. You need consistent, coordinated prevention across all your digital assets.
- **AI and machine learning:** With the growing amount of data being collected, your analysts shouldn't be forced to manually analyze or correlate data to identify threats. You need machine learning and analytics to learn the unique characteristics of your organization and form a baseline of expected behavior to detect sophisticated attacks.

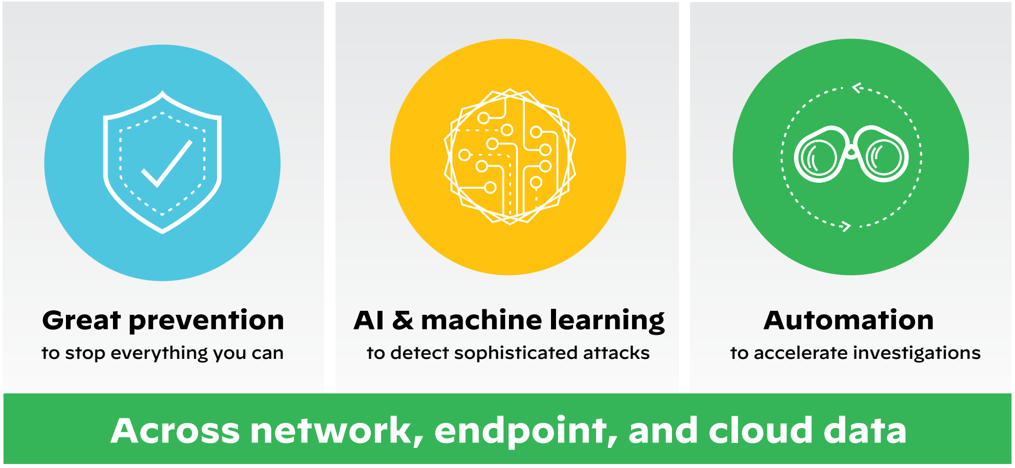

Great prevention
to stop everything you can
AI & machine learning
to detect sophisticated attacks
Automation
to accelerate investigations
Across network, endpoint, and cloud data

Figure 1: Critical integrated capabilities

- **Automation:** To quickly confirm attacks, analysts need actionable alerts with rich investigative details. They should also be able understand the root cause of attacks easily without needing years of experience.

With these three integrated capabilities coordinated across all your critical assets, including your network, endpoints, and clouds, you'll be able to defeat increasingly sophisticated threats.

Upgrade Your Endpoint Security with Cortex XDR

Cortex XDR is the industry's first extended detection and response platform that integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to protect your whole organization holistically while simplifying operations. It leverages behavioral analytics to identify unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

Cortex XDR helps you accelerate investigations by providing a complete picture of each incident. It stitches different types of data together and reveals the root cause and timeline of alerts, allowing your analysts to easily triage alerts. Tight integration with enforcement points lets you contain threats across your entire infrastructure.

With Cortex XDR, you can use your existing Palo Alto Networks network, endpoint, and cloud security as sensors and enforcement points, eliminating the need to deploy new software or hardware. You only need one data source—such as Palo Alto Networks ML-Powered Next-Generation Firewalls

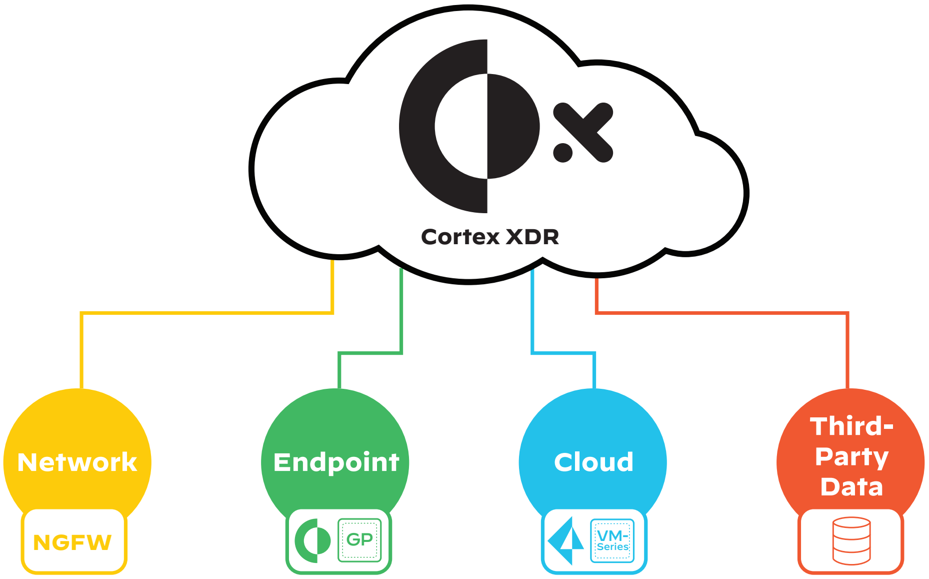


Figure 2: Analysis of data from multiple sources by Cortex XDR

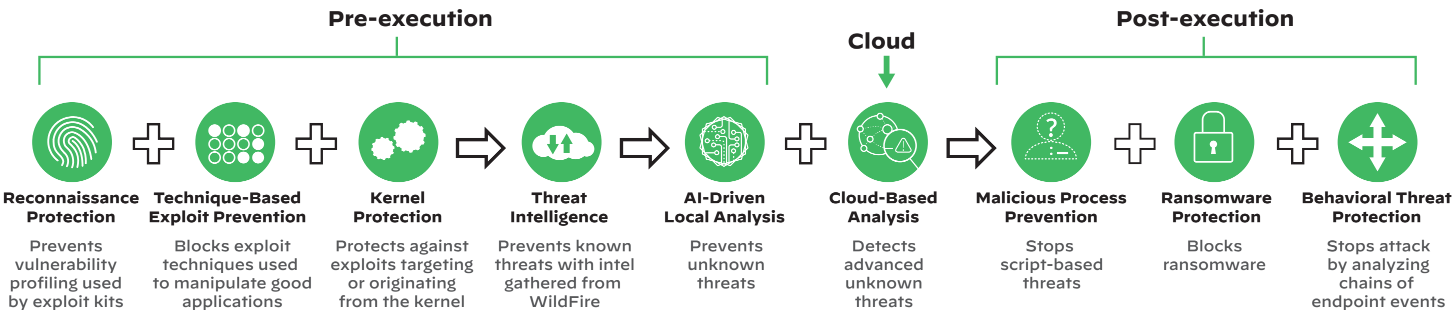

Pre-execution
Cloud
Post-execution
Reconnaissance Protection
Prevents vulnerability profiling used by exploit kits
Technique-Based Exploit Prevention
Blocks exploit techniques used to manipulate good applications
Kernel Protection
Protects against exploits targeting or originating from the kernel
Threat Intelligence
Prevents known threats with intel gathered from WildFire
AI-Driven Local Analysis
Prevents unknown threats
Cloud-Based Analysis
Detects advanced unknown threats
Malicious Process Prevention
Stops script-based threats
Ransomware Protection
Blocks ransomware
Behavioral Threat Protection
Stops attack by analyzing chains of endpoint events

Figure 3: Automatically preventing malware, exploits, and fileless attacks

(NGFWs) or Cortex XDR agents—to use Cortex XDR, but you would need multiple data sources to realize the benefits of data stitching and analysis. You can avoid provisioning cumbersome log infrastructure on-premises by storing all your data in a scalable and secure cloud-based data repository.

Achieve Closed-Loop Prevention, Detection, and Response

Prevent Known and Unknown Threats While Gaining Complete Visibility

Ironclad security starts with great prevention. To this end, Cortex XDR delivers best-in-class prevention to stop exploits, malware, ransomware, and fileless attacks. Designed for minimal endpoint impact, the lightweight Cortex XDR agent blocks attacks while simultaneously collecting event data for Cortex XDR.

The Cortex XDR agent offers a complete prevention stack, starting with 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.

Combining multiple methods of prevention, our next-generation antivirus (NGAV) stands apart in its ability to protect endpoints. It integrates with the Palo Alto Networks WildFire® malware prevention service to analyze suspicious files in the cloud and coordinate protection across all Palo Alto Networks security products. 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.

Palo Alto Networks provides a complete portfolio of network, endpoint, and cloud security offerings that prevent attacks by combining the latest breakthroughs in security, automation, and analytics. Cortex XDR integrates with these world-leading technologies, including our physical and virtual NGFWs as well as Prisma™ Access, enabling you to prevent advanced attacks while also collecting data for detection and response.

Securely Manage USB Devices

Despite their benefits, USB devices can also introduce risk. When users unwittingly connect malware-laden flash drives, keyboards, or web cameras to their computers or copy confidential data to backup disk drives, they expose their organizations to attack. The powerful device control module included with Cortex XDR allows you to 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.

Protect Your 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 encrypted with BitLocker and lists all encrypted drives. With host firewall and disk encryption, you can centrally manage your endpoint security policies from Cortex XDR.

Get Unprecedented Visibility and Swift Response with Host Insights

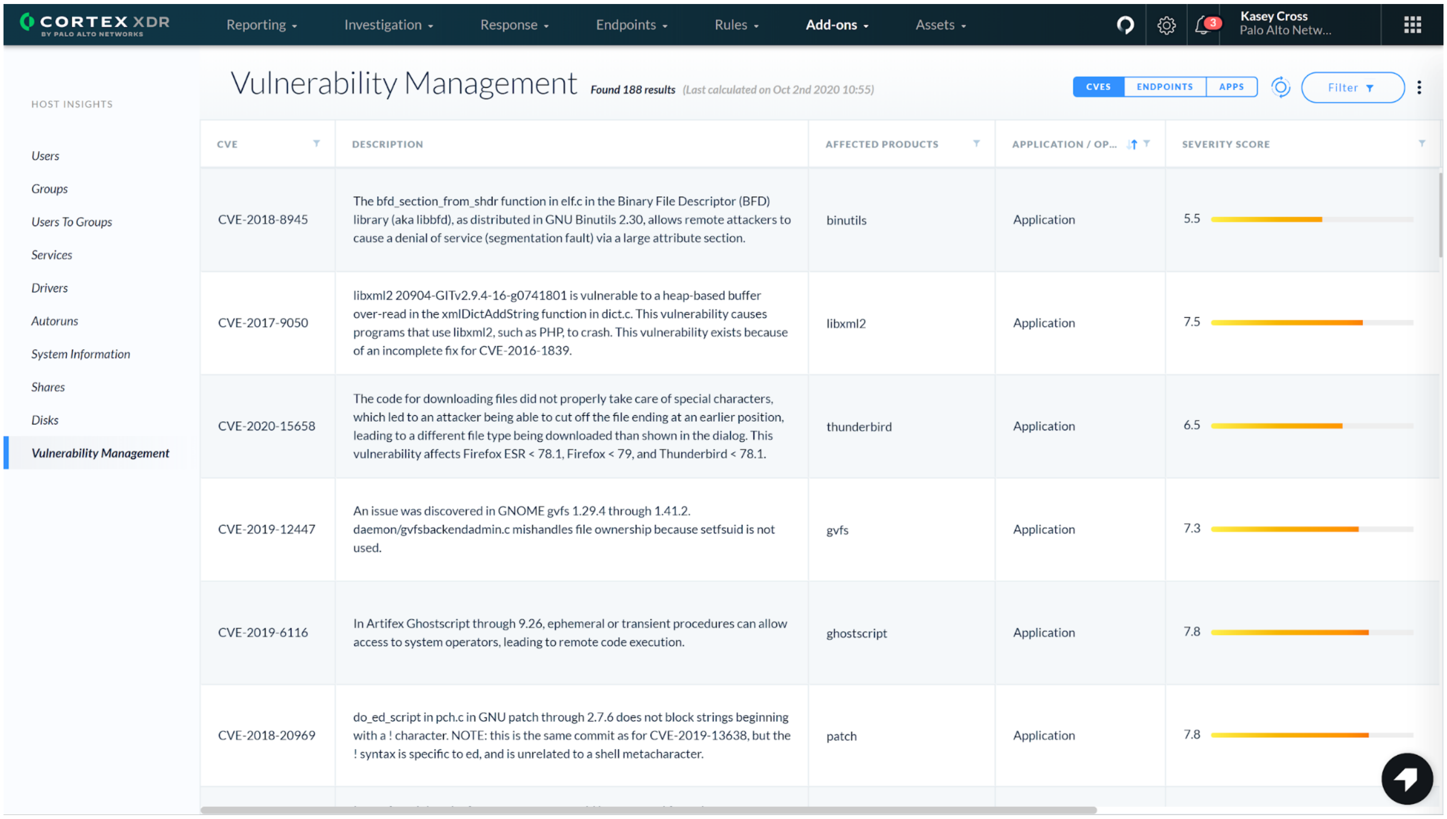
Safeguarding your endpoints starts with getting a clear picture of all your endpoint settings and contents as well as understanding your risks. Once you've identified a threat, you need to stop it quickly and ensure it hasn't spread to multiple endpoints.

With Host Insights, an add-on module for Cortex XDR, you get all these capabilities and more. Host Insights combines vulnerability management, application and system visibility, and a powerful Search and Destroy feature to help you identify and contain threats. Host Insights offers a holistic approach to endpoint visibility and attack containment, helping reduce your exposure to threats so you can avoid future breaches.

Figure 4: Host Insights module

Host Insights includes the following capabilities:

- **Search and Destroy** enables you to instantly find and eradicate threats across all endpoints. This powerful feature indexes all the files on your managed Windows endpoints so you can sweep your entire organization to find and remove malicious files in real time. Granular settings allow you to exclude files and directories on specific hosts.
- **Host inventory** lets you identify security gaps and improve your defensive posture with complete visibility across key Windows host settings and files. You can view information about users, groups, applications, services, drivers, autoruns, shares, disks, and system settings. By getting all your host details in one place, you can quickly identify security issues and speed investigations with additional host context.
- **Vulnerability management** provides you real-time visibility into vulnerability exposure and current patch levels across all endpoints to prioritize mitigation. Cortex XDR 2.5 reveals the vulnerabilities on your Linux endpoints, with up-to-date severity information provided by the NIST National Vulnerability Database. You can also see the Microsoft Windows Knowledge Base (KB) updates installed on your endpoints.



Vulnerability Management Found 188 results (Last calculated on Oct 2nd 2020 10:55)

CVE	DESCRIPTION	AFFECTED PRODUCTS	APPLICATION / OP...	SEVERITY SCORE
CVE-2018-8945	The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section.	binutils	Application	5.5
CVE-2017-9050	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE-2016-1839.	libxml2	Application	7.5
CVE-2020-15658	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.	thunderbird	Application	6.5
CVE-2019-12447	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles file ownership because setfsuid is not used.	gvfs	Application	7.3
CVE-2019-6116	In Artifex Ghostscript through 9.26, ephemeral or transient procedures can allow access to system operators, leading to remote code execution.	ghostscript	Application	7.8
CVE-2018-20969	do_ed_script in pch.c in GNU patch through 2.7.6 does not block strings beginning with a ! character. NOTE: this is the same commit as for CVE-2019-13638, but the ! syntax is specific to ed, and is unrelated to a shell metacharacter.	patch	Application	7.8

Figure 5: Vulnerability Assessment table with up-to-date CVE data from NIST

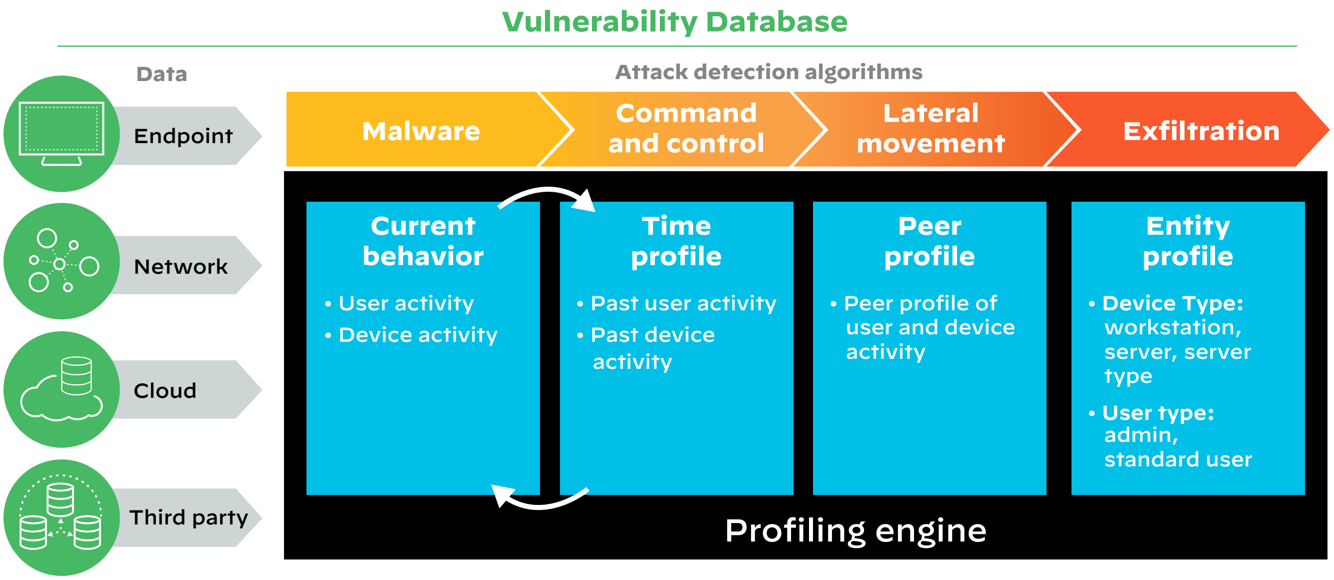


Figure 6: Behavioral analytics architecture for Cortex XDR

Automatically Detect Attacks with Behavioral Analytics and AI

Cortex XDR uncovers stealthy attacks using analytics and machine learning, allowing your team to focus on the threats that matter. Cortex XDR starts by analyzing rich data gathered across the Palo Alto Networks product portfolio, providing you complete visibility and eliminating blind spots. It stitches together data collected from your network, endpoints, and cloud assets to accurately detect attacks and simplify investigations.

Cortex XDR tracks more than 1,000 dimensions of behavior, including attributes that are nearly impossible to ascertain from traditional threat logs or high-level network flow data. It then profiles user and device behavior by taking advantage of:

- **Unsupervised machine learning:** Cortex XDR baselines user and device behavior, performs peer group analysis, and clusters devices into relevant groups of behavior. Based on these profiles, Cortex XDR detects anomalies compared to past behavior and peer behavior to detect malicious activity, such as malware behavior, command and control, lateral movement, and exfiltration.
- **Supervised machine learning:** Cortex XDR monitors multiple characteristics of network traffic to classify each device by type, such as a Windows computer, an Apple iPhone®, a mail server, or a vulnerability scanner. Cortex XDR also learns which users are IT administrators or normal users. With supervised machine learning, Cortex XDR recognizes deviations from expected behavior based on the type of user or device, reducing false positives.

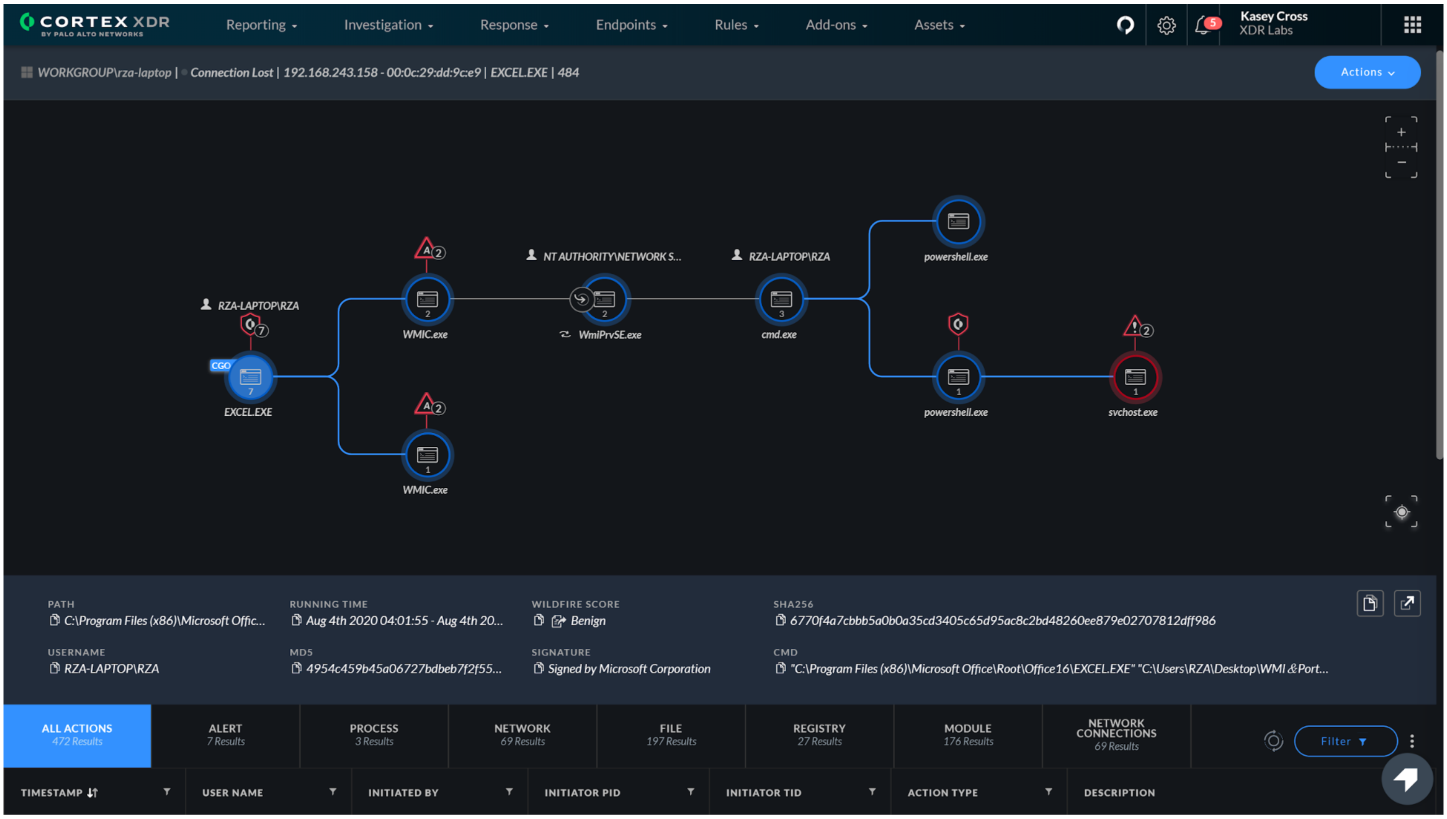
Uncover Evasive Threats with Custom Rules

Your security team can identify threats unique to your environment with flexible custom rules. Triggering alerts against known indicators of compromise (IOCs), such as malware hashes, can help identify known threats, but attackers can easily evade these detection techniques. Cortex XDR provides custom rules that enable your security team to detect complex combinations of behaviors to expose specific attacker tactics, techniques, and procedures (TTPs). As a result, your team can close known security gaps and gain visibility into potentially malicious activity being performed on the most valuable assets. Your custom rules can identify misuse of systems and applications as well as detect zero-day attacks that thwart evasion techniques, ensuring you can uncover threats even if an adversary manipulates malware names, hashes, or IP addresses.

Your analysts can define rules based on dozens of different parameters, including process, file, network, or registry information. More than 200 predefined rules detect a broad array of threats out of the box, including persistence, tampering, privilege escalation, and lateral movement. These detection capabilities work all day, every day, providing you peace of mind.

Hunt Threats and Search IOCs

Threat hunting plays a vital role in security operations, whether analysts are performing an independent search or expanding from an investigation. With search queries, your team can uncover suspicious activity by searching for specific hosts, files, processes, registry updates, network connections, and more. Queries can be precise, such as, "What are the changes made to a specific file by a specific process on a host?" or open-ended, such as "Show me all the processes running in the domain." Your security team can search for attack behaviors as well as traditional IOCs without learning a new query language. Analysts can filter results to reduce the number of events to review and reveal covert threats. Advanced threat hunters can execute complex text-based queries with wildcards and regular expressions to search across all their data in Cortex XDR. By incorporating threat intelligence with a complete set of network, endpoint, and cloud data, your team can find past attacks—or uncover incidents in progress—in seconds.



WORKGROUP\rza-laptop | Connection Lost | 192.168.243.158 - 00:0c:29:dd:9c:e9 | EXCEL.EXE | 484

PATH
C:\Program Files (x86)\Microsoft Offic...

RUNNING TIME
Aug 4th 2020 04:01:55 - Aug 4th 20...

WILDFIRE SCORE
Benign

SHA256
6770f4a7cbbb5a0b0a35cd3405c65d95ac8c2bd48260ee879e02707812dff986

USERNAME
RZA-LAPTOP\RZA

MD5
4954c459b45a06727bdbeb7f2f55...

SIGNATURE
Signed by Microsoft Corporation

CMD
"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\RZA\Desktop\WMI &Port...

Figure 7: Find the root cause of any alert, including network and cloud security alerts

Investigate Eight Times Faster with Data Integration and Automation

To expedite triage and analysis of any threat, your team needs full investigative context at their fingertips. Cortex XDR delivers several key features that accelerate alert triage and incident response. A unique incident management view groups related alerts to depict all elements of an attack, including affected hosts and users; threat intelligence details; and key artifacts, such as domains, IP addresses, and processes involved in the incident. Alert grouping and deduplication reduce the number of individual alerts to review by 98%, alleviating alert fatigue.

Your team can sort, filter, or export alerts. With a single click, they can investigate alerts from any source and instantly understand the root cause, reputation, and sequence of events associated, lowering the experience needed to verify threats.

Your team can conclusively answer the questions posed by any event, using these analysis views:

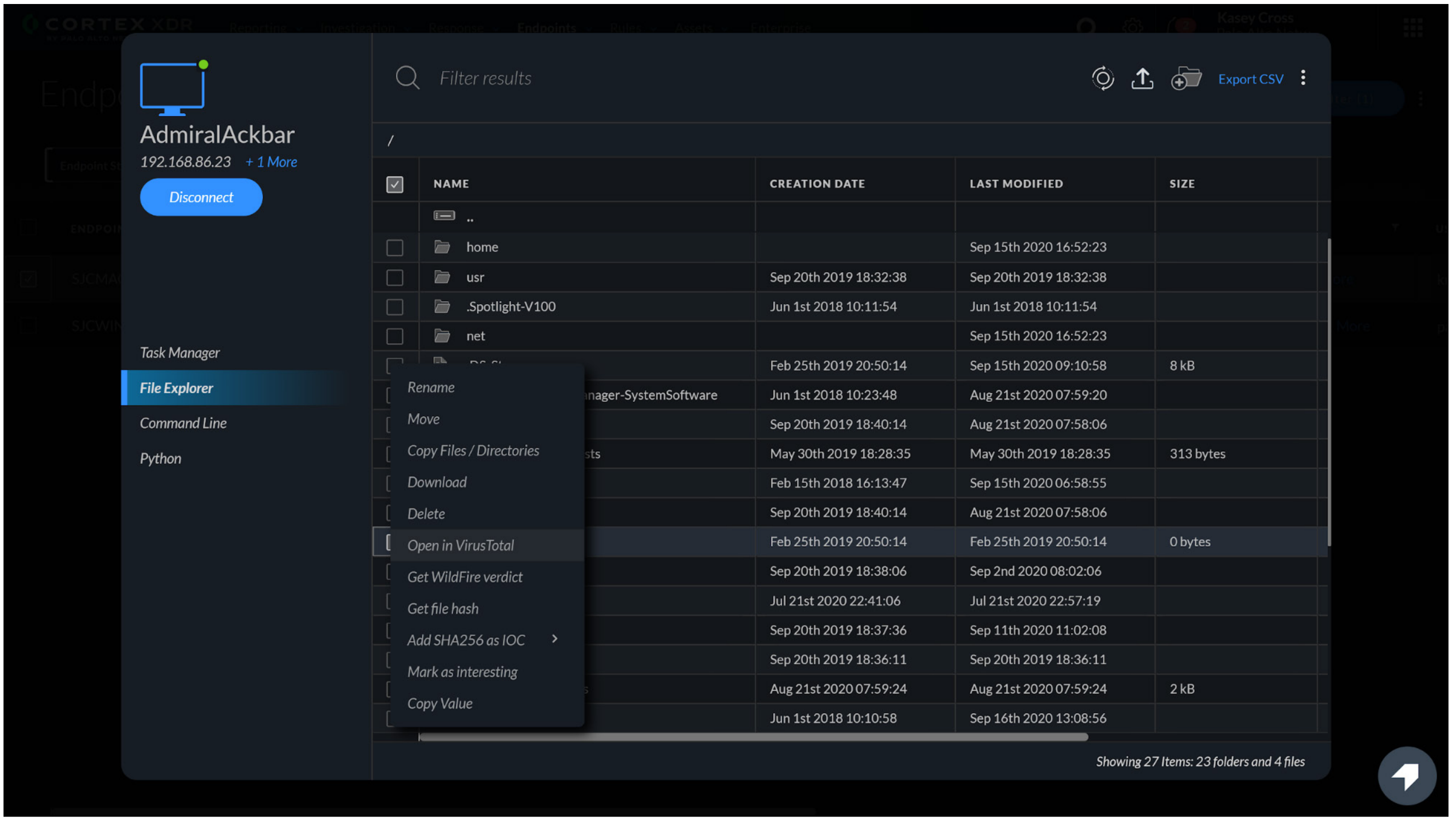
- **Root cause analysis view:** A unique, patented analysis engine continuously reviews billions of events to identify the chain of events behind every threat. It visualizes the attack sequence back to the root cause and provides essential details about each element in the sequence, making complex attacks easy to understand. Your analysts can instantly see which endpoint processes were responsible for network or cloud security alerts without manually correlating events or pivoting between consoles.
- **Timeline analysis view:** A forensic timeline of all attack activity provides actionable detail for incident investigations, allowing your analysts to determine the scope, impact, and next steps in seconds. Informational alerts improve timeline analysis by identifying suspicious behavior and making complex events easy to understand without cluttering your alert dashboard with low-risk events.

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. To discover rogue devices, it combines proactive scans with monitoring of endpoint, network, and third-party data to give you a complete view of all the assets in your environment.

Cortex XDR offers relief to teams struggling with a backlog of alerts and difficult, time-consuming analysis. Moreover, it simplifies alert triage and incident investigation with intuitive, visual, context-driven tools. Analysis that used to take hours, days, or weeks can be accomplished in seconds or minutes—all with less specialized expertise.

Respond and Adapt to Threats

Once you identify threats, you need to contain them quickly. Cortex XDR lets your security team instantly eliminate network, endpoint, and cloud threats from one console. Your team can quickly stop the spread of malware, restrict network activity to and from devices, and update threat



☑	NAME	CREATION DATE	LAST MODIFIED	SIZE
	..			
☐	home		Sep 15th 2020 16:52:23	
☐	usr	Sep 20th 2019 18:32:38	Sep 20th 2019 18:32:38	
☐	.Spotlight-V100	Jun 1st 2018 10:11:54	Jun 1st 2018 10:11:54	
☐	net		Sep 15th 2020 16:52:23	
☐		Feb 25th 2019 20:50:14	Sep 15th 2020 09:10:58	8 kB
☐	nager-SystemSoftware	Jun 1st 2018 10:23:48	Aug 21st 2020 07:59:20	
☐		Sep 20th 2019 18:40:14	Aug 21st 2020 07:58:06	
☐	sts	May 30th 2019 18:28:35	May 30th 2019 18:28:35	313 bytes
☐		Feb 15th 2018 16:13:47	Sep 15th 2020 06:58:55	
☐		Sep 20th 2019 18:40:14	Aug 21st 2020 07:58:06	
☐		Feb 25th 2019 20:50:14	Feb 25th 2019 20:50:14	0 bytes
☐		Sep 20th 2019 18:38:06	Sep 2nd 2020 08:02:06	
☐		Jul 21st 2020 22:41:06	Jul 21st 2020 22:57:19	
☐		Sep 20th 2019 18:37:36	Sep 11th 2020 11:02:08	
☐		Sep 20th 2019 18:36:11	Sep 20th 2019 18:36:11	
☐	s	Aug 21st 2020 07:59:24	Aug 21st 2020 07:59:24	2 kB
☐		Jun 1st 2018 10:10:58	Sep 16th 2020 13:08:56	

Showing 27 Items: 23 folders and 4 files

Figure 8: Cortex XDR Live Terminal task manager

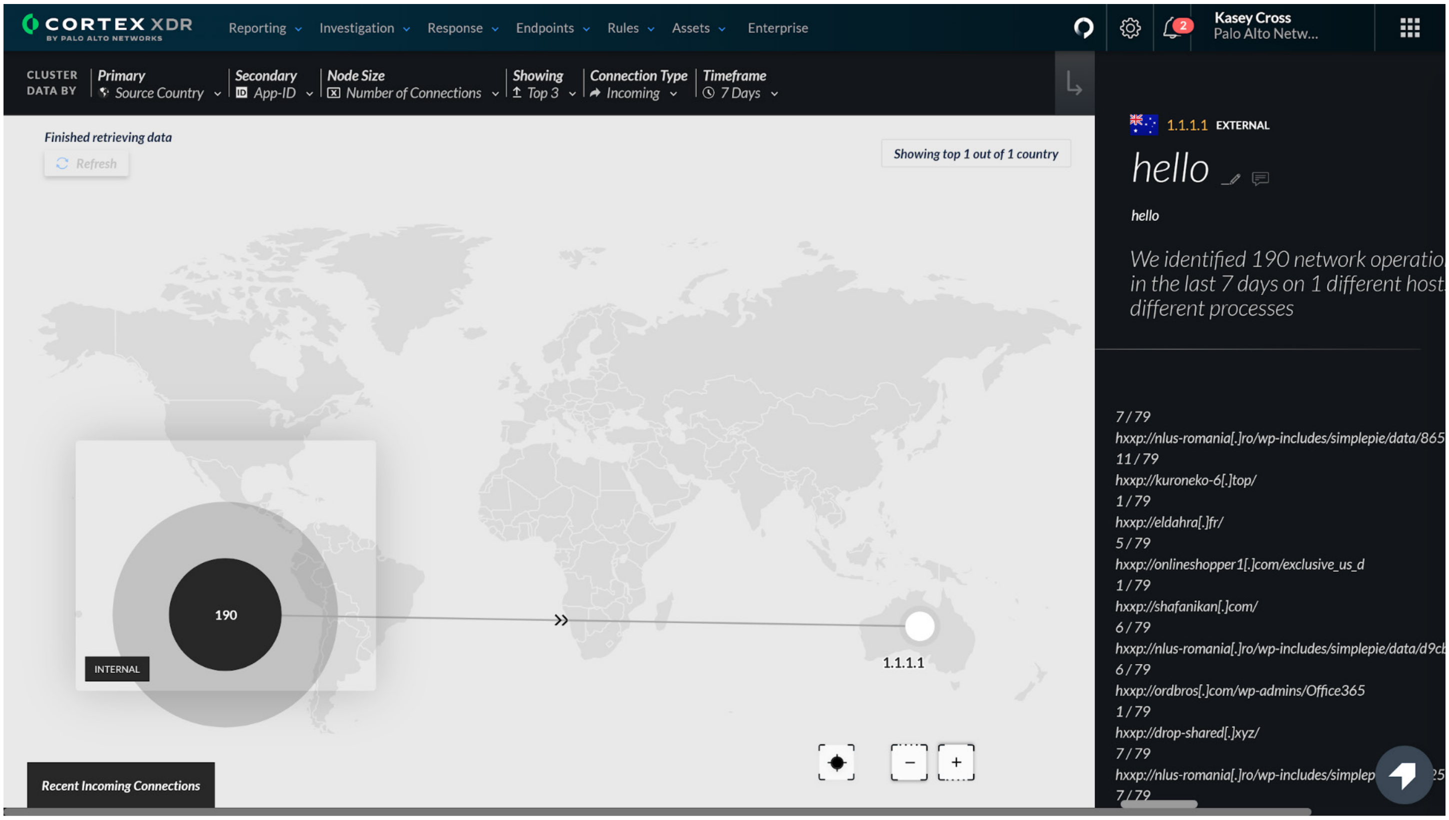
prevention lists (e.g., bad domains) through tight integration with enforcement points.

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

- **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 adding it to the block list 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. Your teams can also terminate and delete processes in a live environment on any host with full auditing conducted as they work. All the while, end users can continue to work without disruption or downtime while threats are eliminated.
- **Use open APIs** to integrate with third-party management tools, enforce policies and collect agent information from any location.
- **Integrate with Cortex™ XSOAR** for security orchestration, automation, and response. Your team can share incident data with Cortex XSOAR for automated, playbook-driven response that spans more than 450 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. Remediation suggestions simplify response by recommending next steps and allowing you to resolve all activities identified in an incident. 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.

Unify Management, Reporting, Triage, and Response

Cortex XDR provides a seamless platform experience by combining endpoint policy management, detection, investigation, and response in one web-based management console. You can quickly assess security status with customizable dashboards and summarize incidents as well as track security trends with graphical reports that can be scheduled or



Finished retrieving data

hello

hello

We identified 190 network operatio
in the last 7 days on 1 different host
different processes

```
7 / 79
hxxp://nlus-romania[.]ro/wp-includes/simplepie/data/865
11 / 79
hxxp://kuroneko-6[.]top/
1 / 79
hxxp://eldahra[.]fr/
5 / 79
hxxp://onlineshopper1[.]com/exclusive_us_d
1 / 79
hxxp://shafanikan[.]com/
6 / 79
hxxp://nlus-romania[.]ro/wp-includes/simplepie/data/d9cb
6 / 79
hxxp://ordbros[.]com/wp-admins/Office365
1 / 79
hxxp://drop-shared[.]xyz/
7 / 79
hxxp://nlus-romania[.]ro/wp-includes/simplep      25
7 / 79
```

Figure 9: IP View—actionable details and investigative context about IP addresses

generated on demand. You can also easily deploy and upgrade Cortex XDR agents from a central location.

Cortex XDR offers industry-leading detection by accurately identifying 90% of attack techniques in MITRE ATT&CK® testing.

Cortex XDR continually evolves to anticipate threats and outsmart attackers. It integrates with WildFire, the industry-leading malware analysis service, to identify malware. As a cloud native application, Cortex XDR can harness community-sourced findings to identify adversaries' latest tactics and improve detection accuracy.

Get Peace of Mind with Managed Threat Hunting

Cortex XDR Managed Threat Hunting offers round-the-clock monitoring from world-class threat hunters and the industry's first threat hunting service operating across integrated endpoint, network, and cloud data. Our Unit 42 experts work on your behalf to discover advanced threats, such as state-sponsored attackers, cybercriminals, malicious insiders, and malware. To detect adversaries hiding in your organization, our hunters comb through comprehensive data from Palo Alto Networks and third-party security solutions.

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.

The Silver Lining of Cloud Deployment

As a cloud-based app, Cortex XDR eliminates the need to deploy additional on-premises software or hardware. It uses your existing Palo Alto Networks products, including the Cortex XDR agent, as sensors and enforcement points to streamline security operations. The data collected from your Palo Alto Networks infrastructure is stored in the Cortex XDR platform, which delivers efficient log storage that scales to handle the large volume of data needed for detection and response. You can quickly deploy Cortex XDR, 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

MITRE | ATT&CK®

Cortex XDR offers industry-leading detection by accurately identifying 90% of attack techniques in MITRE ATT&CK® testing.

cost of ownership by 44% on average. Cortex XDR also boosts the productivity of your security operations team by automatically detecting attacks and accelerating investigations.

Upgrade Your Endpoint Security with Cortex XDR

There's never been a better time to replace your existing antivirus or endpoint protection with Cortex XDR. Here are a few reasons why you should choose Cortex XDR to safeguard your endpoints and future-proof your security operations:

- **Stop real-world threats with proven validation:** In multiple third-party tests, including the MITRE ATT&CK framework, Cortex XDR had the broadest coverage among all vendors evaluated.
- **Block attacks at every stage in the attack lifecycle:** Cortex XDR offers the most complete endpoint protection available, allowing you to replace all your traditional and next-generation antivirus agents with one powerful, lightweight agent that stops exploits, malware, ransomware, and fileless attacks with unmatched accuracy.
- **Reduce infrastructure costs and operational complexity:** Cortex XDR is a cloud native platform that offers effortless deployment and management of endpoint agents. You can eliminate the need for on-premises network sensors for network-based threat detection by collecting traffic data from your existing NGFWs.
- **Eliminate security silos with extended detection and response:** The integrated suite of Palo Alto Networks products delivers greater security value than isolated components. Tight integration between your network, endpoints, and clouds continually improves your security posture and provides coordinated enforcement to protect you from zero-day attacks.
- **Expedite investigation and response:** Cortex XDR speeds up alert triage and incident response by providing a complete picture of an attack, including root cause, and stitching together the sequence of events.

With Cortex XDR, you gain complete visibility and protection across your network, endpoint, and cloud assets, so you can rest assured that all your users and digital assets are secure.

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

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.