Cortex XDR

Breaking the Security Silos for Detection and Response

Security teams face a dizzying array of threats, from ransomware and cyberespionage to fileless attacks and damaging data breaches. However, the biggest headache for many security analysts is not the endless number of risks that dominate news headlines, but rather the repetitive tasks they must perform every day as they triage incidents and attempt to whittle down an endless backlog of alerts.

This paper describes the thorniest challenges security analysts confront, including a deluge of alerts and complex investigation processes that can overwhelm even the most mature security operations centers (SOCs). It then proposes a framework to tackle every stage of security operations with Cortex® XDR™ for detection and response. As the specters of malware, targeted attacks, and insider abuse continually escalate, a tool like Cortex XDR can be your secret weapon to eliminate threats and simplify operations.

Analysts Under Siege

Security teams today face two daunting challenges: a continual barrage of attacks and an endless sea of alerts. Security teams know threat actors can launch an unlimited number of attacks, consequence-free, until one succeeds. To reduce the possibility of an intrusion, teams typically deploy multiple layers of security, but these tools generate a massive 11,000 alerts per week on average.[1]

To keep up with all these alerts, analysts often operate in firefighting mode, attempting to triage as many alerts as possible every day. Because these alerts often lack essential context needed for investigations, analysts are forced to waste valuable time chasing down additional details. Overwhelmed by inaccurate and incomplete alerts, 53% security teams can review less than half of the alerts they receive,[2] increasing the risk of a data breach.

Looking for Threats in All the Wrong Places

The rising tide of attacks has convinced organizations of all sizes to embrace detection and response. To address this newfound demand, the IT security industry has introduced a slew of siloed tools, such as endpoint detection and response (EDR), network detection and response (NDR), and user behavior analytics (UBA). However, these siloed tools provide a narrow view of activity and require years of specialist experience to operate. Security teams that provision these tools will be burdened with the costs of deploying and maintaining new network sensors and endpoint agents everywhere.

On the other hand, organizations that don't deploy detection and response will likely overlook stealthy attacks, such as highly evasive malware, malicious insiders, or targeted attacks. This is because advanced attacks often do not use traditional indicators of compromise (IOCs), such as attack signatures or malicious domains. The only way to detect these threats is to examine activity—not just alerts—over time and across data sources with machine learning and analytics.

Manual Investigations Increase Attacker Dwell Times

Detecting attacks is only half the battle. Analysts must also investigate alerts and assess the "who, what, when, why, and how" details to determine what action to take. Unfortunately, many of today's security tools only present high-level alerts with limited user, endpoint, network, application, and threat intelligence information. These high-level alerts rarely provide all the context needed for investigation and response. As a result, analysts must 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.

Since these tools rarely work together, analysts cannot easily coordinate response across all their enforcement points. Instead of quickly blocking an attack, they must submit a ticket or ask other team members to update security

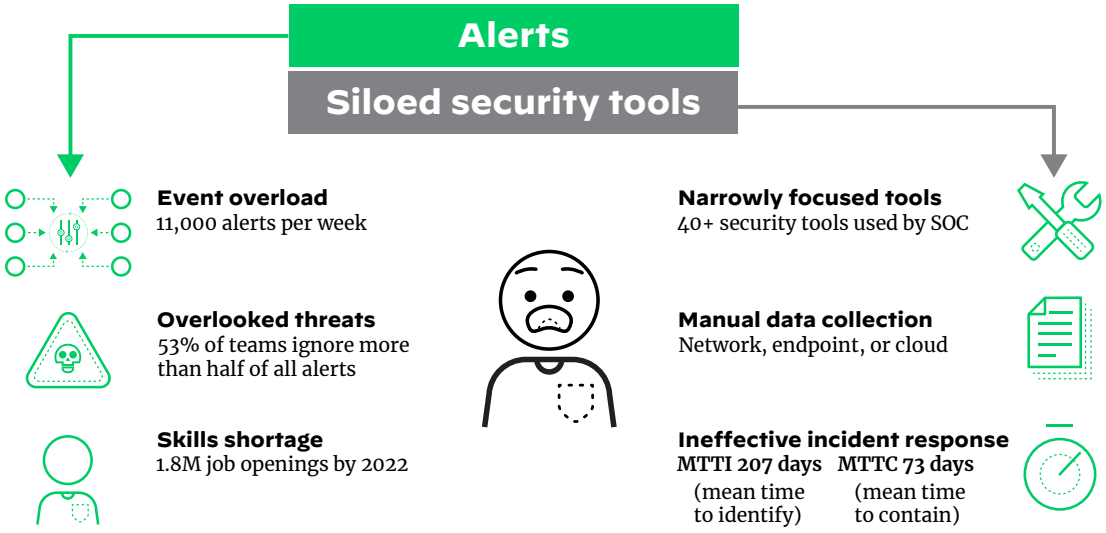

Figure 1: A security analyst's many burdens

1. "The 2020 State of Security Operations," Forrester, September 2020, https://start.paloaltonetworks.com/forrester-2020-state-of-secops.html.
2. Ibid.

policies, which might take days or weeks. It's not surprising, then, that it takes organizations 207 days to identify a breach, and 73 day to contain it, on average.[3] Faced with a shortage of cybersecurity professionals, teams need to break down security silos and simplify incident response or they will struggle to prevent successful cyberattacks.

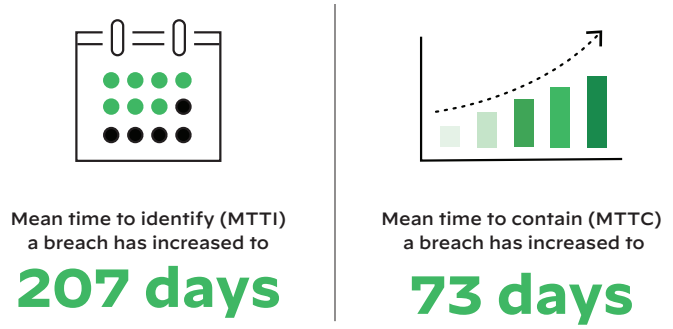

Figure 2: Rising MTTI and MTTC

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 three integrated capabilities working together to lower risk and simplify operations:

- **Great 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.
- **Automation**: To quickly confirm attacks, analysts need actionable alerts with rich investigative details. They should also be able to 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.

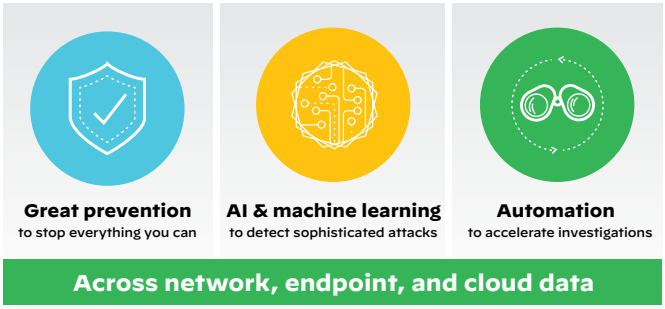

Figure 3: Critical integrated capabilities

Cortex XDR Detection and Response

Cortex XDR is the industry's first extended detection and response platform that natively integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations like yours secure your digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

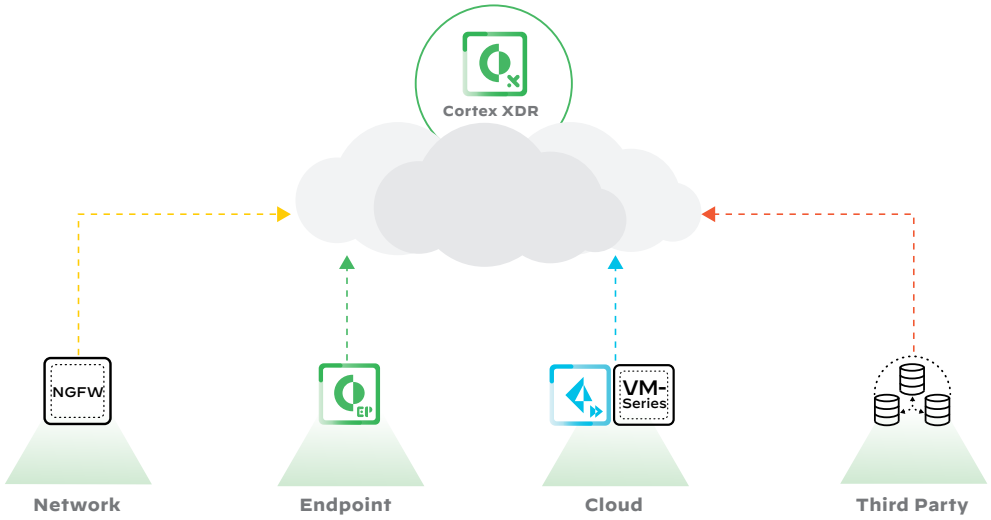

Figure 4: Analysis of data from multiple sources by Cortex XDR

3. "2020 Cost of a Data Breach Study," Ponemon Institute, July 2020, https://www.ibm.com/downloads/cas/861MNWN2.

Cortex XDR helps you accelerate investigations by providing a complete picture of each alert. It stitches different types of data together and reveals the root cause and timeline of alerts, allowing analysts of all experience levels to perform triage. Tight integration with enforcement points lets you respond to threats anywhere in your organization or restore hosts to a clean state easily.

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 to use Cortex XDR, but you 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.

Cortex XDR Protects You at Every Stage of Security Operations

Attackers continually innovate. To outpace them, security teams must implement a repeatable process to proactively block attacks with best-in-class prevention and to discover and stop active threats. Cortex XDR gives you the tools to accomplish four iterative steps:

1. Prevent
2. Automatically detect
3. Rapidly investigate
4. Respond and adapt

This framework provides everything you need to secure your organization today and in the future.

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 Next-Generation Firewalls, Prisma® Access, and an array of third-party tools, enabling you to prevent advanced attacks while also collecting data for detection and response.

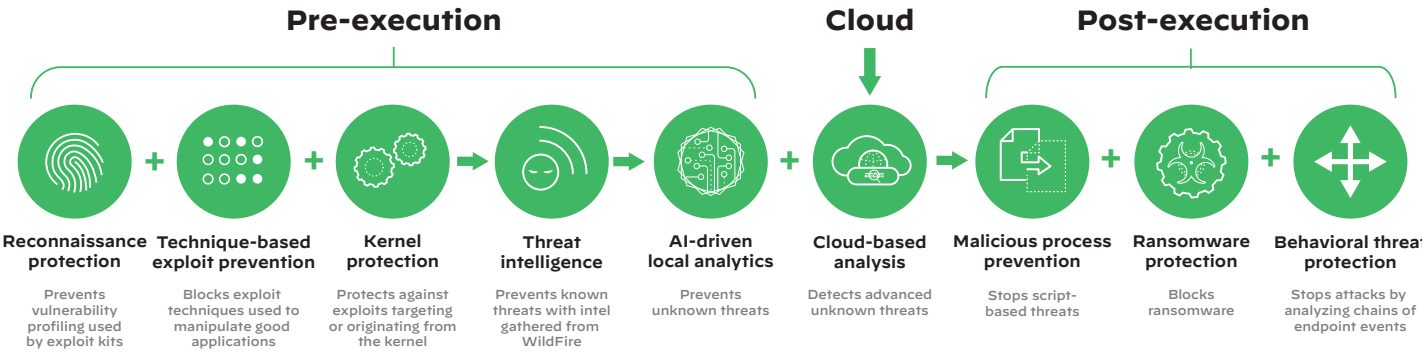

Figure 5: Automatically preventing malware, exploits, and fileless attacks

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® or macOS® endpoints. Additionally, you can apply BitLocker® or FileVault® encryption or decryption on your endpoints by creating disk encryption rules and policies. Cortex XDR provides full visibility into endpoints encrypted with BitLocker or FileVault 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 and 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 assessment, 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 6: Host Insights module features

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 Assessment** provides real-time visibility into vulnerability exposure and current patch levels across all endpoints to prioritize mitigation. Cortex XDR reveals the vulnerabilities on your Linux and Windows endpoints, with up-to-date severity information provided by the NIST National Vulnerability Database and Microsoft Security Response Center. You can also see the Microsoft Windows Knowledge Base (KB) updates installed on your endpoints.

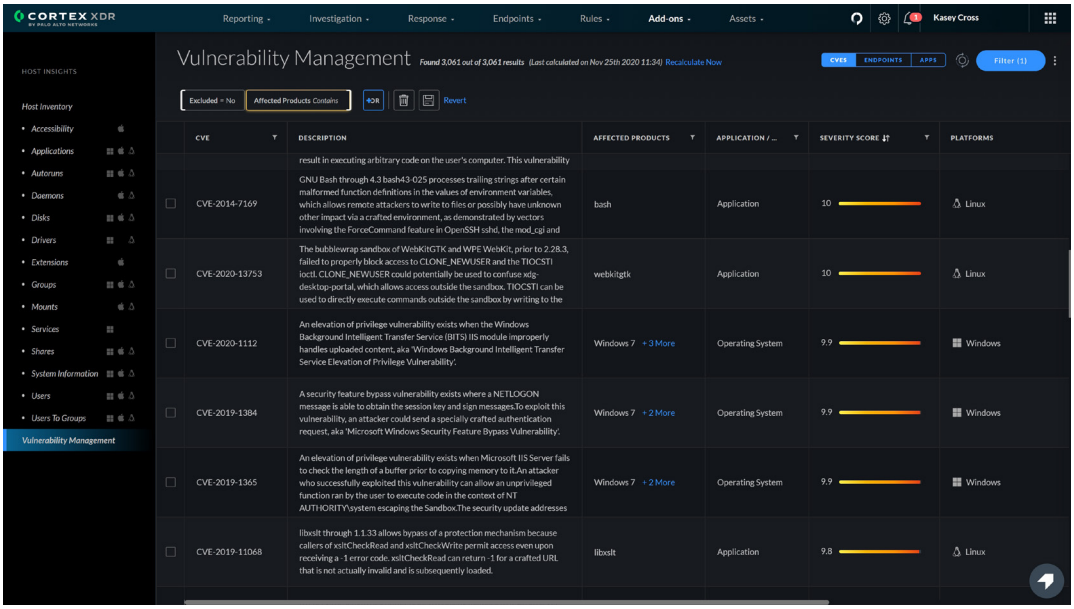

Figure 7: Vulnerability Assessment table with up-to-date CVE data

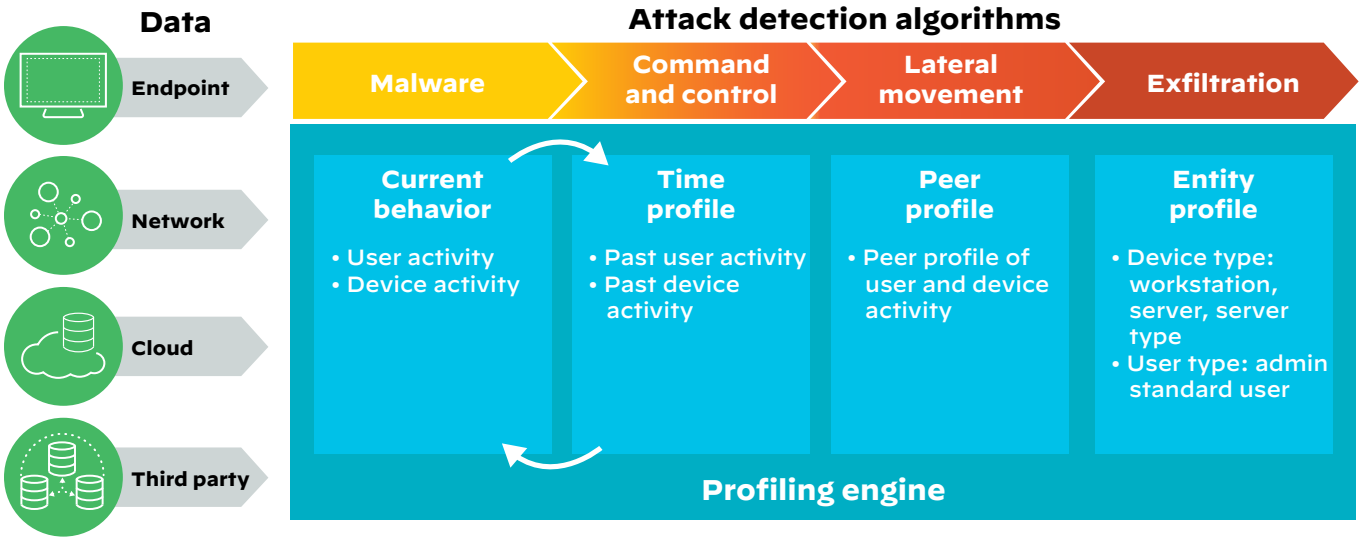

Figure 8: Behavioral analytics architecture for Cortex XDR

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.

By examining rich network, endpoint, and cloud data, building behavioral profiles, and analyzing these profiles with a broad set of detection algorithms, Cortex XDR can pinpoint stealthy attacks with unparalleled precision.

Uncover Evasive Threats with Custom Rules

Your security team can identify threats unique to your environment with flexible custom rules. Triggering alerts against known 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.

Data Inspected by Cortex XDR

Cortex XDR analyzes protocol-level metadata in traffic logs, enhanced application logs, and threat logs collected by Palo Alto Networks physical and virtual NGFWs as well as Prisma Access. It also examines endpoint data from Cortex XDR agents, third-party alerts, and log data. By building a profile based on hundreds of dimensions of behavior, including frequency of connections, source and destination of traffic, protocols used, and more, Cortex XDR can learn the expected behavior of users and devices. Cortex XDR also monitors internal traffic as well as outbound traffic from clients and servers to the internet.

Session-Level Data

Firewall traffic logs provide the metadata needed to profile user and device behavior, including:

- Source IP, destination IP, source port, and destination port
- Bytes sent and received
- Connection duration
- Enhanced application logs with transaction-level data on DNS, HTTP, DHCP, RPC, ARP, ICMP, and more
- Application details from App-ID™ technology

User Data

Cortex XDR analyzes network traffic and endpoint data to extract user context, such as:

- Logged-in user
- Typical user of a machine
- User creating the process that initiated the communication
- User group and organizational unit from Directory Sync
- Authentication events from Okta, Azure Active Directory, PingOne, PingFederate, Kerberos, and Windows event logs

Cloud Data

Cortex XDR gathers comprehensive cloud logs from:

- Prisma Access and VM-Series
- Google Cloud and Google Kubernetes® Engine
- Amazon CloudWatch and AWS® CloudTrail®

Endpoint Data

Cortex XDR analyzes all endpoint activity, including:

- File creation, deletion, and update
- File hash
- File path
- Process name
- Registry change
- CLI arguments, RPC calls, and code injection
- Hardware events, such as USB
- Event log manipulation
- Cortex XDR agent security alerts
- WildFire malware verdict

Host Data

Cortex XDR identifies machines by tracking:

- Hostname
- MAC address
- Operating system

Data Retention

- Minimum 30 days

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 queries with wildcards and regular expressions, aggregate and visualize their search results, and search across all their data with XQL Search. 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.

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. Incident scoring lets you rank and prioritize high-risk incidents to focus on what matters. Your team can sort, filter, or export incidents and 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.

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.

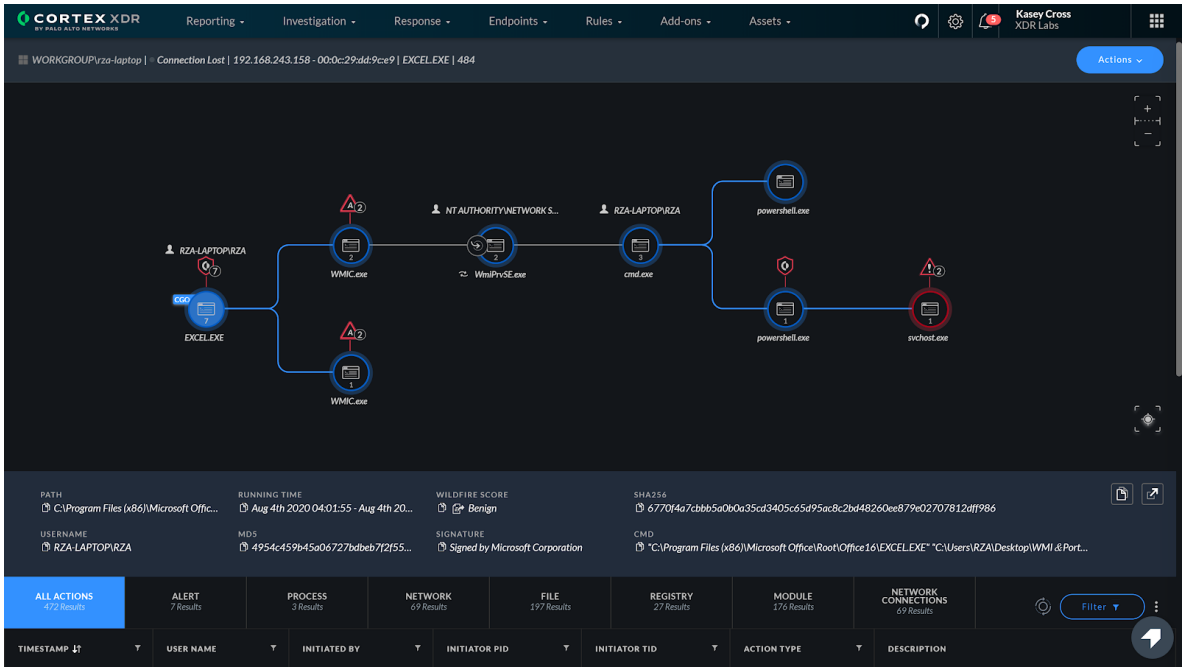

Figure 9: Root cause of alerts along with key artifacts, displayed in Cortex XDR

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 prevention lists, such as bad domains, through tight integration with enforcement points.

You can quickly eliminate threats with flexible response options that allow you 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.

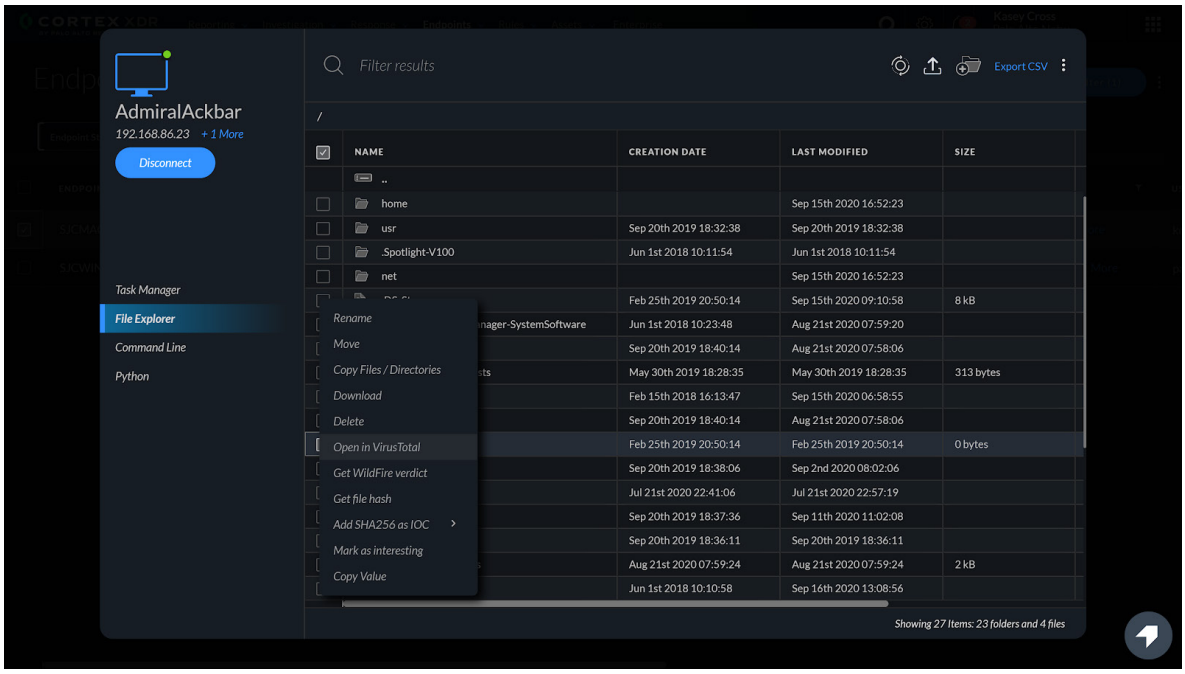

Figure 10: Cortex XDR Live Terminal task manager

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

MITRE | ATT&CK®

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's most comprehensive 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 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.

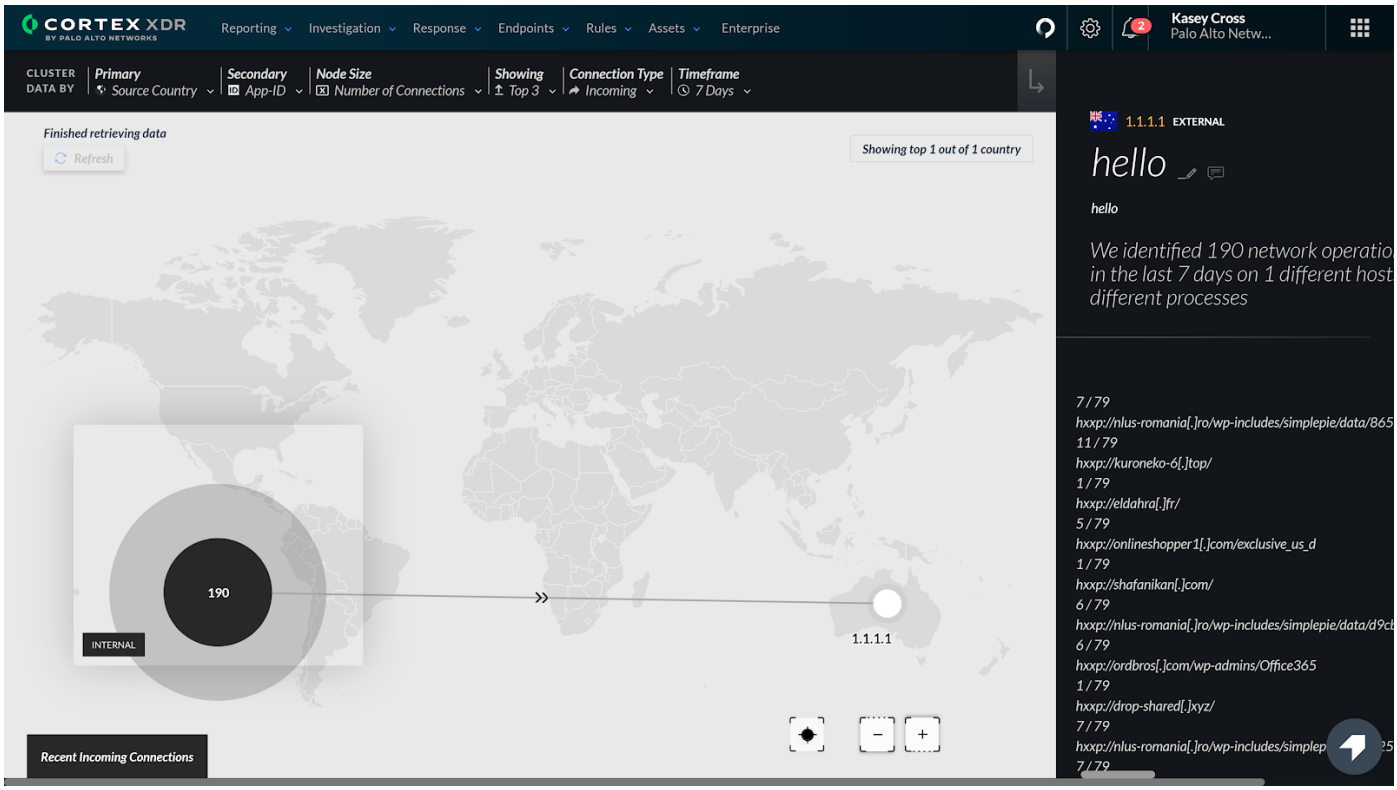

Figure 11: IP View—actionable details and investigative context about IP addresses

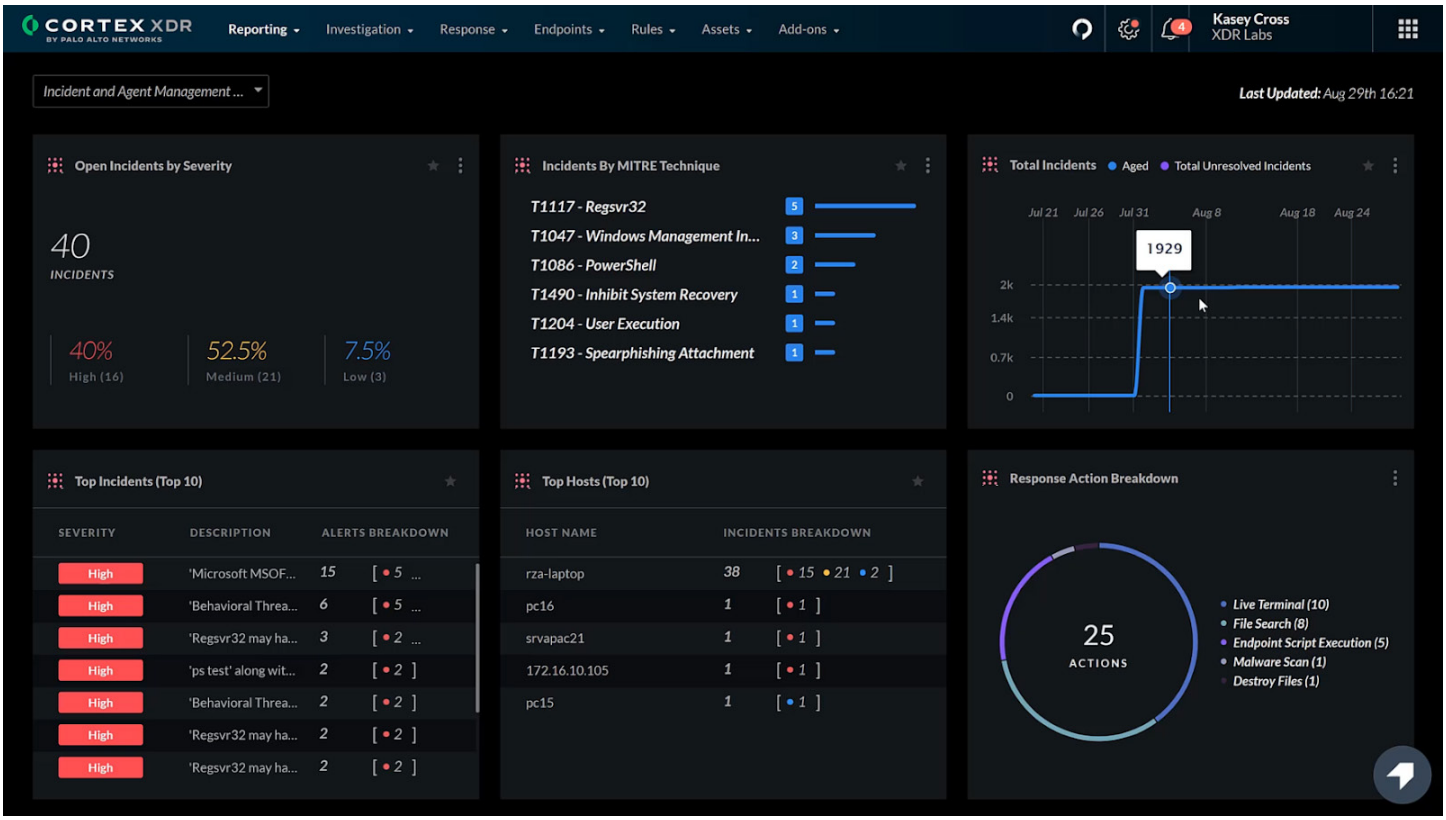

Figure 12: Cortex XDR dashboard

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 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.

Elevate Your Security with Cortex XDR

These are the times that try analysts' souls. To keep up with ever-increasing threats, organizations deploy more and more siloed tools that produce an avalanche of incomplete, inaccurate alerts. Instead of using cloud-based machine learning to cut through the noise and find hard-to-detect attacks, legacy security information and event management (SIEM) products focus on aggregating alerts for threats that were identified and typically stopped by security infrastructure. On the other hand, siloed detection and response tools force IT staff to deploy additional hardware and software, but they only offer a narrow view of threats, creating blind spots while forcing analysts to gather and correlate clues from multiple tools.

Cortex XDR gives your analysts the secret weapon they need to eradicate elusive threats anywhere in your environment by stitching together and analyzing all your network, endpoint, and cloud data. With Cortex XDR, you can:

- Prevent advanced malware, exploits, and fileless attacks with the Cortex XDR agent.
- Automatically detect stealthy attacks with machine learning and analytics.
- Accelerate alert triage and investigations to increase the productivity of all your security analysts by revealing the root cause of any alert.
- Quickly contain threats by coordinating response across enforcement points.
- Simplify operations and improve scale and agility with cloud native deployment.

With Cortex XDR, you gain complete visibility across your network, endpoint, and cloud assets, so you can rest assured that all your users and data 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

© 2021 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. cortex_wp_cortex-xdr_112920