TOP FIVE REQUIREMENTS FOR EFFECTIVE ENDPOINT PROTECTION

Attackers must complete a certain sequence of events, known as the attack lifecycle, to accomplish their objectives, whether stealing information or running ransomware. Nearly every attack relies on compromising an endpoint to succeed, and although most organizations have deployed endpoint protection, infections are still common.

Cortex XDR™ provides everything you need to safeguard your endpoints. It combines industry-best AI and behavior-based protection to block advanced malware, exploits, and fileless attacks. By integrating Cortex XDR with your existing network and cloud security from Palo Alto Networks, you can achieve consistent, coordinated security across your organization.

Ransomware continues to plague organizations. Many advanced attackers today are blending two primary attack methods: targeting application vulnerabilities and deploying malicious files, including ransomware. These methods can be used individually or in various combinations, but they are fundamentally different in nature:

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

Due to the fundamental differences between malware and exploits, an effective prevention approach must protect against both. The Cortex XDR agent combines multiple methods of prevention at critical phases of 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 or not it is connected to an organization's network.

This paper highlights the primary benefits our customers enjoy with the Cortex XDR agent.

1. Fighting Threats with Cloud-Based Malware Analysis

Today's complex threat landscape—combined with the diversity, volume, and sophistication of threats in the modern enterprise environment—makes effective threat prevention challenging. This problem is compounded by the challenge of detecting never-before-seen malware and exploits in addition to identifying known malicious content.

To address these sophisticated, targeted, and evasive threats, endpoint protection must integrate with shared threat intelligence to learn and evolve its defenses. IDC Research reports that 39% of security professionals consider shared threat intelligence a high or extreme priority to improve security posture.[1] To that end, integrating cloud-based threat intelligence with endpoint protection enables deeper analysis to rapidly detect potentially unknown threats.

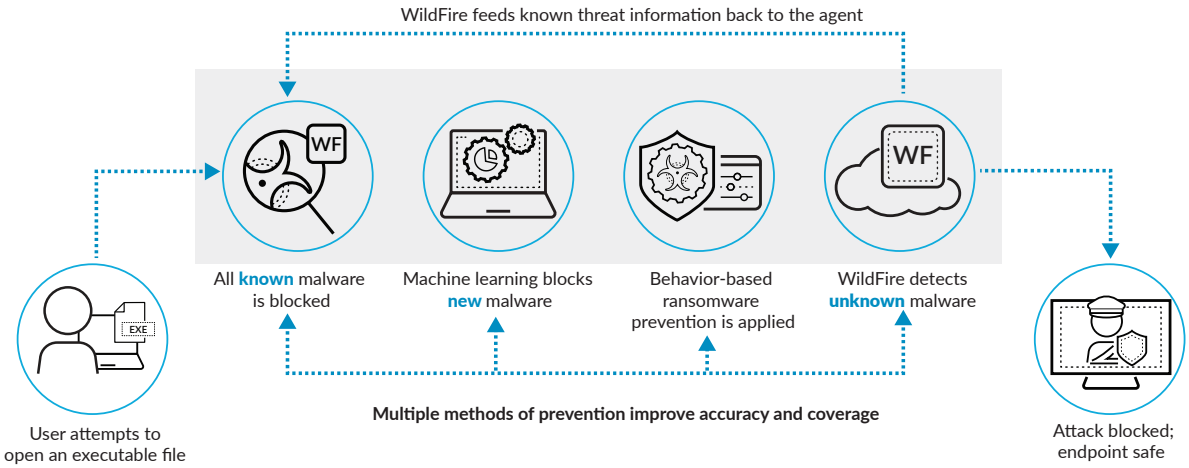

Figure 1: Preventing known and unknown threats

Cortex XDR and WildFire

The Cortex XDR agent prevents the execution of malicious files with an approach tailored to face traditional and modern attacks. To increase prevention accuracy and coverage, the agent takes advantage of multiple elements of WildFire® malware prevention service.

Threat Intelligence

Cortex XDR queries WildFire to quickly determine whether an instance of malware has been seen before, shortening the time to a verdict and immediately blocking known threats.

Machine Learning on the Endpoint

Cortex XDR uses machine learning to identify new threats. With more than 14 billion samples and 7 trillion artifacts collected and processed, WildFire has trained the Cortex XDR agent to identify both bad and good files to provide more accurate verdicts as well as minimize false positives. This analysis looks at thousands of a file's characteristics in a fraction of a second without relying on signatures, scanning, or behavioral analysis. Any new threats the Cortex XDR agent identifies are sent to WildFire for additional analysis, including dynamic analysis, static analysis, machine learning, and bare metal analysis.

1. Konstantin Rychkov and Duncan Brown, "Bridging Security Gaps with Network-to-Endpoint Integration," IDC Research, October 2018, https://www.paloaltonetworks.com/resources/whitepapers/bridging-security-gaps-with-network-to-endpoint-integration.

Malware Analysis

In the case of a never-before-seen file, WildFire performs static analysis to observe the file's behavior and render a verdict of malicious or benign. The file, if still unknown, is further subject to dynamic analysis by our custom hypervisor. Threats attempting to evade analysis are subject to full hardware execution in a bare metal sandbox to detect and prevent even the most evasive malware.

With Cortex XDR and WildFire working together, you get:

- The latest, most up-to-date detection technologies available at scale.
- Automated, proactive protection as well as accurate zero-day detection and prevention delivered in minutes for threats found across tens of thousands of customer networks around the globe.
- Extensibility with virtually unlimited scale to meet the analysis needs of even the largest organizations.
- Automatic distribution of up-to-the-minute threat intelligence, to and from firewalls, clouds, and endpoints, to reprogram prevention and coordinate enforcement.
- Flexibility, with no additional hardware to purchase, deploy, configure, update, or maintain.

As an integral part of the Palo Alto Networks Security Operating Platform®, Cortex XDR continuously exchanges threat intelligence with WildFire. This two-way communication, which enables Cortex XDR to use intelligence from WildFire to automatically block newly identified malware, turns all your endpoints into a network of sensors and enforcement points that can strengthen security across your entire environment. Additionally, endpoint logs stored in Cortex™ Data Lake are combined with logs from other sensors, enabling behavioral analytics across your infrastructure, and allowing other Palo Alto Networks products—such as AutoFocus™ contextual threat intelligence service and Panorama™ network security management—to aid in incident response.

2. Prevent Ransomware

Although ransomware is not new, major attacks like WannaCry, Petya/NotPetya, and TrickBot have shown that traditional prevention methods are ineffective against advanced ransomware. Attackers have evolved their approach and use of malware to become more sophisticated, automated, targeted, and highly evasive.

WannaCry: Combining Malware and Exploits

When WannaCry first hit in May 2017, it was so effective that coverage of breaches attributed to it still appears in the news today. It remains effective due to a combination of malware and exploits. First, it exploits a vulnerability in the Microsoft Server Message Block protocol to gain kernel-level privileges through the use of a kernel asynchronous procedure call (APC) attack. Kernel APC attacks use kernel privileges to carry out their objectives—making legitimate programs execute malicious code, in this case.

From the end user's point of view, ransomware like WannaCry locks up the screen on the endpoint, making it impossible to see other activities the ransomware is carrying out. At the same time, the malware spreads east-west, infecting as many vulnerable machines as it can, both internally and externally.

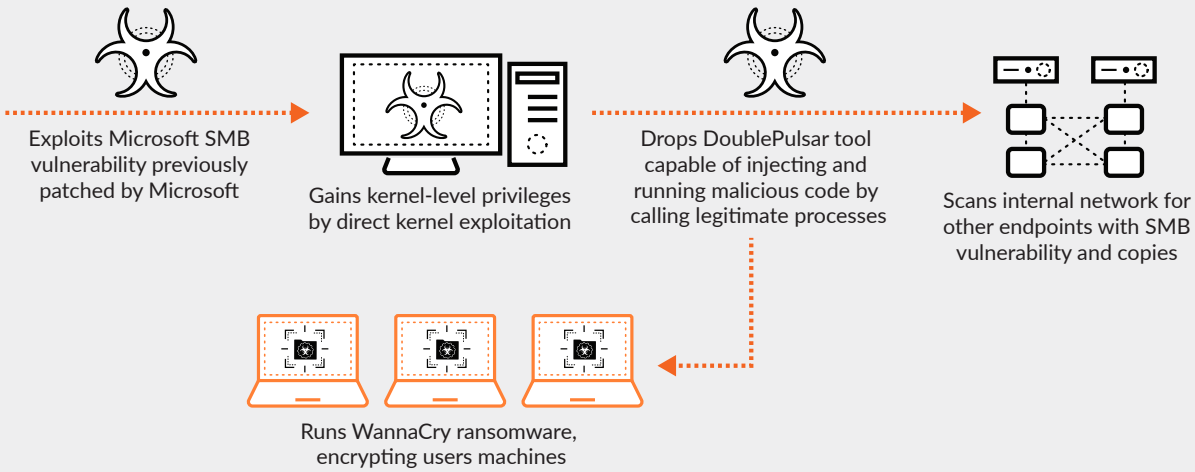

Figure 2: Simplified WannaCry attack sequence

The Cortex XDR agent combines multiple methods of prevention against known and unknown malware, ransomware, and exploits to stop the execution of malicious programs before an endpoint can be compromised. With protection at critical stages of the attack lifecycle, the Cortex XDR agent can prevent successful ransomware attacks regardless of operating system and whether an endpoint is online or offline, connected to the corporate network or not.

Leading up to the WannaCry outbreak, endpoints protected by the agent detected and shut down the ransomware in multiple stages of the attack lifecycle. First, the agent would have detected the exploit technique attempting to escalate kernel privileges to the user level, and shut down the attack. If that had failed, the malicious process protection module would have detected the parent process and stopped it from spawning a child process. If previous modules had not detected the threats, the agent would have detected and stopped the attack by identifying it as a known threat through one of multiple means, including local analysis, the ransomware protection module, or detailed WildFire analysis.

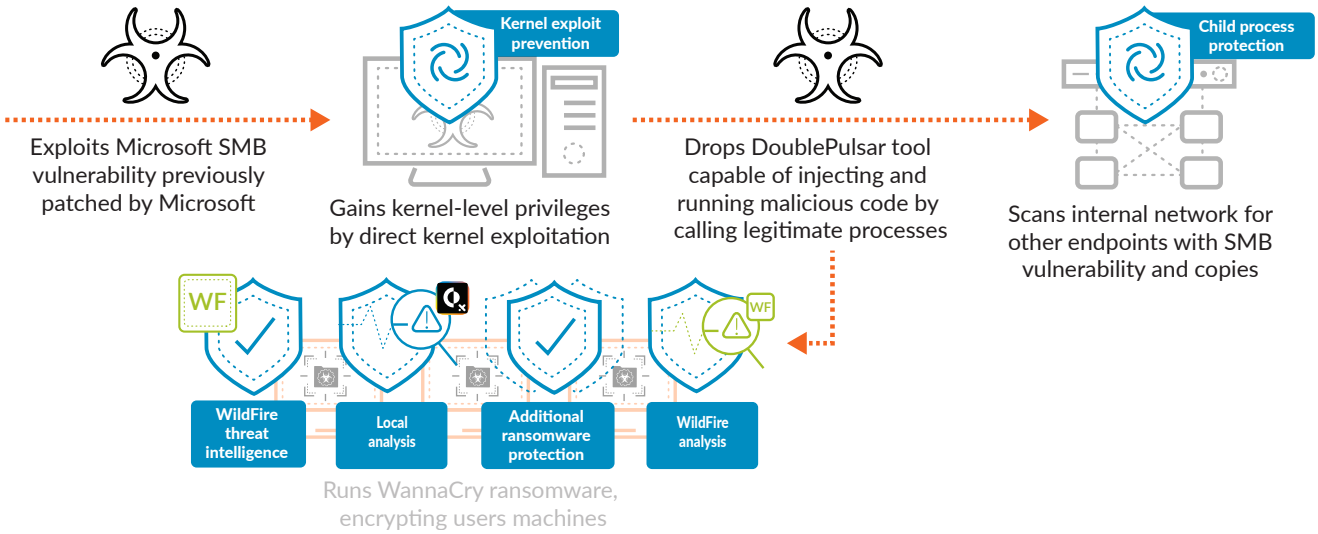

Figure 3: Cortex XDR vs. WannaCry

During and after the outbreak, no known Palo Alto Networks customer networks were infected by WannaCry as the threat had been submitted to WildFire almost a month before the May 12, 2017, attack on the UK's National Health Service. According to AutoFocus data, WannaCry was first discovered on April 16, 2017, at which time protections were created and distributed to all Palo Alto Networks devices and services.

To finish the job, an attacker must succeed at every stage of the attack lifecycle. Cortex XDR only has to succeed in one stage to shut down the attack.

3. Hit Pause on "Patch Tuesday"

Thousands of new software vulnerabilities and exploits are discovered each year, requiring diligent software patch distribution by software vendors on top of patch management by system and security administrators in every organization. This regular flow of patches and updates often lands on "Patch Tuesday," the monthly or semimonthly day when Microsoft releases security patches for its software.

Patching is a critical part of a sound endpoint protection strategy. However, patch management only protects an organization's endpoints after vulnerabilities are discovered and patched. Delays of days, weeks, or longer are inevitable as patches for newly discovered vulnerabilities must be developed, distributed, tested, and deployed. Although patch management is an important aspect of any information security program, much like signature-based malware detection, it is an endless race against time that offers no protection against zero-day exploits. Vulnerability exploits, however, constitute the primary reason patches are applied.

A great deal of attention has been paid to malware since the earliest days of computing, and although malware prevention is critical to endpoint protection, it is only one part of a comprehensive endpoint security strategy. Exploit prevention is equally important but less understood.

Understanding Exploit Techniques

Many advanced threats work by placing malicious code in seemingly innocuous data files. When these files are opened, the malicious code leverages unpatched vulnerabilities in the native application used to view the file, and the code executes. Because the application being exploited is allowed by IT security policy, this type of attack bypasses application whitelisting controls.

Although there are many thousands of exploits, they all rely on a small set of core techniques that change infrequently. Regardless of the exploit or its complexity, for an attack to succeed, the attacker must execute a series of these core exploit techniques in sequence, like navigating a maze to reach the goal.

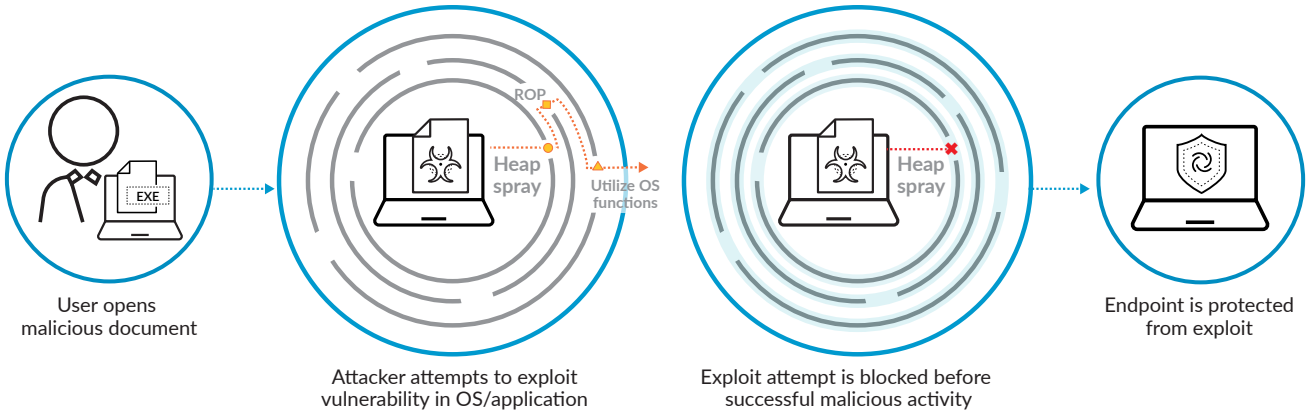

Figure 4: Focus on exploit techniques, not exploits themselves

The Cortex XDR agent focuses on the core techniques all exploits use and, by rendering those techniques ineffective, negates application vulnerabilities whether they are patched or not.

Naturally, it's still best to keep up with the latest security patches. However, Cortex XDR gives you the option to hit "pause" on Patch Tuesday, confident that Cortex XDR will continue protecting vulnerable applications. The Cortex XDR agent injects itself into individual processes as they start up. If a process attempts to execute any core attack technique, the corresponding exploit prevention module (EPM) prevents that exploit, kills the process, and reports details to the cloud-based Cortex XDR console.

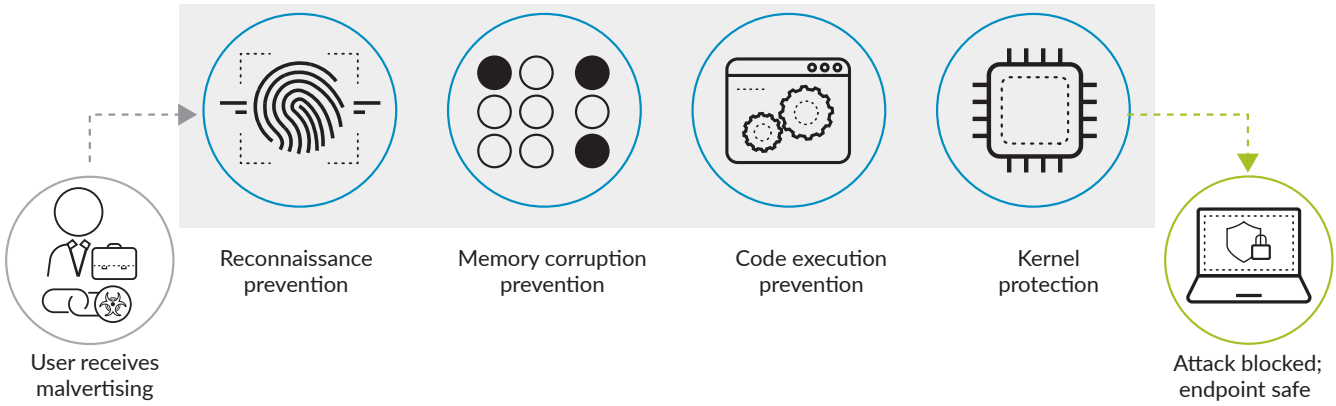

Figure 5: Multiple methods of exploit prevention

By default, Cortex XDR policies are configured to protect more than 100 processes, each with dozens of proprietary EPMs. Beyond the defaults, you can protect all manner of processes and applications by simply adding them to the policy configuration. Processes that have run on the endpoint automatically show up in the management console, making it easy to protect them with the click of a button. This is especially useful for organizations running industry-specific applications, such as point-of-sale systems, ATMs, and SCADA systems.

A prevention-based endpoint protection strategy intercepts and blocks attacks before malicious activity occurs on endpoints. This means preventing an exploit from running or preventing malware from being executed. Such a proactive approach proves an ounce of prevention is worth a pound of cure.

4. Protect Resource-Sensitive Environments

Virtual endpoints and servers, whether in virtual desktop infrastructure (VDI) environments or cloud workloads, encounter the same security challenges as their physical counterparts. This has led to a slew of new challenges for the professionals tasked with securing them.

The frequent antivirus signature updates, application patches, and operating system updates required to secure endpoints against known vulnerabilities are particularly challenging in virtual environments, where "golden images" are used to provision virtual endpoints. Many traditional physical endpoint products can create unforeseen complications when applied to virtual environments. Furthermore, purpose-built virtual security products often leave gaps in the overall security architecture if they are not part of a cohesive security infrastructure.

A new approach is needed to protect virtual and cloud environments from the ground up—one that offers continuous protection without the need for signatures, patches, or updates; integrates seamlessly into any virtual environment; and is part of an end-to-end security platform that encompasses physical, virtual, and cloud-based computing environments.

No Patching or Signature Updates Required

To secure VDI and cloud workloads against known vulnerabilities, traditional security procedures require the most recent antivirus signatures, application patches, and operating system updates after the initial boot from a golden image. This presents several technical and operational challenges.

For instance, the required updates increase network traffic, straining available bandwidth and system resources. Where immediate updates are not performed, administrators must schedule updates during off-peak hours, which is often challenging in organizations with 24/7 uptime requirements. After the initial boot up from a golden image, these endpoints and workloads remain vulnerable until all necessary security updates have been completed.

The Cortex XDR agent prevents known and unknown exploits, as well as malicious executable files that target operating system and application vulnerabilities, without the need for signatures, patches, or updates. It protects endpoints and servers—physical, virtual, or in the cloud—from the moment they become available, removing the need to urgently patch the golden image or live systems.

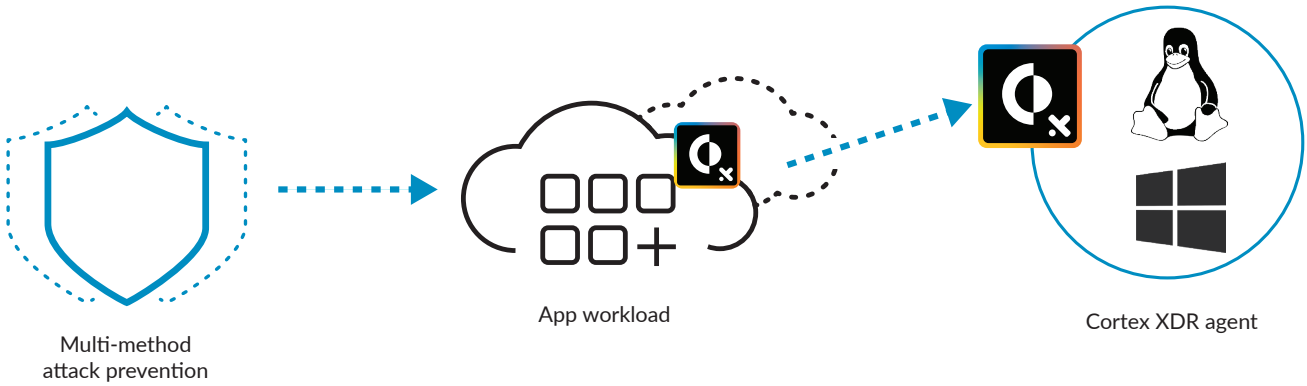

Figure 6: Cloud workload protection

Traditional security products, ill-suited for deployment in VDI and cloud environments, often create unforeseen technical and operational challenges. Presenting a new approach that eliminates many of these, Cortex XDR:

- Does not use signatures or require system patches or updates
- Protects VDI endpoints and servers from the moment they are initialized
- Features license elasticity and scalability, built into its architecture
- Performs no system scans and thus does not affect shared storage or end-user productivity
- Is fully integrated with the Security Operating Platform

Optimized for Virtual and Cloud Environments

Deploying security built for physical endpoints to protect virtual environments often introduces logistical and architectural challenges, such as requiring organizations to develop mechanisms to track and apply software and licenses as virtual instances are spun up or down.

Security must be able scale to accommodate thousands of simultaneous virtual sessions. In VDI environments where storage is shared among virtual sessions, organizations must mitigate the performance impact of system scans that are often at the core of "detective" security measures.

The Cortex XDR agent is designed to work seamlessly in these environments, with license elasticity and the ability to scale to tens of thousands of endpoints built into its architecture.

5. Protect Endpoints from Day One

Deploying and managing endpoint protection shouldn't be difficult. However, customers of traditional endpoint protection products complain about day-to-day management, database maintenance, agent updates, and constant tuning to eliminate false positives and keep resource utilization in check. Worst, even with all this work, endpoints still get compromised.

A customer who was evaluating Cortex XDR put the agents into "listen mode" to see if it would catch anything the customer's existing endpoint protection product could not. Within minutes of deploying agents, a domain controller lit up the Cortex XDR management console with alerts. When the incident response team pulled up the console, they immediately identified a piece of targeted malware that had been running on that server for some time. This was an eye-opener, and the customer immediately realized the simplicity and power Cortex XDR offers, even from day one.

Cortex XDR Agent Deployment

As new malware variants pop up around the globe, and as new software bugs and vulnerabilities are discovered, it can be challenging to ensure your endpoints remain secure. With the cloud-based Cortex XDR management console, you save the time and cost of building out your own global endpoint security infrastructure. Its simplified deployment requires no server licenses, databases, or other infrastructure to get started, enabling you to start protecting your endpoints from day one.

Cortex XDR security infrastructure is deployed in multiple locations around the world to manage endpoint security policies, ensuring the service is secure, resilient, up to date, and available when you need it. This allows you to focus on defining the policies to meet your corporate usage guidelines instead of deploying and managing the infrastructure.

Cortex XDR comprises the following components:

- **The Cortex XDR management console** is a cloud-based service designed to minimize the operational challenges of protecting your endpoints. From Cortex XDR, you can manage your endpoint security policies, review security events as they occur, and perform additional analysis of associated logs.
- **The Cortex XDR agent** protects each local or remote endpoint. The agent enforces your security policy on endpoints and reports when it detects a threat. Agents communicate securely with Cortex XDR using Transport Layer Security (TLS) 1.2.
- **Cortex Data Lake** is a cloud-based logging service that allows you to centralize the collection and storage of Cortex XDR agent logs, regardless of location. Cortex XDR agents forward all logs to Cortex Data Lake in addition to performing their own local analysis. You can view these logs in Cortex XDR, and with the Log Forwarding app, you can forward logs to an external syslog receiver.

Integrated with Cortex XDR, WildFire® malware prevention service identifies previously unknown malware and generates signatures that Palo Alto Networks Next-Generation Firewalls and Cortex XDR can use to detect and block the malware. When a Cortex XDR agent detects an unknown sample, Cortex XDR can automatically forward it to WildFire for analysis. Based on the properties, behaviors, and activities the sample displays when analyzed and executed in the WildFire sandbox, WildFire delivers a verdict: benign, grayware, phishing, or malicious. WildFire then generates signatures to recognize any newly discovered malware and makes the signatures globally available in as few as five minutes.

Cortex XDR Security Profiles for Endpoints

Out of the box, Cortex XDR provides default security profiles for each type of platform, which you can use to begin protecting your endpoints from threats immediately. Although security rules enable you to block or allow execution of files on your endpoints, security profiles help you customize and reuse settings across different groups of endpoints. When the Cortex XDR agent detects a behavior that matches a rule defined in your security policy, it applies the security profile attached to the rule for further inspection. You can enjoy immediate protection with multiple security profiles:

- **Exploit profiles** block attempts to exploit system flaws in browsers and operating systems. These help protect against exploit kits, illegal code execution, and other attempts to exploit process and system vulnerabilities.
- **Malware profiles** protect against the execution of malware, including Trojans, viruses, worms, and grayware. Malware profiles serve to define how to treat behavior common with malware, such as ransomware or script-based attacks, and how to treat known malware and unknown files.
- **Restrictions profiles** limit where executable files can run on an endpoint. For example, you can restrict files from running from removable media or specific, local folders.
- **Agent settings profiles** let you customize settings that apply to the Cortex XDR application, such as the disk space quota for log retention. For Mac® and Windows® platforms, you can also customize user interface options for Cortex XDR, such as accessibility and notifications.

Conclusion

Security built solely to protect virtual endpoints often lacks the broader contextual intelligence critical to an effective enterprise security architecture. Integrated threat intelligence, including data on the tactics, techniques, and procedures of new and previously seen cyberattacks, is often critical to successfully defend systems and networks.

As an integral part of the Palo Alto Networks Security Operating Platform, Cortex XDR prevents cyberattacks automatically and in real time, regardless of the nature of the endpoints and systems you have deployed. In concert with WildFire, the Cortex XDR agent and the entire suite of Palo Alto Networks products benefit from increased contextual visibility into—and protection against—correlated threat actors and campaigns, wherever they may try to attack.

Customers depend on Cortex XDR to ensure endpoints are protected, whether online or off, on-site or remote. IT teams must be able to confidently apply policies that control access to critical resources, and you need confidence in the integrity and configuration of the devices being used to connect to your network, whenever and wherever that may be. Protection cannot depend on full-time network access—it should just work, out of the box, from day one.

For more information about Cortex XDR, please visit paloaltonetworks.com/cortex/cortex-xdr.

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

top-five-requirements-for-effective-endpoint-protection-wp-010920