CyberArk Secrets Manager and Palo Alto Networks Cortex XDR

Securely Investigate Attacks

Highlights

Together, Palo Alto Networks and CyberArk enable you to:

- Leverage policy-based privileged account management to secure endpoints.
- Collect detailed endpoint data from unmanaged endpoints to simplify investigations.
- Implement strong authentication when interrogating endpoints for malicious processes.
- Meet audit and compliance requirements by securely managing privileged credentials used by applications.

Palo Alto Networks Products

- Cortex XDR
  - » Cortex XDR Pathfinder

CyberArk Product

- Secrets Manager

Despite multiple layers of security and the best efforts of IT security teams, motivated attackers can still infiltrate networks in a variety of ways. Once attackers gain a foothold inside a network, they often go undetected for months—ample time to conduct reconnaissance before stealing valuable data or disrupting operations.

Palo Alto Networks and CyberArk have collaborated to deliver secure access for endpoints to help analysts quickly investigate and contain attacks. By integrating with CyberArk Secrets Manager, Cortex XDR Pathfinder can use policy-based privileged access management controls when authenticating to endpoint devices and collect comprehensive endpoint data. Together, Palo Alto Networks Cortex XDR and CyberArk Secrets Manager can uncover advanced cyberattacks in real time and prevent them from wreaking havoc on your network.

Root Out Active Attackers and Malware with Cortex XDR and CyberArk Secrets Manager

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. It safeguards your entire organization holistically while simplifying security operations.

Cortex XDR lets you find dangerous network threats—such as active attackers, malware, and rogue insiders—that have bypassed traditional security controls. Cortex XDR learns the expected behavior of users and devices to detect anomalies indicative of attack. Alerts provide rich investigative data with rich user, endpoint, and network context, enabling swift triage and resolution.

CyberArk is the global leader in privileged access management that focuses on protecting data, infrastructure, and assets across cloud and hybrid environments and throughout the DevOps pipeline. CyberArk is trusted to reduce risk introduced by privileged credentials and secrets used by human and nonhuman users alike. CyberArk Secrets Manager protects critical assets and applications by eliminating hard-coded credentials from application scripts, configuration files, and software code. It also automates the management and rotation of application credentials to reduce the operational resources required to secure critical business applications.

Cortex XDR integrates with CyberArk Secrets Manager to securely access and gather data from endpoints to identify malware, riskware, and unwanted processes. When Cortex XDR Pathfinder needs to deploy an agentless data collector on suspicious endpoints, it first needs to supply a valid credential. Through the integration, the CyberArk Secrets Manager authenticates Cortex XDR Pathfinder based on application characteristics, and Cortex XDR Pathfinder then automatically obtains the necessary credentials via CyberArk Secrets Manager to securely log in to the endpoint or server in question.

This enables you to:

- Get endpoint context after observing anomalous activity by deploying a dissolvable data collector.
- Gather comprehensive data for two weeks to identify the telltale signs of malware or advanced threats.

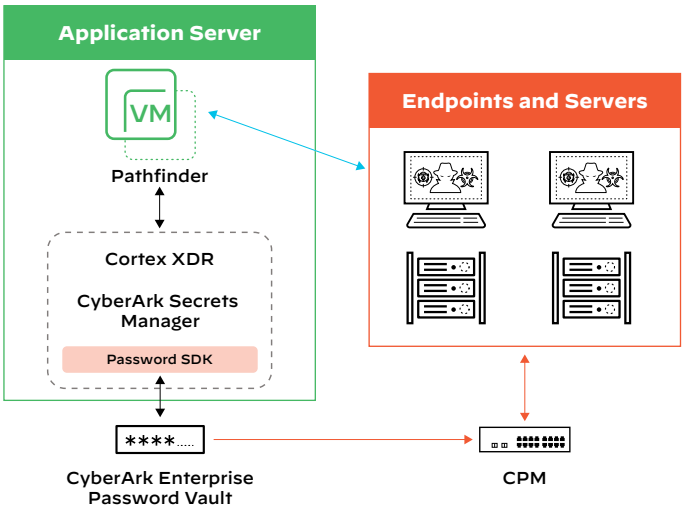

Figure 1: Cortex XDR and CyberArk Secrets Manager integration

Monitor Suspicious Endpoints with "Agentless" EDR

For many SOC teams, investigating security alerts requires painstaking analysis as well as hands-on access to compromised endpoints. Data gathered by an endpoint detection and response (EDR) agent can expedite this process, but it is not always possible to install a persistent agent on all endpoints.

Cortex XDR Pathfinder provides the visibility your analysts need to quickly verify threats and observe endpoint activity to determine the scope of an attack without requiring an agent. It offers insights into unmanaged hosts that let you quickly pinpoint active threats. When Cortex XDR identifies an unmanaged endpoint displaying anomalous behavior, it automatically deploys a data collector to gather detailed endpoint data from the endpoint for up to two weeks. Your team can query and investigate the EDR data gathered by the collector.

Cortex XDR Pathfinder accelerates incident analysis by automatically identifying the source executable on an endpoint that was responsible for anomalous network behavior. It can forward the executable to Palo Alto Networks WildFire malware prevention service to identify malware. Based on this information, your analysts gain context on alerts, enabling them to quickly remediate in-progress attacks.

The Cortex XDR Pathfinder service must gain access to managed endpoints before it can deploy the data collector. This is where the CyberArk Secrets Manager comes into play. Each broker VM with Cortex XDR Pathfinder includes a locally installed CyberArk Secrets Manager agent to cache the credential and ensure that the broker VM will always have secure access to the required credentials for interrogations, independent of network availability or performance. As a result, Palo Alto Networks customers do not need to manage endpoint credentials from within Cortex XDR Pathfinder.

Conclusion

Together, Cortex XDR and the CyberArk Secrets Manager, part of the CyberArk Privileged Access Security Solution, allow organizations to use policy-based privileged access management controls to extend detection and response to unmanaged endpoints.

The CyberArk Secrets Manager provides secure, on-demand credentials to the Cortex XDR Pathfinder service. The joint solution provides shared customers with a lightweight, secure, credential-protected endpoint data collection service that offers additional context for network security alerts, records endpoint activity for investigations, and streamlines forensic analysis.

The joint Palo Alto Networks and CyberArk solution enables you to:

- Verify threats and ease investigations by collecting detailed endpoint activity from unmanaged devices.
- Accelerate threat hunting by automatically determining which endpoint processes and users initiated network attacks.
- Secure and manage privileged credentials used by Cortex XDR Pathfinder.
- Satisfy regulatory authentication policy requirements by monitoring privileged access and securely controlling privileged accounts used by the Palo Alto Networks solution.

About CyberArk

Centered on intelligent privilege controls, the CyberArk Identity Security Platform seamlessly secures human and machine identities accessing workloads from hybrid to multi-cloud, and flexibly automates the identity lifecycle—all with continuous threat detection and prevention to enable Zero Trust and enforce least privilege.

The platform is based on a set of foundational shared services, including AI-powered Identity Security Intelligence, that delivers a unified user experience through a single admin portal and enhances value with robust automation and analytics. Through our vast partner network and out-of-the-box integrations, CyberArk supports each organization along every step of their Identity Security journey, while helping them maximize existing security investments.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice. For more information, visit www.paloaltonetworks.com.

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