Trellix · CYBERARK® SOLUTION BRIEF

Protect Privileged Access Activity from Compromise

CyberArk Privileged Access Management and Trellix XDR

Overview

Highlights

The Trellix and CyberArk integrated solution:

- Provides unequaled privileged access management using a shared technology platform.
- Shares privileged account event data and user activities.
- Applies the most current security intelligence to the monitored events and threat indicators.
- Quickly generates detailed threat alerts for immediate investigation by the customer's incident response team.
- Enables vigilance until the threat is resolved.

Many of the top global firms in cyber threat detection and investigations have identified a common link in today's most dangerous, targeted attacks and information security breaches: the exploitation of privileged accounts, credentials and secrets.

Privileged accounts represent one of the largest security vulnerabilities an organization faces today. These accounts grant extensive control over and access to sensitive data and IT systems, and they are used in nearly every cyber-attack. They allow anyone who gains possession of them to control organizational resources, disable security systems, and access vast amounts of sensitive data. Organizations that protect these accounts and the critical resources they provide access to need comprehensive controls in place to protect, monitor, detect and respond to all privileged account activity.

Unique challenges emerge in cloud environments where new, powerful credentials are instantly created to provision, configure, and manage thousands of machines from a single console. New machines, created with a single click, instantly produce new, unmanaged privileged accounts. In this dynamic environment, it is a requirement that organizations detect changes and monitor all activity for maximum privileged access management and efficient compliance audits.

The Challenge

The challenge is not only to protect privileged accounts from unauthorized access and use, but also to identify when compromises occur and prevent the serious consequences that are likely to result. Attackers steal credentials so they can take control while posing as authorized privileged account holders and take the following actions:

- Bypass security controls and monitoring processes set up to prevent security breaches.
- Access all of the data on compromised devices and leverage that access to exfiltrate data from selected targets or potentially the entire network.
- Disrupt operation of the compromised device to sabotage normal functionality.
- Cause physical damage to the compromised device or other parts of the network.

Trellix Product and Version

XDR 1.x and later versions are supported.

Trellix Product and Version

Privileged Access Management Version

7.x and later versions are supported

The Integrated Solution

The critical nature of privileged credentials and the potentially devastating consequences of a breach of privileged accounts dictate that organizations deploy multiple levels of security as part of a core security strategy. This implementation can best be achieved by deploying the Trellix XDR with CyberArk Privileged Access Management, a leading solution for securing privileged accounts. The joint integration between Trellix XDR and CyberArk PAM can provide the latest intelligence on the dynamic, ever-evolving, and extremely adaptable threat actors and their most current activities and behaviors. The correlation of event data from CyberArk with the threat indicators provided by Trellix XDR allows identification of otherwise normal- appearing activities as a privileged account compromise or potentially malicious behavior that poses a threat to privileged account integrity.

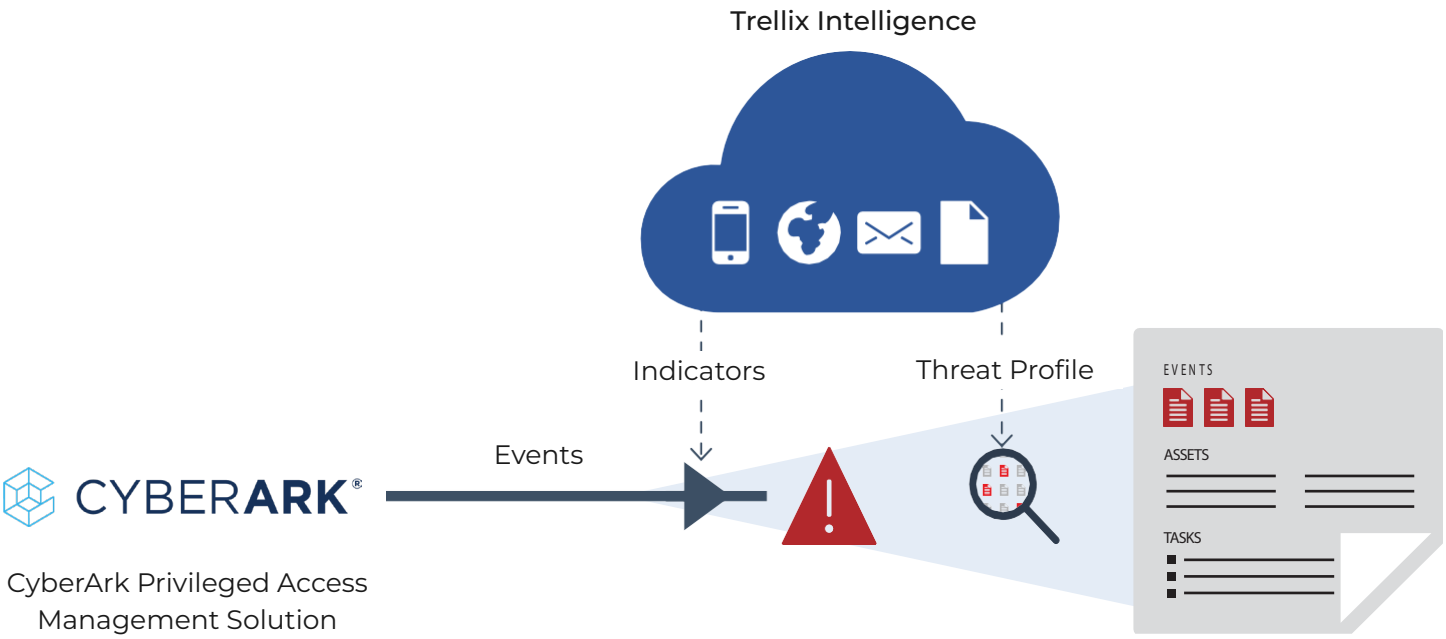
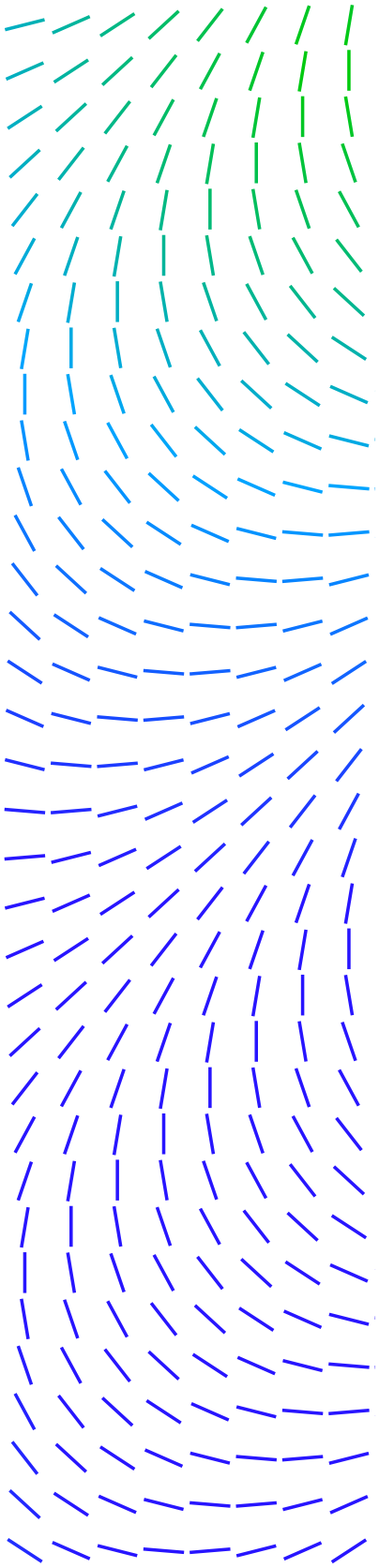


Figure 1. Trellix and CyberArk joint solution.



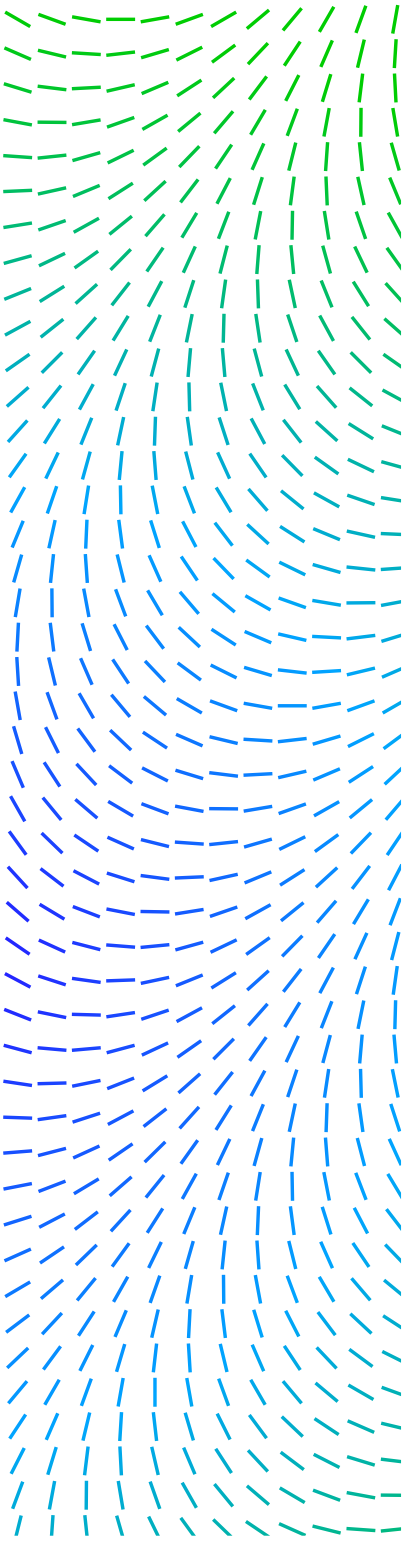
How The Joint Solution Works Together

The integration of Trellix XDR and CyberArk PAM solutions helps achieve the dual goals of securing and protecting privileged accounts and preventing or minimizing damage if any of the privileged accounts is compromised. This assimilation is achieved by enabling Trellix XDR to monitor all events related to the CyberArk solution and correlate the events using Trellix threat intelligence to identify potentially malicious behaviors that are outside of normal account and user activities. If privileged activity is matched to potential threat indicators, an alert is generated to the customer's incident response team. Trellix alerts compile the incident data into a threat profile that equips the customer's incident responder and incident handler with enough specific information about the incident. This recognizance allows them to pinpoint the malicious activities in the CyberArk PAM solution, identify the potential compromise, and resolve the compromise or mitigate the impact. Trellix XDR enables the customer's incident response team to monitor the incident to resolution.

The Value of This Partnership

The intelligence behind this combined solution enables the protection of privileged accounts from various attacks. The solution:

- Continuously monitors privileged account and service account access, usage and activity in real time.
- Proactively detects threats through correlation and analysis of all privileged account user or application activity.
- Identifies and generates alerts of anomalous behaviors that indicate malicious activity.
- Provides detailed privileged account forensics data for incident investigators.
- Detects and monitors anomalous privileged account activity in real time and terminates the session if required in order to disrupt the potential attack.
- Isolates, controls and manages privileged user access across the enterprise.
- Secures and rotates privileged credentials (passwords and SSH keys) in accordance with policy.
- Continuously monitors and controls the commands that the superusers run based on their role and task.



About Cyberark

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

Trellix

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.

122023-15