SOLUTION BRIEF

Limiting Threats That Take Advantage of Endpoint Privileges

Endpoint threat correlation and analysis from CyberArk and FireEye

INTEGRATED SOLUTION HIGHLIGHTS

- Correlates malware alerts from FireEye Helix and FireEye Malware Analysis with visibility into server/endpoint data supplied by CyberArk Endpoint Privilege Manager.
- Provides unique information related to the behavior of executables on the endpoint and a timeline of events that facilitates analysis with FireEye Helix.
- Further leverages customer investments in FireEye technology by extending security mechanisms to endpoints.
- Provides more protection that reduces the footprint should a breach occur.
- Saves time and resources by flagging malicious files that need blocking on all servers/endpoints.

Overview

In an ever changing IT security landscape, organizations are faced with the challenge of reaching a balanced approach to security investments. Analysts suggest that over the next several years there will be a large move toward monitoring, detection, and response and away from the more traditional blocking and prevention techniques. Enterprises are beginning to understand that they are under continuous attack, and there is a need for a continuous response to decrease dwell time.

Researchers suggest that security teams deploy context-aware networks, endpoints, and application security protection platforms from vendors that provide and integrate prediction, prevention, detection and response capabilities.

With this in mind, FireEye and CyberArk integrated their solutions to create an adaptive protection architecture through direct, real-time collaboration.

The challenge

Unnecessary local admin privileges on endpoints play a part of every major cyber attack as bad actors seek to gain access to endpoints and systems within an organization by exploiting administrator privileges. The challenge for IT professionals is to remove these local administrative privileges from business users without impacting network performance and end-user productivity. Additionally, existing threat protection applications are hampered by the lack of information sharing among these applications.

The integrated solution

The joint integration is designed to correlate suspect applications on endpoints with network-based indicators of compromise to detect attacks aimed at exploiting excess privileges rights. The in-depth forensic information provided helps to accelerate incident response and remediation. It also deepens the threat investigation reach for FireEye administrators as they can utilize CyberArk Endpoint Privilege Manager's endpoint data during investigations.

It offers:

- Continuous server/ endpoint to FireEye Helix collaboration that decreases dwell time and reduces potential damage.
- Enforcement of restricted execution of suspicious applications on servers and endpoints and blocking up malware identified by FireEye Helix.
- Deeper threat investigation due to the ability of FireEye Helix to read the CyberArk Endpoint Privilege Manager's endpoint data. This improves the ability to understand:
  - All computers on which malware is present.
  - Who, when and from where the application or file was introduced.
  - The exact actioon performed by the malware. (This can be a video that shows credentials of a specific stolen admin account.)
  - Traces of this application's access to the registry.

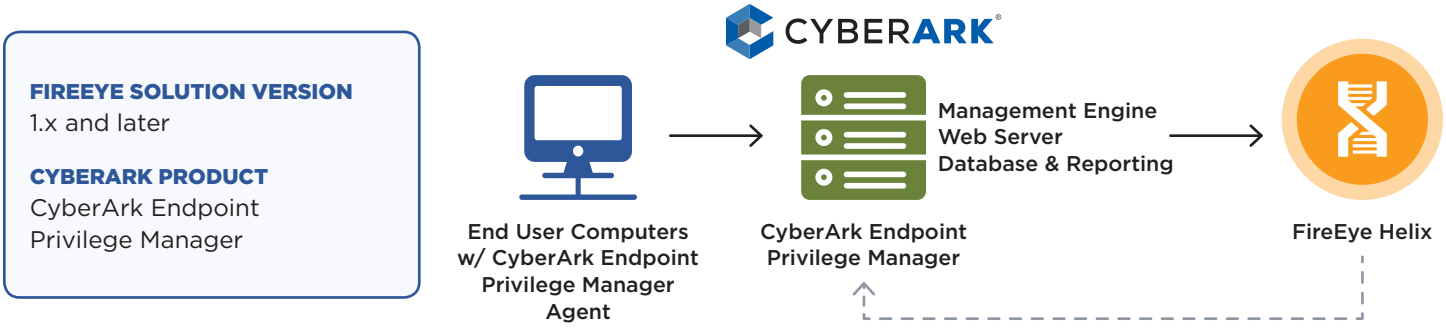

Figure 1. FireEye and CyberArk joint solution.

How the joint solution works

FireEye Malware Analysis and FireEye Helix take advantage of visibility into server/endpoint data supplied by CyberArk Endpoint Privilege Manager.

Step 1: The CyberArk Endpoint Privilege Manager data collector sends suspicious "grey" files/hashes/URLs and file history to FireEye Helix.

Step 2: FireEye Helix sends new malware/APT alerts and cross-references against applications reported as "grey" by CyberArk Endpoint Privilege Manager.

Step 3: CyberArk Endpoint Privilege Manager blocks malware and/or restrictive use policies to suspicious software across all endpoints.

Partnership value

With the joint integration enabled by the FireEye-CyberArk partnership, application and endpoint data are correlated with enterprise-wide security and network threat information. Using FireEye Helix, security teams can view one dashboard with relevant threat data prioritized by threat level. This centralized dashboard allows security teams to quickly identify malicious activity and, with the CyberArk Endpoint Privilege Manager integration, enforce the restricted execution of suspicious applications and block malware identified by FireEye Helix on the endpoint.

This partnership broadens and reinforces application control, endpoint security prevention and network threat protection. Near real-time detection of malicious activity and behavioral indicators lead to expedited incident response and improved attack prevention.

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

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.

For more information contact **CSC@FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

CYBERARK®

FireEye®