FireEye
SECURITY REIMAGINED

FireEye Threat Analytic Platform and FireEye AX Integrated with CyberArk Endpoint Privilege Manager

SOLUTION BRIEF

SECURITY REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- Correlates malware alerts from FireEye AX and FireEye TAP 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 offers data crucial to FireEye TAP analytics.
- 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 and

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 Endpoint Privilege Manager integrated their solutions to create an adaptive protection architecture through direct, real-time collaboration.

CYBERARK

THE CHALLENGE

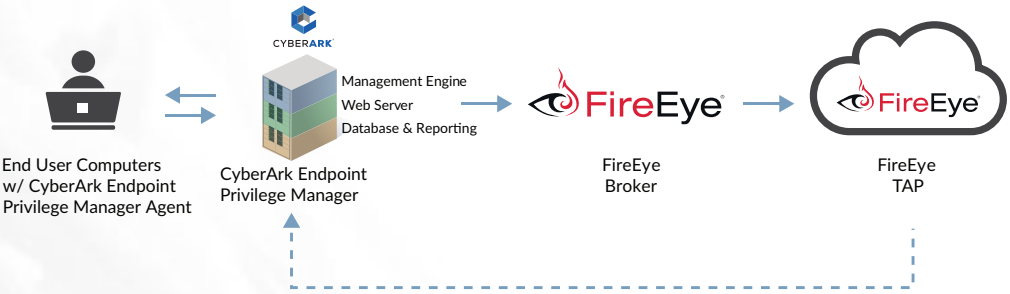
Unnecessary local admin privileges on endpoints play a part of every major cyber attack as bad actors seek to gain access to endpoints and systems within an organization by exploiting administrator privileges. The challenge for IT professionals is to remove these local administrative privileges from 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 TAP collaboration that decreases dwell time and reduces potential damage.
- Enforcement of restrictedexecution of suspicious applications on servers and endpoints and blocking up malware identified by FireEye TAP.
- Deeper threat investigation due to FireEye's ability 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 action 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.



FIREEYE PRODUCT AND VERSION

12.01 and newer

CYBERARK PRODUCT

CyberArk Endpoint Privilege Manager

HOW THE JOINT SOLUTION WORKS TOGETHER

The FireEye integration with Cyberark Endpoint Privilege Manager alerts from FireEye AX and FireEye TAP with visibility into server/endpoint data supplied by CyberArk Endpoint Privilege Manager.

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

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

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

THE VALUE OF THIS PARTNERSHIP

With the joint integration enabled by the FireEye-CyberArk Endpoint Privilege Manager partnership, application, and endpoint data are correlated with enterprise-wide security and network threat information within FireEye TAP and FireEye AX. Using FireEye TAP, 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 FireeEye TAP 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 protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT CYBERARK

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

FireEye