FireEye Threat Analytics Platform (TAP) and CyberArk Privileged Account Security

Protecting Privileged Account Activity from Compromise

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

The FireEye TAP and CyberArk integrated solution:

- Provides unequaled privileged account security 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.

OVERVIEW

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.

Privileged accounts represent one of the largest security vulnerabilities an organization faces today. These accounts grant extensive control over 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 account security 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.

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 FireEye Threat Analytics Platform (TAP) with CyberArk Privileged Account Security (PAS), a leading solution for securing privileged accounts. Utilizing the joint integration between TAP and PAS can provide the latest intelligence on

FIREEYE PRODUCT AND VERSION

Threat Analytics Platform (TAP) 12.01 and later versions are supported

CYBERARK PRODUCT AND VERSION

Privileged Account Security Version 7.0 and later versions are supported

the dynamic, ever-evolving, and extremely adaptable threat actors and their most current activities and behaviors provided by the FireEye TAP solution. The correlation of event data from CyberArk with the threat indicators provided by FireEye allows identification of otherwise normal-appearing activities as a privileged account compromise or potentially malicious behavior that poses a threat to privileged account integrity.

HOW THE JOINT SOLUTION WORKS TOGETHER

The integration of FireEye TAP and CyberArk Solution 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 the FireEye TAP to monitor all events related to CyberArk PAS and correlate the events using FireEye intelligence to identify potentially malicious behaviors that are outside of normal account and user activities. If FireEye matches privileged activity with potential threat indicators, an alert is generated to the customer's incident response team. FireEye 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 Solution, identify the potential compromise, and resolve the compromise or mitigate the impact. Then with FireEye TAP the customer's incident response team monitors the incident to resolution.

THE VALUE OF THIS PARTNERSHIP

The combination of the FireEye TAP solution intelligence and CyberArk's Privileged Account Security solution enable protection of privileged accounts from various attacks. Together they:

- Continuously monitor privileged account and service account access, usage and activity in real-time.
- Proactively detect threats through correlation and analysis of all privileged account user or application activity.
- Identify and generate alerts of anomalous behaviors that indicate malicious activity.
- Provide detailed privileged account forensics data for incident investigators.
- Detect and monitor anomalous privileged account activity in real-time and terminate the session if required in order to disrupt the potential attack.
- Isolate, control, and manage privileged user access across the enterprise.
- Secure and rotate privileged credentials (passwords and SSH keys) in accordance with policy.
- Continuously monitor and control the commands that the super-users run based on their role and task.

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 3,400 customers across 67 countries, including over 250 of the Fortune 500.

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**