CyberArk has partnered with McAfee Enterprise Security Manager to deliver a real-time privileged activity monitoring solution. By combining the CyberArk Privileged Account Security Solution with McAfee Enterprise Security Manager, security analysts and audit teams can now access the information they need to identify and respond to the most critical incidents, those involving privileged accounts, while meeting demanding compliance requirements.

Cyber attackers target privileged accounts in order to reach the heart of the enterprise and gain access to sensitive, valuable data. To protect these accounts and the critical resources they provide access to, organizations require comprehensive controls in place to effectively monitor, detect and respond to all privileged account activity in real time.

CyberArk’s Privileged Account Security Solution integrated with McAfee Enterprise Security Manager enables security teams to monitor and protect privileged activity and gain unified, real-time visibility to identify critical security threats. The solution generates exceptionally detailed tracking and reporting on all privileged activity, meeting audit and compliance requirements.

Centralized Privileged Account Activity Collection and Incident Management

The CyberArk Privileged Account Security Solution is an enterprise-class, unified solution that manages and secures all privileged accounts. It secures credentials, including passwords and SSH keys, controls access to these accounts, isolates and records privileged sessions for auditing and forensics analysis. Built on a single platform, the solution centralizes all privileged activity and provides a single data source into McAfee Enterprise Security Manager.

CyberArk enhances McAfee’s SIEM visibility into privileged account threats by sending all privileged activity as syslog messages in McAfee Common Event Format (CEF). Integrating the CyberArk Solution enables McAfee Enterprise Security Manager to fully monitor and archive all privileged user and account activities. This includes individual user activity when using shared accounts as well as embedded application logins. These alerts are then correlated with other real-time information collected from the organization, and the most critical security threats are identified.
CyberArk Privileged Account Security Solution Integrated with McAfee® Enterprise Security Manager

Real-time Privileged Activity Monitoring and Compliance

By integrating and correlating the log data of privileged account activity into McAfee, security and forensic analysts now have the widest range and depth of actionable information available via a unified dashboard. This rich data enables analysts to gain a real-time view of enterprise-wide threats that originate from privileged account activity, as well as deeper forensics analysis and evidence collection by drilling-down into privileged user sessions.

Capabilities include:

- Link events that are triggered through the use of privileged accounts with the individuals who initiated them; reveal who had access to which systems and data, and when and for what purpose
- Quickly investigate alerts by replaying exactly what transpired with video playback revealing the user's actions
- Review command-level logs that are sent to McAfee Enterprise Security Manager when anomalous activity is detected (e.g. credit card information is being copied); remotely locate and monitor the session in real-time via CyberArk Privileged Session Manager and terminate the session if required in order to disrupt the potential attack
- Monitor changes within the CyberArk Vault by sending activity logs to McAfee Enterprise Security Manager whenever a privileged user accesses the vault to make changes (e.g. creating a new administrator account, etc.)
- Generate compliance reports to show which privileged user accessed an organization's most sensitive assets, modified configuration settings and ran programs on the network

Advanced Behavioral Analysis, Monitoring and Detection Capabilities Using CyberArk Privileged Threat Analytics

The joint CyberArk Privileged Account Security and McAfee Enterprise Security Manager solution is bi-directional, whereby McAfee sends enterprise-wide data privileged account activities directly to CyberArk Privileged Threat Analytics™. This enables CyberArk Privileged Threat Analytics to conduct User Behavior Analysis (UBA) based on a rich set of data, facilitating a joint solution to correlate additional data, reducing false positives and enhancing the overall value of the alerts. When CyberArk Privileged Threat Analytics detects anomalous privileged account activities, the system generates real-time alerts to the McAfee Enterprise Security Manager dashboard allowing security teams to quickly monitor and respond to alerts from a single-pane-of-view.

Conclusion

The integration of the CyberArk Privileged Account Security Solution and McAfee Enterprise Security Manager enables organizations to focus their efforts and resources on the highest priority targets and identify the most significant risks. The joint solution supports a more comprehensive approach to unified visibility with centralized policy-based privileged activity management. Once deployed, the solution effectively arms organizations with the information they need to identify and respond to the most critical incidents and meet demanding compliance requirements.

Joint CyberArk-McAfee Enterprise Security Manager Solution:

- Provides enterprise-wide, real-time visibility to identify and investigate critical security threats associated with privileged activity
- Enables enhanced forensics analysis and evidence collection by drilling-down into privileged user sessions to understand the true nature and scope of the event
- Meets a diverse set of compliance requirements with individual accountability combined with detailed tracking and reporting on all privileged activity
- Improves security with end-to-end privileged activity lifecycle management
- Enables fast and effective incident response using automated controls

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 immeasurable business damage.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security’s mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com. Intel, the Intel logo, McAfee and the McAfee logo are trademarks of Intel Corporation in the U.S. and/or other countries.

1 This is a companion piece to our CyberArk Privileged Threat Analytics™ Integrated with McAfee Enterprise Security Manager Platform solution brief

©CyberArk Software Ltd. | cyberark.com