Privileged Identity Management
Combine McAfee security with privileged user access control and management

Cyber-Ark Software solutions help reduce data breach risks, meet strict IT compliance and audit requirements, and improve security posture and operational efficiencies on corporate networks, whether on premises or in the cloud. Cyber-Ark delivers privileged password vaulting and user-access control, session recording and auditing, continuous monitoring, and forensics. Cyber-Ark solutions are integrated with McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee® Enterprise Security Manager, and McAfee® Vulnerability Manager.

Today's threat landscape has elevated the need to continuously monitor threats related to industrial espionage, cybercrime, and cyberwarfare. Trusted insiders (such as IT administrators) have nearly unlimited access to both mission-critical resources and highly sensitive information entrusted to their care. Too often, accidental (or deliberate) misuse of a shared credential occurs at the beginning of a breach, where the credential is compromised and abused either by insiders, disgruntled employees, or cybercriminals.

Cyber-Ark’s PIM Suite Integration with McAfee ePO Software
When a violation is detected by Cyber-Ark, the integration surfaces alerts and a view of privileged user account activity for critical assets in the McAfee ePO software dashboard, including domains, servers, databases, networking components, and applications across the entire data center. This can be especially useful for highly regulated firms, service providers, and government agencies.

The Cyber-Ark plug-in agent, tested by McAfee and rewarded a “McAfee Compatible” designation, forwards alerts for the utilization of user-defined privileged accounts. Users set policies for alerts to be forwarded to McAfee ePO software dashboards based on the most important IT assets they wish to monitor. This gives SOC personnel a proactive view of which privileged accounts are currently and historically in use and by whom, and facilitates compliance reporting directly from within McAfee ePO software.

Customers of the joint solution often deploy the capability for McAfee ePO software administrators to receive alerts whenever a user attempts to access a critical firewall, server, database, or other critical asset. Real-time notifications are then delivered to specified operational groups via email or SMS text—and if the access is deemed to be improper or anomalous, prompt corrective action can be taken.
Cyber-Ark’s PIM Suite Integration for McAfee Enterprise Security Manager
Privileged Monitoring and Advanced Forensics

This integration enables a dashboard for continuous monitoring of privileged account usage, syslog aggregation and analysis, and audit trail and advanced forensics for privileged account activities. Users can view and monitor privileged sessions in real time and play back privileged session recordings to review keystroke logging. Based on CEF syslog consumption, the integration creates an advanced privileged identity audit trail and forensics capability within McAfee Enterprise Security Manager. It provides a personalized view of which specific services account executed, or which domain user accessed a shared privileged account (for example, root, Cisco Enable, DomainAdmin, and others), when that access occurred, and (optionally) what was done during the access (via command line auditing, AVI recordings, and so on).

A user-defined PIM dashboard may also be created within the McAfee Enterprise Security Manager console to continuously monitor the current state of privileged account access. This creates an improved IT security stance for customers, in which SOC personnel may proactively monitor privileged accounts that are currently in use, and can run important reports, such as the “Top 10 Used.”

Cyber-Ark’s Privileged Session Manager (PSM) recording session IDs are also passed via syslog to McAfee Enterprise Security Manager, allowing SOC personnel to play back privileged sessions either historically or in real time (for example, while the session is still active) and enabling continuous monitoring of both privileged user accounts and web sessions.

Cyber-Ark’s PIM Suite Integration for McAfee Vulnerability Manager

This McAfee Compatible integration enables fully automated, password-protected network scans using the Cyber-Ark Enterprise Password Vault (EPV) as the authoritative authentication store and administrative password credential repository. McAfee Enterprise Security Manager accesses an EPV for secure scan credential storage and automated authentications of vulnerability scanners during runtime. This alternative authentication method utilizes EPV’s existing ultra-secure credential repository and change management facility to fully automate the scanning process, providing an audit trail of all resources touched during the scanning process.

**Benefits of the Joint Solutions**

**McAfee ePO software integration**
- User-defined critical PIM events reported to McAfee ePO software
- McAfee ePO software notification engine for privileged account activity
- PIM audit and compliance entitlement and access reporting directly from McAfee ePO software

**McAfee Vulnerability Management integration**
- Enables fully automated vulnerability scanning and audit trail, authoritative authentication using credentials stored in the Cyber-Ark Enterprise Password Vault (EPV)
- EPV provides automatic password changes without user intervention

**McAfee Enterprise Security Manager integration**
- Native SIEM Integration via SYSLOG
- Dashboard views of privileged activity
- Privileged session recording playback from within the McAfee Enterprise Security Manager console

![Figure 2. Configuration screen for Cyber-Ark PIM's integration with McAfee Enterprise Security Manager.](image)

Cyber-Ark’s PIM Suite is based on a robust, highly available, fault tolerant enterprise architecture that has been proven in the most demanding highly regulated vertical markets. Global enterprise customers include these sectors: banking, brokerage, insurance, retail, energy, healthcare, pharmaceutical, manufacturing, technology, government, and defense.
Figure 3. Cyber-Ark deployment architecture.

About Cyber-Ark Software
Cyber-Ark Software is a global information security company that specializes in protecting and managing privileged users, applications and highly sensitive information to improve compliance, enhance productivity, and protect organizations against insider threats. With its award-winning Privileged Identity Management (PIM) and Highly-Sensitive Information Management software, organizations can more effectively manage and govern application access while demonstrating returns on security investments. [www.cyber-ark.com](http://www.cyber-ark.com).

About McAfee ePolicy Orchestrator Software
McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.