

# Continuous Monitoring of Privileged Users

Cyber-Ark's PIM Suite integration enables a near real-time view of privileged user activity within McAfee® ePolicy Orchestrator® platform dashboards

Cyber-Ark Software, a leader in privileged identity management (PIM) and highly sensitive information management (HSIM), delivers solutions that improve enterprise security posture, drive operational efficiency, and help organizations meet IT compliance and audit requirements.

Cyber-Ark's PIM Suite integration with the McAfee ePolicy Orchestrator (McAfee ePO™) platform provides near real-time alerts and a view of privileged user activity for critical IT assets, including servers, databases, networking components, and applications across the data center, which is particularly useful for highly regulated firms, service providers, and government agencies.

## Controlling Privileged User Access Helps Mitigate Threats Inside and Outside the Firewall

Today's IT regulatory environment, coupled with best practices in information security risk management, creates a need for continuous monitoring of threats related to industrial espionage, cybercrime, and cyberwarfare that can damage both enterprise networks and critical infrastructure, including power plants and telephony grids.

Trusted insiders (such as IT administrators) have nearly unlimited access to both mission-critical resources and the highly sensitive information entrusted to their care. All 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, cyberterrorists, or cybercriminals.

## Continuous Monitoring: Enables Current State Analysis of Privileged Account Usage

The concept of continuous monitoring assumes a proactive model for managing enterprise information security. The Federal Information Security Act (FISMA) of 2002, Office of Management and Budget (OMB) policy, and the implementing standards and guidelines developed by the National Institute of Standards and Technology (NIST) require a continuous monitoring approach. According to NIST, continuous monitoring is defined as "one of six steps in the risk management framework (RMF), described in *NIST Special Publication 800-37, Revision 1, Applying the Risk Management Framework to Federal Information Systems (Feb 2010)*." Continuous monitoring is now mandated across all federal agencies to better thwart cyberwarfare as well as to assist in the American Homeland Security Presidential Directive 12 (HSPD-12) related to critical infrastructure protection (CIP).

Cyber-Ark has developed a McAfee Compatible plug-in that forwards alerts in near real time for use by selected privileged accounts. Users define policies for alerts to be forwarded to the McAfee ePO platform based on the most important IT assets they wish to monitor from within McAfee ePO dashboards.

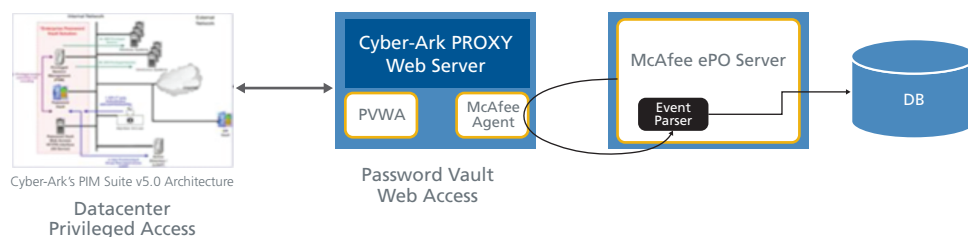


Figure 1. Cyber-Ark and McAfee ePO platform integration diagram.

### McAfee Compatible Solution

Cyber-Ark PIM Suite 6.0  
McAfee ePO 4.0 & 4.5

### Benefits of the joint solution

- Real-time privileged session monitoring
- Critical events reported to the McAfee ePO platform
- Privileged user management
- Auditable credential storage repository
- Automated privileged password changes
- Privileged single sign-on
- Privileged session recording with DVR-like playback
- Audit and compliance entitlement reports
- Tamperproof storage of recordings, and logs
- Workflow automation
- Change control (ticketing) integration
- Identity management integration provisioning, directory services, access certification
- Authoritative personalization for use of powerful, shared IT administrative accounts
- Native security information and event management (SIEM) integration via SYLOG

### Relevant Compliance Regulations & Security Best Practices

- SOX
- PCI DSS
- HIPAA
- FISMA; NIST 800-53a
- FERC/NERC
- CIP
- BASEL-II
- SAS 70
- ISO 9002
- COBIT and ITIL

**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, boost 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 ePolicy Orchestrator 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.

For instance, McAfee ePO platform administrators may wish to be immediately notified whenever access is either attempted or successful on a critical firewall, server, or database. If the access is determined to be anomalous, they can take prompt corrective action to minimize any damage.

**Improved Visibility and Remediation Response Times**

Many data breaches involve the deliberate use or accidental misuse of a privilege account to gain access to mission-critical resources or data. The ability to quickly analyze and remediate privileged access control is, therefore, a key factor for a proactive, as opposed to a reactive, information security posture.

Cyber-Ark integration with the McAfee ePO platform creates real-time visibility and situational awareness of privileged account use anomalies within the McAfee ePO console, enabling security operations personnel to respond to critical events with the right countermeasures.

**“Authoritative” Privileged Audit Trail**

Establishing accountability is an important factor in determining root cause and expediting remediation during any privileged access security incident. Cyber-Ark’s PIM Suite, as the central control point for all privileged administrative access, automatically personalizes privileged session access by creating logs of *which* unique user IDs have used (or have attempted to use) a privileged account, *when* this was done, and, optionally, *what* that user did with the access (via privileged session recording). This unique, native by-product of the Cyber-Ark PIM Suite enables advanced identity analytics.

**Redundant, High-Availability Architecture**

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

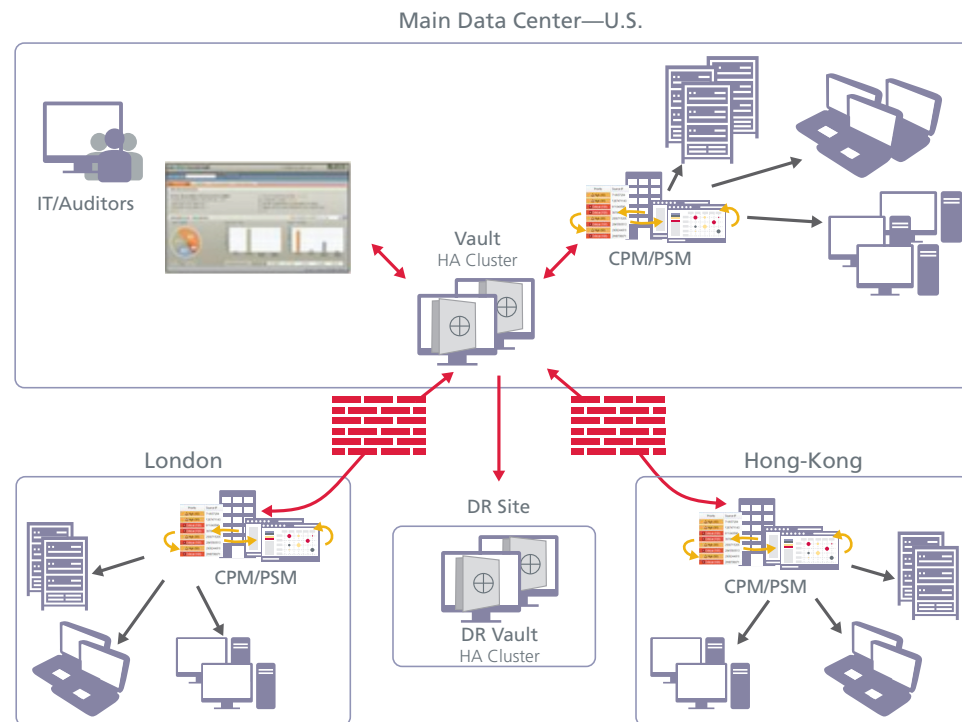


Figure 2. Cyber-Ark PIM Suite, version 6.0 architecture.



McAfee  
 2821 Mission College Boulevard  
 Santa Clara, CA 95054  
 888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee, the McAfee logo, McAfee ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright ©2011 McAfee, Inc. 37703brf\_cyber-ark\_1011\_fnl