SOLUTION BRIEF

Unified Least Privilege, Endpoint Security, and Threat Intelligence

Increase visibility and enhance breach detection capabilities

Through the integration of network security data with multidimensional privileged user and behavioral analysis, your organization can increase visibility and improve your ability to more quickly and accurately detect potentially damaging breaches. The powerful combination of BeyondTrust with McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee Enterprise Security Manager provides visibility into the cause of a data breach by unifying least privilege and endpoint security and by adding real-time privileged session activity and vulnerability intelligence to security event analysis.

McAfee Compatible Solution

- BeyondTrust BeyondInsight 6.0
- BeyondTrust PowerBroker for Windows 7.2
- McAfee ePO version 5.3.2
- McAfee Enterprise Security Manager 9.6 and above

The Business Problem

Data breaches typically occur as a result of misuse or abuse of excessive user privileges in combination with the exploitation of a known system vulnerability. When an affected user is an administrator, the risk is even greater—an external attacker or malicious insider can leverage elevated permissions to move laterally throughout an environment, wreaking untold damage to a company's data and assets.

Normally, IT investigates the source of the breach looking for anomalous behavior, updates endpoint protection, and removes administrator rights so that attacks such as these cannot gain a beachhead on important assets. But this approach often requires multiple tools that don't talk to one another, leading to complexity and wasted time to find and fix the problem. This is fertile ground for potentially more negative consequences to the business.

McAfee and BeyondTrust Joint Solution

BeyondTrust and McAfee collaborate together to:

- Provide a single, lightweight client that integrates with the existing environment to perform the functions of least privilege.
- Enable the removal of administrative rights and credentials without impacting the user's workflow.
- Protect against keystroke loggers and password stealing techniques like Pass-the-Hash using a least-privileged client to perform application elevation.
- Deliver real-time correlation of exposed vulnerabilities—including missing patches and configuration weaknesses—across the entire IT environment for enterprise threat intelligence.
- Enable accurate threat detection by linking meaningful events with conditional logic and current threat analytics to reduce the number of false positives and false negatives.
- Provide a single management platform for auditing, policy, and reporting of privileged events.

How the McAfee and BeyondTrust Joint Solution Works

Integration between McAfee ePO software and BeyondTrust PowerBroker for Windows provides a unified approach to least-privileged access that optimizes the effectiveness of an organization's entire security infrastructure by linking security threats to privileged access based on policy.

Using the PowerBroker Editor, policies are created that target applications approved for elevation and stored within the McAfee ePO software solution. The client-side McAfee agent reads the PowerBroker for Windows policies and delivers these to the BeyondTrust Endpoint Least Privilege client. Events and other auditable data are forwarded to McAfee ePO software for analysis and maintenance of the least privilege solution.

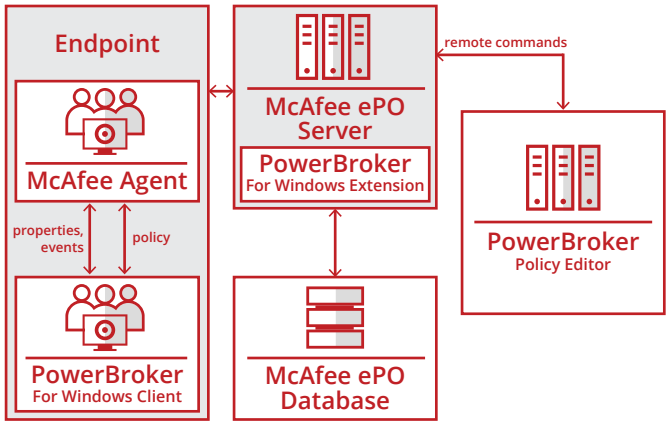

Figure 1. How McAfee ePO software integrates with BeyondTrust PowerBroker for Windows.

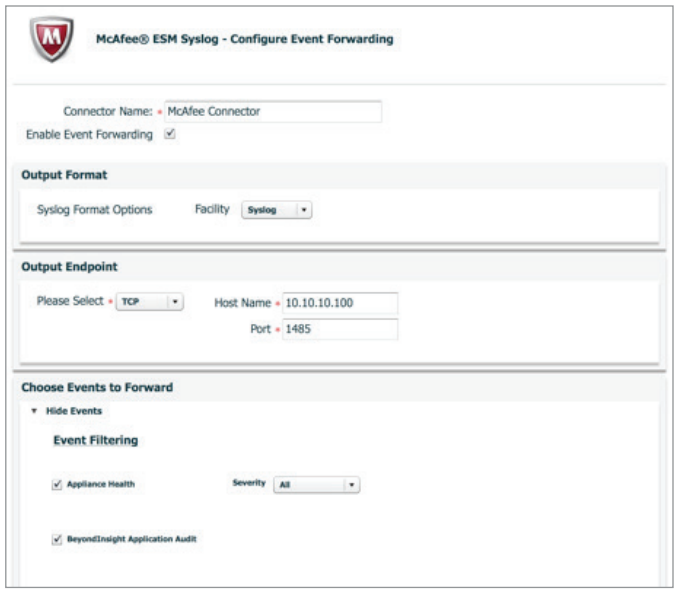

Figure 2. McAfee Enterprise Security Manager integration with the BeyondInsight platform.

McAfee Enterprise Security Manager integration with the BeyondInsight platform provides a single contextual lens for all privilege and vulnerability events generated by BeyondTrust solutions. BeyondInsight has an IT risk management platform for all of BeyondTrust's PowerBroker and Retina solutions that can be configured to forward all events, including advanced threat analytics from the patent-pending BeyondTrust Clarity capability, to McAfee Enterprise Security Manager.

Since PowerBroker for Windows is fully integrated with the BeyondInsight platform, it leverages data gathered on privileged user behavior and correlates it against BeyondTrust and multiple third-party threat data feeds to determine a risk score for applications and assets. This intelligence provides security administrators with the insights they need to reduce the risk of damaging data breaches.

About BeyondTrust

BeyondTrust is a global information security software company that helps organizations prevent cyberattacks and unauthorized data access due to privilege abuse. Our solutions give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And, because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. BeyondTrust's security solutions are trusted by more than 4,000 customers worldwide,

including Fortune 100 companies. To learn more about BeyondTrust, please visit **www.beyondtrust.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

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com