

Endpoint Security for a Mobile Workplace

Aruba ClearPass and McAfee® ePolicy Orchestrator® software integration

Wireless and mobile technologies have enabled laptops and smart devices to be used outside of the enterprise perimeter, creating blind spots for administrators in terms of end-to-end visibility and control. As mobile and cloud computing gain greater traction, safeguarding the enterprise data that traverses in and out of the enterprise has become a major challenge.



McAfee Compatible Solution

- Aruba ClearPass v6.6.2 and above
- McAfee ePolicy Orchestrator v5.3.2 and 5.1.3
- McAfee Enterprise Security Manager v9.6 and above



SOLUTION BRIEF

The Business Problem

Requirements for greater security and compliance is driving customers to:

- Ensure that desktops and laptops meet baseline compliance policies via automated access control to lower the security risk posed by unchecked devices attaching onto enterprise wired and wireless networks
- Understand the profiles and compliance posture of devices attaching to its networks, especially for bring your own device (BYOD), which has increasingly become an acceptable practice within enterprises
- Obtain contextual information, such as user identity and device type, so that security information and event management (SIEM) systems can correlate alerts to automatically identify security events and compress an incident response window

McAfee and HP Aruba Integrated Solution

While enterprises traditionally deploy McAfee ePolicy Orchestrator (McAfee ePO™) software and McAfee Enterprise Security Manager within its enterprise perimeter, the advent of wireless and mobile technologies is now driving the need for an orchestrated approach to safeguarding enterprise data as users can connect from anywhere at any time—inside and outside of perimeter security deployments.

This is where Aruba, a Hewlett Packard Enterprise company, with the Aruba ClearPass solution, provides added value. McAfee is leveraging this network access control (NAC) partner to maximize the efficiency and effectiveness of McAfee ePO software and McAfee

Enterprise Security Manager to meet today's shifting customer requirements.

On the technical front, the integration between McAfee ePO software, McAfee Enterprise Security Manager, and Aruba ClearPass covers two dimensions in the latest advanced security protection paradigm:

- Threat intelligence sharing among vendor applications
- Automatic detection and remediation based on shared intelligence

How It Works

The integration between Aruba ClearPass and McAfee products is bi-directional and allows for the following:

1. As devices connect, ClearPass profiles every device that connects.
2. ClearPass then uses McAfee ePO software to gather device posture information in order to authorize access to the enterprise network or to quarantine a device(s).
3. If a device does not meet posture requirements, the device can be denied access or placed in a quarantine VLAN to allow McAfee ePO software to correct the posture on computers or, in the case of enterprise mobile management (EMM), to remediate mobile endpoints.
4. McAfee Enterprise Security Manager then consumes contextual data sent via syslog and performs additional SIEM analysis to detect security events. It send alerts to the rest of the McAfee security platform for further action.

SOLUTION BRIEF

- In the event that McAfee Enterprise Security Manager does detect a security event, a notification can be sent to Aruba ClearPass to alter the state of the device's connection. A device can be bounced on wireless or wired infrastructure and either be denied access or placed into a quarantine VLAN.
- ClearPass can also be used to generate a help desk ticket and alert a user as to why their device has been disconnected from the network or placed into quarantine.

Solution Reference Architecture Network Access Control with Unified Endpoint Management

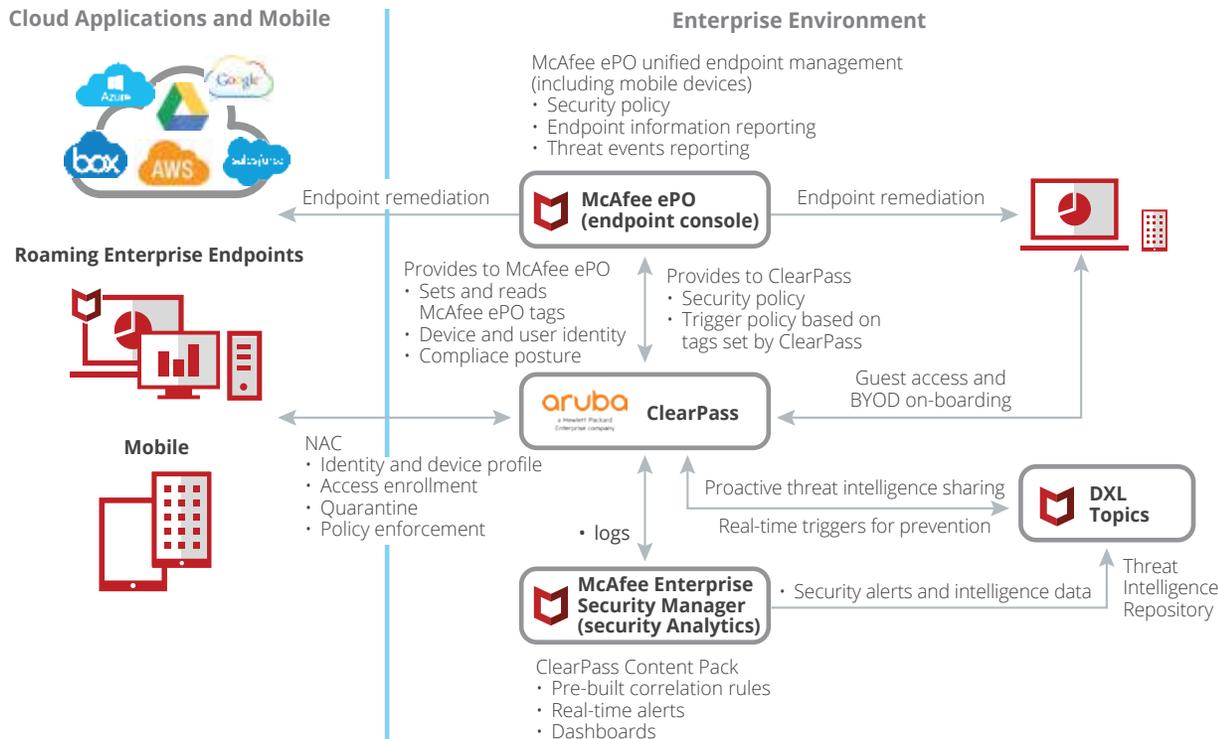


Figure 1. Network access control (NAC) and McAfee ePO software/McAfee Enterprise Security Manager workflow: automated device authorization for any wired or wireless infrastructure.

SOLUTION BRIEF

The end result is an automated workflow that safeguards enterprise resources in real time, regardless of user, device type, location, or time of day. Other components within ClearPass can also be used for guest access, IoT categorization and control, and BYOD onboarding.

About Aruba

Aruba, a Hewlett Packard Enterprise company, is a member of the McAfee Innovation Alliance Partner Program. ClearPass has been certified as McAfee Compatible to securely interoperate with McAfee ePO software and McAfee Enterprise Security Manager.

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.



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

McAfee and the McAfee logo, ePolicy Orchestrator, and McAfee ePO are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 2177_1216
DECEMBER 2016