

Real Time for ePolicy Orchestrator

Technology preview—joint development project

Real Time for ePolicy Orchestrator® (Real Time for McAfee ePO™) sets a new bar for security management by enhancing McAfee ePO software with real-time capabilities. With actionable information about threats, your devices, and your policies, you can remediate issues and improve your security posture in seconds.

When Seconds Count, Real Time for McAfee ePO Delivers

In today's information driven enterprises, time is not on the side of the IT security manager. When complete, expedient knowledge of the IT landscape can mean the difference between risk mitigation and catastrophe, seconds count.

With existing security management toolsets, administrators of complex infrastructures with hundreds of servers and thousands of endpoints cannot afford to wait days or weeks to collect endpoint data, and then days or weeks more to remediate through traditional policy enforcement tools. Real Time for McAfee ePO is the first and only solution that allows enterprises to query assets in seconds, identifying potential issues to mitigate risk in seconds rather than days. This groundbreaking technology dramatically reduces exposure risk and cost of security events, outages, breach potential, and damage to reputation.

A Revolutionary Architecture

Real Time for McAfee ePO is the first security control system that allows you to instantly find any information about any computer, deploy products, or update configurations in the environment in a matter of seconds. In large or complex environments, this is literally hundreds or thousands of times faster than traditional solutions.

Real Time for McAfee ePO delivers:

- Instant information on the state of computing assets in seconds, not hours or days
- Increased protection through policy enforcement to ensure that antivirus, encryption, and other crucial services are always installed, running and up to date

- Cross-referenced threat information via a large, continuously monitored peer-to-peer network
- Instant enhancement to antivirus, data loss protection, host-based intrusion protection, whitelisting, web filtering, firewall, encryption, and other security products by increasing scalability and reducing management timeframes

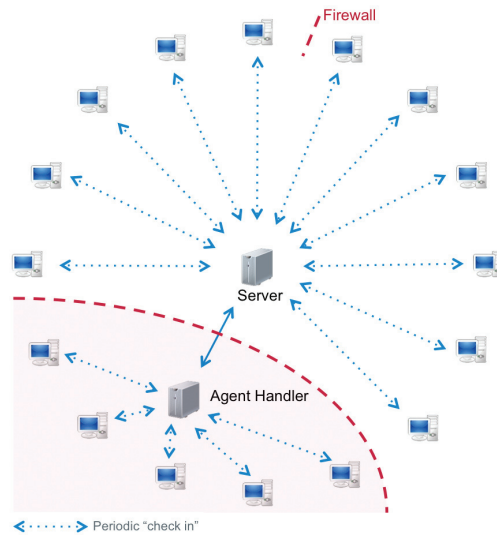
How Does It Work?

Real Time for McAfee ePO uses a scalable peer-to-peer methodology for querying information from hundreds of thousands of endpoints in mere seconds. This enhancement results in expedited feedback from queries, providing more precise and current information on which to base more intelligent analysis and decision making.

Let's look at how it works. After installation, clients contact the McAfee ePO server from time to time and transmit minute amounts of information regarding peers in their vicinity. Over time, a best path hierarchy emerges, and the data path is optimized for expedient results. Further, clients automatically route around obstacles in communication to avoid bottlenecks, and newly acquired clients are evaluated to further enhance speed. The end result is a robust network of chained clients, each receiving and distributing information to optimize efficiency and avoid "speed bumps." The volume of traffic on the WAN is insignificant, further enabling quick data transfer between nodes for rapid query response. The economic size of the distributed packet in concert with the streamlined communication chain facilitates this rapid querying efficiency and speed.

Architecture Comparison

Traditional security management topology



Real Time for McAfee ePO security management topology

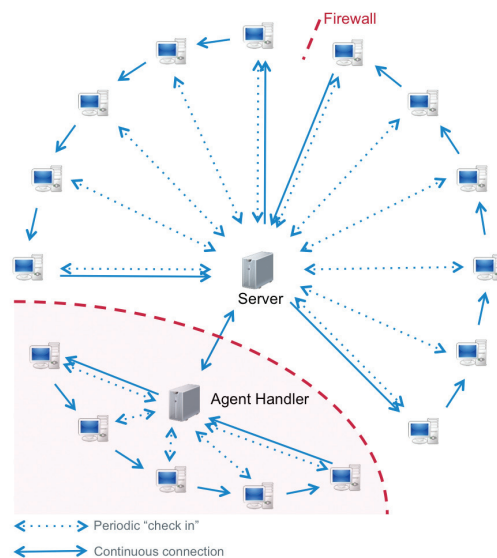


Figure 1. Peer-to-peer relationship and economical packet size work in concert to significantly improve query response time.

Typical Queries, Lightning Fast Results

Real Time for McAfee ePO uses this architecture to instantly query and report back on common criteria such as:

- What applications are installed where?
- Are there any unauthorized applications installed to machines in my system?
- Do all machines have up-to-date virus definitions and enabled firewalls?
- Which machines are not using encryption?
- Which machines contain personal identifiable information?
- Are any unauthorized machines currently attached to my system?
- What mobile devices are accessing data within my system?

Real Time for McAfee ePO is designed as an enhancement to existing McAfee ePO software functionality and includes the following and much more:

- Real Time for McAfee ePO Server API for query
- Integrated McAfee ePO software workflow and asset modeling
- Real Time for McAfee ePO Agent plug-in

Availability

For current McAfee ePO software subscribers (version 4.6 and above), Real Time for McAfee ePO is an entitlement. Real Time for McAfee ePO is scheduled for first customer shipment in the first quarter of 2013.

For more information, contact your McAfee Sales Representative or Realtime@mcafee.com for inquiries.

