SOLUTION BRIEF

McAfee
Together is power.

Real-Time Network Visibility for Comprehensive Endpoint Detection and Response

McAfee ePolicy Orchestrator software and Lumeta Spectre Integration

Using McAfee® ePolicy Orchestrator® (McAfee ePO™) software and Lumeta Spectre together gives IT organizations the real-time visibility they need to proactively identify, manage, and respond to endpoint security issues and threats across dynamic cloud, virtual, mobile, and physical networks.

McAfee Compatible Solution

- Lumeta Spectre
- McAfee ePO software 5.3.2

McAfee
COMPATIBLE

SIA Rookie of the Year Award Winner for 2017

LUMETA
DETECT WITH A HIGHER SENSE

The Challenges

Endpoint security solutions can only protect assets that are known, and, in most instances, require agents to work effectively. Blind spots may result when agents are disabled, rogue devices are connected to the network, unauthorized networks are created, or networks are misconfigured, even in a minor way. Blind spots like these may render the entire environment vulnerable to compromise. Field-tested Spectre demonstrates a 20% increase, on average, of IT infrastructure visibility when using the solution to identify previously unknown network segments and endpoints.

The McAfee ePO/Lumeta Spectre Integrated Solution

McAfee ePO software includes McAfee Active Response, a comprehensive endpoint detection and response (EDR) solution used for detection and investigation of indicators of attack (IoAs) and remediation.

Lumeta Spectre's situational awareness capability recursively and authoritatively indexes all connected endpoints, plus all networks and devices, whether physical, mobile, virtual, or cloud. In addition, Lumeta Spectre immediately detects and monitors new devices connecting to the network.

Lumeta Spectre's authoritative index of all network devices ensures that McAfee ePO software is aware of all endpoints that require deployment of the McAfee ePO software agent—ensuring 100% coverage across all hosts. Together, McAfee ePO software and Lumeta Spectre enable IT organizations to obtain real-time network visibility for endpoint security across the entire enterprise network.

From within the Lumeta Spectre user interface, users can proactively launch the McAfee ePO software user interface to initiate threat containment, blocking, and remediation activities. The integration makes your security more effective by delivering continuous, real-time detection of and response to advanced security threats. This helps security professionals monitor security posture, improve threat detection, and expand incident response capabilities by way of forward-looking discovery, detailed analysis, forensic investigation, comprehensive reporting, and prioritized alerts and actions.

How It Works

Lumeta Spectre queries the McAfee ePO software application programming interface (API) at a polling interval set by the user and retrieves the inventory of hosts, servers, and other endpoint systems (McAfee ePO software managed assets).

Lumeta Spectre correlates this inventory against its authoritative index of IP address space and highlights the differences and commonalities into views:

Highlights

- Shorten time from insight to response through actionable dashboards with advanced queries and reports—this integration provides the ability to launch directly from Lumeta Spectre into an actionable McAfee ePO console.
- Get the comprehensive visibility you need, in real-time, to proactively address endpoint security issues.
- Reveal, on average, more than 20% of your IT infrastructure, including previously unknown, unmanaged, and unsecured networks and endpoints.

- **Lumeta Spectre-only IPs:** IP addresses Lumeta Spectre knows about but are not yet managed by McAfee ePO software.
- **McAfee ePO software and Lumeta Spectre-managed IPs:** IP addresses known by both McAfee ePO software and Lumeta Spectre.
- **McAfee ePO software-only IPs:** IP addresses McAfee ePO software knows about, but are unknown to Lumeta Spectre (for example, if Lumeta Spectre does not have access to a network or an off-network device, but McAfee ePO software is still aware of the client agent).

Lumeta Spectre then pushes the missing elements back to the McAfee ePO software server. This ensures that McAfee ePO software has the complete set of networks and devices to manage, so it can provide more complete security coverage and eliminate blind spots.

These views, along with reports and maps, are available in Lumeta Spectre via the endpoint management dashboard, a visual display of events and issues related to McAfee ePO software-managed hosts. This dashboard facilitates identification and remediation of vulnerable and compromised endpoints.

In reviewing the data on the Lumeta Spectre dashboard, users can view device details. If the user selects endpoint context/action, it will launch the McAfee ePO software user interface, where the user can initiate a remediation action on hosts or view context related to any managed host.

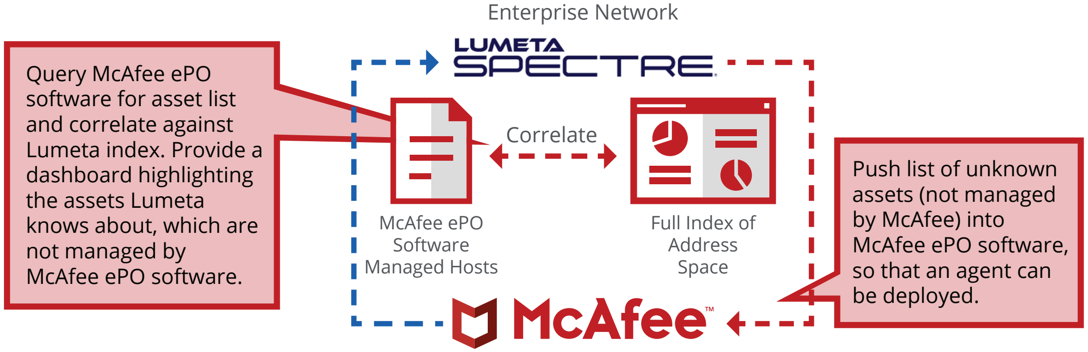
Enterprise Network
LUMETA SPECTRE
Query McAfee ePO software for asset list and correlate against Lumeta index. Provide a dashboard highlighting the assets Lumeta knows about, which are not managed by McAfee ePO software.
Correlate
McAfee ePO Software Managed Hosts
Full Index of Address Space
Push list of unknown assets (not managed by McAfee) into McAfee ePO software, so that an agent can be deployed.
McAfee

Figure 1. Lumeta Spectre operates in real time and detects devices connecting to the network.

As Lumeta Spectre operates in real time, when it detects a device connecting to the network, it checks to see whether the asset has a McAfee ePO software agent installed and active. If not, this would represent an undefended endpoint. Lumeta Spectre alerts administrators, and they can then view device details to launch the McAfee ePO user interface to automatically deploy a McAfee ePO software agent to the asset.

About Lumeta Spectre

Lumeta Spectre provides true visibility into networks that extend into the cloud and to connected endpoints. Our ability to discover rogue and shadow networks and endpoints, including virtual machines, in your organization's infrastructure sets us apart from the myriad of companies with lots of promises in preventing breaches. We take that unique level of visibility and combine it with threat intelligence to achieve a new level of situational awareness to help security and network teams identify potential malicious or harmful activity on the network. They gain the context and intelligence to detect and stop threats before a breach can occur.

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.

McAfee™
Together is power.

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