LUMETA
DETECT WITH A HIGHER SENSE

DATASHEET

McAfee ePolicy Orchestrator (McAfee ePO) and Lumeta Spectre Integration

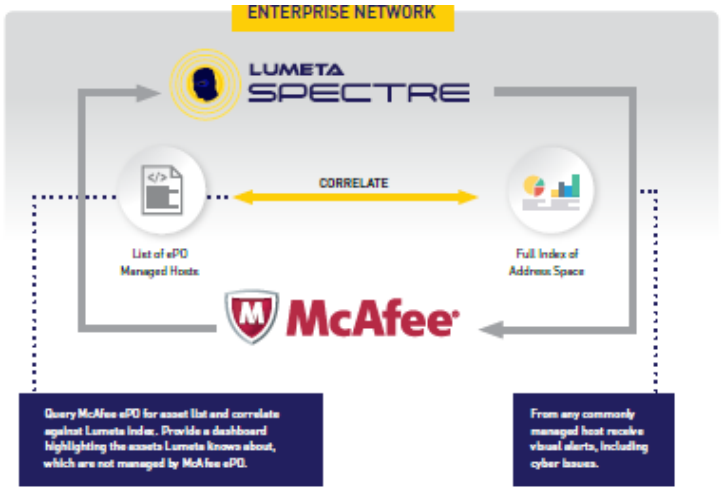
Using McAfee ePO and Lumeta Spectre together gives IT organizations the real-time visibility they need to pro-actively identify, manage, and respond to endpoint security issues and threats across dynamic cloud/ virtual/mobile/physical networks.

The Challenge - you can't secure endpoints you don't know about
McAfee ePO software includes McAfee Active Response, a comprehensive endpoint detection and response (EDR) feature for indicator of attack (IoA) investigation and remediation. It requires a client agent to be active on every device. If an organization has any blind spots – "undefended" endpoints –remain extremely vulnerable to cyber attacks.

Benefits of the McAfee ePO – Lumeta Spectre Integrated Solution
McAfee ePO software includes McAfee Active Response, a comprehensive endpoint detection and response (EDR) feature for indicators of attack (IoA) investigation and remediation. However, in order to be effective, Lumeta's field experience has proven that Lumeta Spectre typically reveals, on average, more than a 20% gap in visibility of IT infrastructure which includes entire network segments and endpoints. The visibility gap is typically due to network changes that leave endpoints unprotected and vulnerable to compromise from rogue activity or malicious actors.

HIGHLIGHTS

- McAfee ePO's capabilities include endpoint security management.
- Lumeta Spectre provides real-time authoritative indexing for network visibility.
- The integration identifies unknown assets on your network, not yet managed by McAfee ePO, so you can bring them under control.
- Shorten time from insight to response through actionable dashboards with advanced queries and reports – the 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 pro-actively address endpoint security issues.
- Lumeta Spectre can reveal, on average, more than 20% of IT infrastructure which includes previously unknown, unmanaged and unsecured networks and endpoints.



McAfee ePO and Lumeta Spectre Integration

Even a single unprotected host can expose an organization to a significant breach!

Lumeta Spectre cyber situational awareness recursively and authoritatively indexes all connected endpoints (plus all networks and devices), whether physical, mobile, virtual, cloud. And, in real time, Lumeta Spectre immediately detects and monitors new devices connecting to the network. Together, McAfee ePO and Lumeta Spectre enable IT organizations to obtain real-time network visibility for endpoint security across the entire enterprise network.

The integration provides continuous, real-time monitoring of any hosts that are not yet managed by McAfee ePO, and situational awareness of cyber threats present on devices. Lumeta Spectre's authoritative index of all network devices ensures that McAfee ePO is aware of all endpoints that require deployment of the ePO agent – ensuring 100% coverage to all hosts.

For proactive response, from within the Lumeta Spectre UI, users can launch directly into the McAfee ePO UI for threat containment, banning and remediation activities. The integration allows for a more effective security program by delivering continuous, real-time detection of and response to advanced security threats to help security practitioners monitor security posture, improve threat detection, and expand incident response capabilities through forward-looking discovery, detailed analysis, forensic investigation, comprehensive reporting, and prioritized alerts and actions.

How It Works

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

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

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

Lumeta Spectre then pushes the missing elements back to the ePO server. This ensures that ePO has the complete set of networks and devices to manage for more complete security coverage and eliminating blind spots providing breach prevention. 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 ePO managed hosts, facilitating 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 UI where the user can take action on hosts or view context related to any managed host.

As Lumeta Spectre operates in real-time, when it detects a device connecting to the network, it checks to see whether the asset has an ePO agent installed and active. If not, this would represent an undefended endpoint. Lumeta Spectre alerts administrators (and they can view Devices Details to launch the ePO UI to deploy a McAfee agent to the asset) and advises the ePO server to automatically deploy a McAfee agent to the asset (if ePO is configured as such).

At Lumeta, we have firmly established our flagship product as truly providing visibility into networks that even extend into the cloud and connected endpoints. Our ability to discover rogue and shadow networks and endpoints, including VMs even in the darkest corners of an organization's infrastructure is the first piece of the puzzle that sets us apart from the myriad of companies with lots of promises in preventing breaches. When we take that unique level of visibility and combine that with threat intelligence we achieve a new level of what we call Cyber Situational Awareness to help security and network teams identify potential malicious or harmful activity on the network and have the context and intelligence to detect and stop threats before a breach. As part of your overall security program, including protecting endpoints from compromise, Lumeta Spectre is a critical piece for contributing to the success of your security program.

LUMETA
DETECT WITH A HIGHER SENSE