DATA SHEET

Lumeta
Cyber Situational Awareness

Eliminating Blind Spots with Real-Time Visibility and Monitoring for Network Endpoints

Lumeta ESI Works With Next Generation Anti-Virus and Endpoint Threat Detection and Response Solutions to Prevent Compromises

Lumeta ESI working with various endpoint security solutions 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. Lumeta ESI is fully integrated with McAfee ePO and Carbon Black Response, but also works side-by-side with any endpoint security solution.

The Challenge - you can't secure endpoints you don't know about

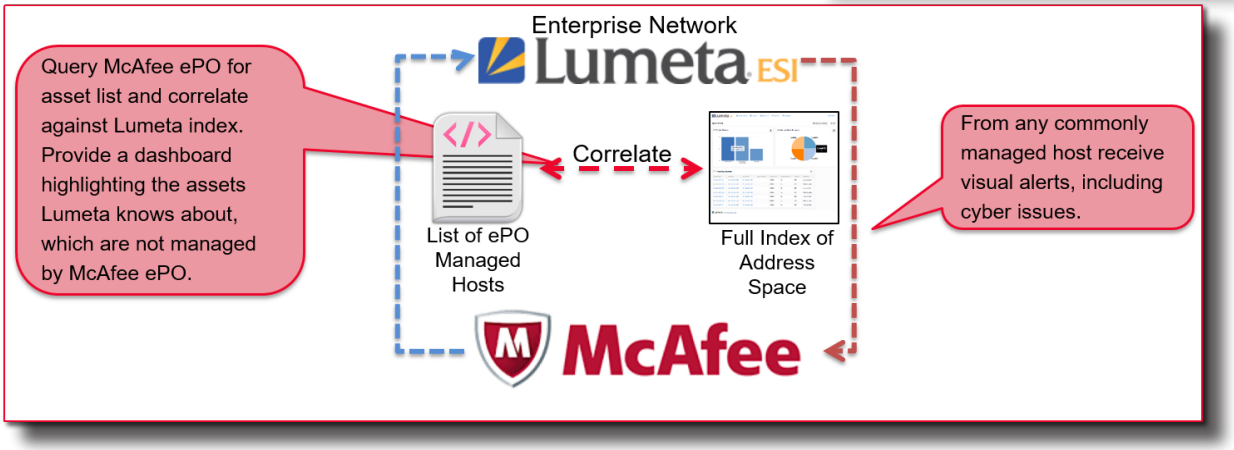
The majority of even the most comprehensive next generation anti-virus (NGAV) and endpoint detection and response (EDR) feature solutions requires a client agent to be active on every device. If an organization has any blind spots – "undefended" endpoints – they remain vulnerable to cyber attacks.

Benefits of the using Lumeta ESI with Endpoint Security

In order to be effective, Lumeta's field experience has proven that ESI typically reveals, on average, more than 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. Even a single unprotected host can expose organization to a significant breach.

Highlights

- Lumeta ESI is integrated with McAfee ePO and Carbon Black Response but can help any endpoint solution be more effective.
- Lumeta ESI provides real-time authoritative indexing for network visibility.
- The integration identifies unknown assets on your network, not yet managed by your endpoint security solution, so you can bring them under control.
- Shorten time from insight to response through actionable dashboards with advanced queries and reports
- Get the comprehensive visibility you need, in real time, to pro-actively address endpoint security issues.
- ESI can reveal, on average, more than 20% of IT infrastructure which includes previously unknown, unmanaged and unsecured networks and endpoints.



Example of Enhanced Endpoint Management and Protection for McAfee ePO integrated with Lumeta ESI

Lumeta ESI 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 ESI immediately detects and monitors new devices connecting to the network. Lumeta ESI, integrated with or working side-by-side with today's leading endpoint security vendors 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 the majority of endpoint security platforms, and situational awareness of cyber threats present on devices. Lumeta ESI's authoritative index of all network devices ensures that endpoint security solutions are aware of all endpoints that require deployment of an agent – ensuring 100% coverage to all hosts.

How It Works with McAfee ePO and Carbon Black Response

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

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

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

Lumeta ESI 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.

These views (along with reports and maps) are available in Lumeta ESI 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.

For proactive response, from within the Lumeta ESI dashboard, 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.

As Lumeta ESI operates in real-time, when ESI 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. ESI 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 ESI is a critical piece for contributing to the success of your security program.