LUMETA
DETECT WITH A HIGHER SENSE

DATASHEET

Eliminating 100% Endpoint Security Blind Spots with Lumeta Spectre and Carbon Black Response

Carbon Black Enterprise Response and Lumeta SPECTRE Integration
Using Carbon Black Enterprise Response and Lumeta Spectre together enables IT organizations to provide eliminate over 40% of their unknown, unmanaged, rogue and shadow endpoints in real-time through enhanced network visibility, enabling complete endpoint threat detection across the enterprise.

The Challenges
In the age of large organizations being brought down by data breaches, your business can't afford to let malware invade your network. Endpoint security needs to be proactive and disrupt advanced attacks on the endpoint. EDR (Endpoint Detection and Response) software requires a client agent/ component on every device. If an organization has any blind spots – "undefended" endpoints – they remain vulnerable to cyber attacks. In addition, companies are lacking in overall visibility into network and cloud infrastructure including connected endpoints.

Benefits of the Carbon Black Enterprise Response – Lumeta Spectre Integrated Solution

Carbon Black Enterprise Response continuously records, centralizes and retains activity from every endpoint to identify attacks and keep a history of an attacker's every action.

Lumeta Spectre, the pioneering solution in real-time cyber situational awareness, provides an authoritative index of all devices (and networks with devices), whether physical, mobile, virtual, cloud. And, in real time, Spectre immediately detects new devices connecting to the network.

Together, Carbon Black Enterprise Response and Lumeta Spectre enable IT organizations to obtain real-time network visibility for endpoint security across the entire enterprise network – the best prevention to detect threats and disrupt adversary behavior.

Highlights

- Carbon Black Enterprise Response provides EDR (Endpoint Detection and Response) capabilities.
- Lumeta Spectre provides real-time authoritative indexing for network visibility.
- The integration determines if any hosts are not yet managed by Carbon Black Enterprise Response or unknown to Lumeta Spectre.
- The integration provides network-based context related to hosts and the ability
to launch directly from Lumeta Spectre into an actionable Carbon Black Enterprise Response console.

Lumeta Corporation | 300 Atrium Drive, Suite 302 | Somerset, NJ 08873 USA | +1.732.357.3500 | www.lumeta.com

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta Spectre's authoritative index of all network devices ensures that Carbon Black Enterprise Response is aware of all endpoints that require deployment of the EDR software – ensuring you have 100% coverage to all the hosts.

Also, from within the Lumeta Spectre UI, users can go directly back to the Carbon Black Enterprise Response UI for threat containment, banning and remediation activities.

How Does It Work?

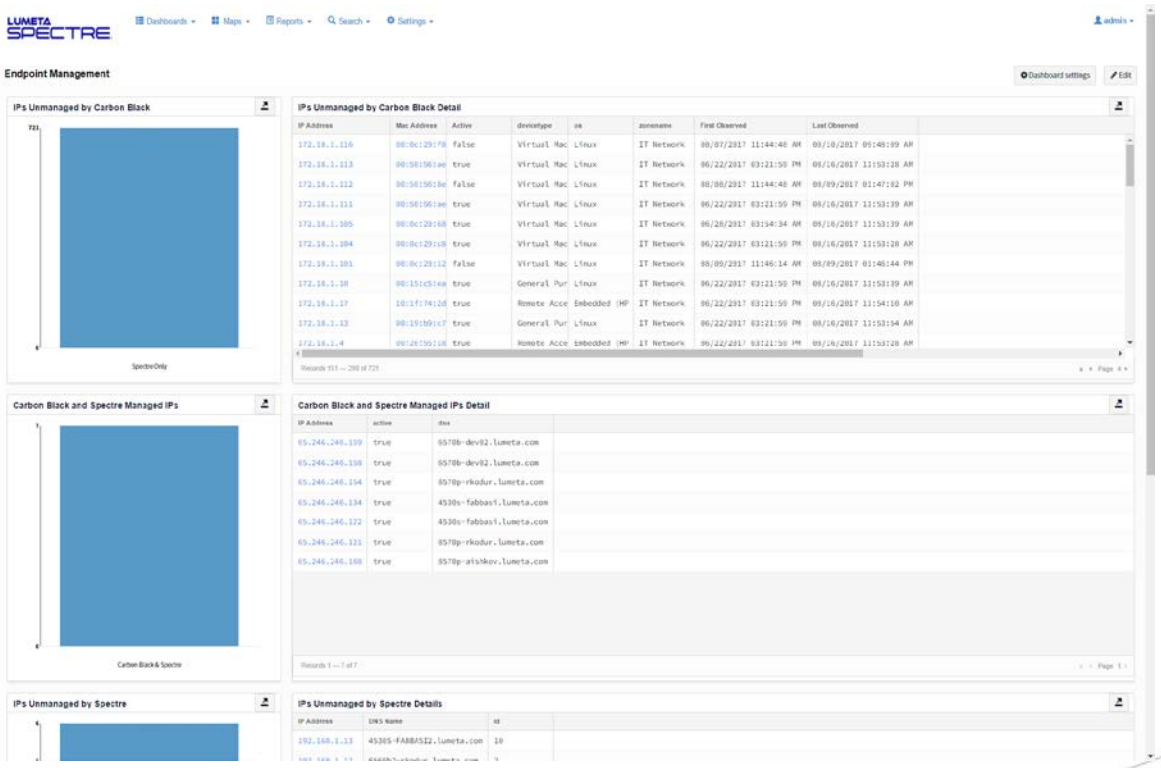
Lumeta Spectre accesses the API of Carbon Black Enterprise Response (at a polling interval set by the user) and retrieves the inventory of hosts, servers, and other endpoint systems ("Carbon Black managed endpoints").

Lumeta Spectre correlates this inventory against Spectre's authoritative index of IP address space – comparing to advise Carbon Black Enterprise Response of any devices where it doesn't see a Carbon Black endpoint indicated on the device, as those would be undefended endpoints.

Lumeta Spectre highlights the differences and commonalities into views:

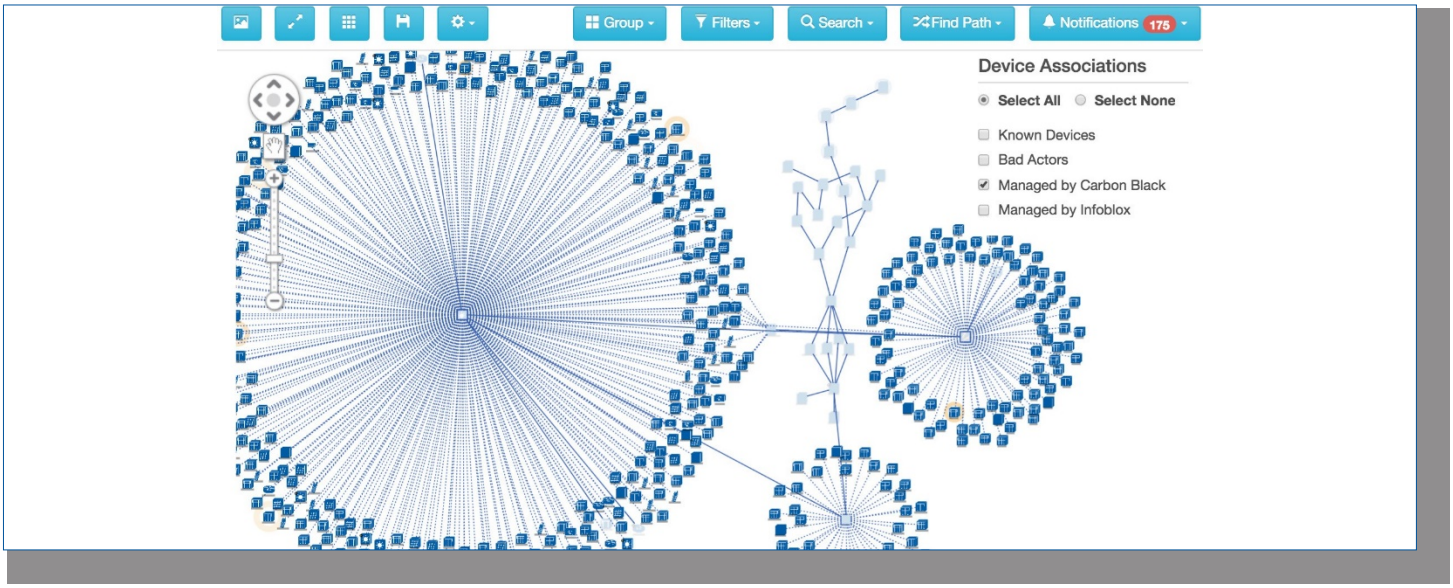
- Spectre Only IPs: IP addresses Lumeta Spectre knows about, but are not yet managed by Carbon Black Enterprise Response
- Carbon Black Only IPs: IP addresses Carbon Black Enterprise Response knows about, but are unknown to Lumeta Spectre (e.g., if Lumeta does not have access to a network or an off-network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

This information is available in Lumeta Spectre via the Endpoint Management Dashboard, as well as reports and maps, facilitating identification and remediation of vulnerable and compromised endpoints.

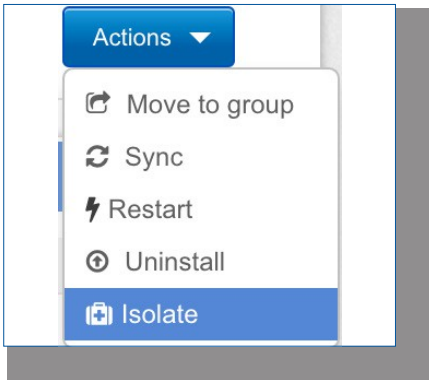


LUMETA
DETECT WITH A HIGHER SENSE

In reviewing the data on the Lumeta Spectre dashboard, users can view Device Details. If the user selects Endpoint Context/Action, it will redirect to the Carbon Black Enterprise Response UI where the user can take action to restart, remove, sync or isolate an endpoint.



Lumeta Spectre *map indicating endpoints managed by Carbon Black Enterprise Response*



Black Enterprise Response UI where the user can take action to restart, remove, sync or isolate an endpoint