

Application Note on Lumeta Integrations

If your hybrid enterprise manages risk with a blend of EDR, HVM, IPAM, and breach management solutions, FireMon Lumeta is the glue your platform needs. Lumeta is the real-time discovery, visibility, and cybersecurity-automation solution that finds unknown networks, devices, and connections and then provides this information to both customers and integrated applications. Real-time, authoritative data about the network and its devices are selectively shared with all of the integrated security applications managing your enterprise network. Lumeta synthesizes device responses, performs analyses to surface risk, and alerts both systems and people with the power to remediate—lightening the load on cloud, network, and security teams, and amplifying the value of network-management applications by supplying them with better data. FireMon Lumeta feeds the integrated applications better device data and enhances what they know.

The FireMon platform delivers superior results and supports superior security intelligence: The broadest reach and most comprehensive network discovery in the industry, authoritative visibility, and an integrated way to understand and automate the remediation of significant events, trends, security gaps, threats, and misconfigurations. Integrate FireMon Lumeta with your security applications today to achieve the full value of your network security ecosystem.

What is a Lumeta Integration?

An integration in the context of the FireMon Lumeta solution is analogous to a plugin, add-on, or extension. It joins Lumeta to other parts of your network-security platform, enabling

the two to exchange information. Lumeta does not replace these applications—it makes them work better by making Lumeta's authoritative index of device data, connections, and networks available to the integrated platform. Feeds are attached through the Lumeta API and through various integrated data connectors. Some of these connectors identify vulnerable networks and devices by matching Lumeta-discovered data with ingested threat intelligence. Other connectors can identify endpoints lacking agents or unknown to your network manager, or push missing addresses to your address manager, notifications to your alert manager, and session data to your user identifier. Unstructured data and query results are transmitted via API; only what's unknown to the integrated application is conveyed. Your current security solutions work better because Lumeta supplies the missing pieces to eliminate blind spots.

Configuring an integration is as easy as supplying Lumeta with login credentials to the integration's application server and specifying how often you want the two to exchange data.

The results from most integrations are ingested by Lumeta, indexed, and displayed in Lumeta dashboards. Data attributes ingested from them are used to enhance the Lumeta device profiles. Discovery and profile data from Lumeta is also shared to the management consoles of partner applications. The overarching value and most important thing to know about Lumeta integrations is that they amplify the value of your network security stack by ensuring that it manages a comprehensive and authoritative set of data.

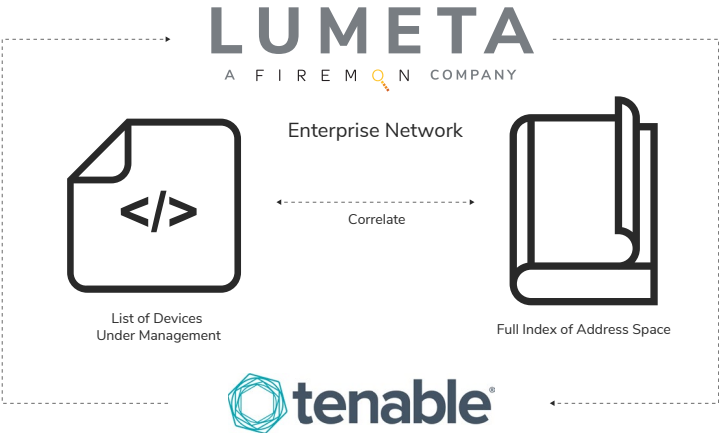
Host Vulnerability Management Integrations

Host Vulnerability Management (HVM) integrations such as Qualys and Tenable leverage threat intelligence to help organizations prioritize vulnerabilities for remediation. The Lumeta HVM integrations enable your organization to 1) identify devices in your network that are not managed by Qualys or Tenable SecurityCenter, 2) push metadata of those devices to integrated vulnerability management systems, and 3) extend the capabilities of your vulnerability management platform by feeding it Lumeta's authoritative data set.

Integrated Host Vulnerability Managers	Dashboard
Qualys	Qualys Management
Tenable SecurityCenter	Tenable SecurityCenter Management

► **Spotlight on Tenable**

The Tenable integration tells you which hosts on your enterprise network are either undefended by Tenable or unknown to Lumeta. By comparing Lumeta's comprehensive index of your network devices against that subset of network devices managed by Tenable, you can generate a list of network hosts that are not managed in the Tenable SecurityCenter and then push that information to an asset group on the Tenable SecurityCenter server. What's pulled from Tenable to Lumeta is only what you request, not an exhaustive collection of all the device details and attributes that Tenable manages. This enables Lumeta to scan just the network device attributes of value to you.



Endpoint Detection and Response Integrations

Endpoint Detection and Response software is installed on last-hop, non-forwarding devices such as laptops and printers to protect them from malware, exploits, and attacks. When you activate endpoint security integrations, Lumeta queries the integrated applications at the frequency you configure to identify the endpoints: 1) only the integrations are managing, 2) only Lumeta is managing, and 3) endpoints both are managing. Lumeta also pushes unmanaged devices to the integration partner so that agents can be installed on them.

Integrated EDR Managers	Dashboard
Carbon Black	Endpoint Management
McAfee ePO	McAfee ePO Management
RedSeal	RedSeal Management

► Spotlight on McAfee ePO

The McAfee ePO integration provides McAfee ePO customers with a way to ensure that McAfee's ePolicy Orchestrator agent is installed comprehensively on all network devices in one or more network segments. The integration reconciles McAfee findings with Lumeta findings to uncover: 1) assets lacking the McAfee ePO agent, 2) assets to which visibility is blocked, 3) assets with comprehensive management.

The devices listed in this Lumeta dashboard widget are missing McAfee's ePolicy Orchestrator agent, which is a required element in the customer's network. The end customer would be unaware of these policy violations without Lumeta.

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed
2600:802:460:652::2		true			Lumeta	08/13/2019 02:54:53 PM	02/06/2020 10:00:32 AM
2600:802:460:652::1		true			Lumeta	11/11/2019 04:16:55 PM	02/06/2020 10:00:32 AM
2600:802:460:624::1		true			Lumeta	11/19/2019 02:05:37 PM	02/06/2020 10:00:32 AM
2600:802:460:425:250:56ff:feb9:cdce	00:50:56:b9:cd:ce	true	Server		Lumeta	01/19/2020 03:33:16 PM	02/06/2020 10:00:32 AM
2600:802:460:425:250:56ff:feb5:88a8	00:50:56:b5:88:a8	true	Server		Lumeta	11/23/2019 06:43:01 PM	02/06/2020 10:00:32 AM
2600:802:460:425:250:56ff:feae:3f8e		true			Lumeta	09/13/2019 08:17:40 AM	02/06/2020 10:00:32 AM
2600:802:460:425:250:56ff:fe82:40f		true			Lumeta	11/11/2019 04:14:47 PM	02/06/2020 10:00:32 AM
2001:da8:a008:ffff:ffff:ffff:ffe:f82e	50:c5:8d:ec:78:52	true	Infrastructure	Embedded Juniper	Lumeta	12/13/2019 01:57:35 AM	02/06/2020 10:00:32 AM
2001:da8:a008:ffff:ffff:ffff:ffe:f82a	50:c5:8d:ec:79:73	true	Infrastructure	Embedded Juniper	Lumeta	12/13/2019 01:57:35 AM	02/06/2020 10:00:32 AM
2001:da8:a008:ffff:ffff:ffff:ffe:f81e	50:c5:8d:ec:7a:94	true	Infrastructure	Embedded Juniper	Lumeta	12/13/2019 01:57:35 AM	02/06/2020 10:00:32 AM

IP Address Management (IPAM) Integrations

An important early step in conducting any census of managed assets is to validate IPAM tracking and allocation data. To that end, BlueCat and Infoblox have been integrated with Lumeta. When you activate the Infoblox IPAM integration, Lumeta queries Infoblox, correlates the query results against what Lumeta "knows," generates responses, and pushes metadata about discovered devices to Infoblox. Infoblox is one of several Lumeta integrations that not only pulls data from the integrated application, but also pushes data to it.

Integrated IP Address Managers	Dashboard
BlueCat	BlueCat Management
Infoblox	Infoblox Management

► Spotlight on BlueCat

The BlueCat Management dashboard enables you to identify any IP address space that is missing from your BlueCat Address Management (BAM) server.

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed
172.18.1.195	00:50:56:82:b8:36	true	Server	Linux	Zone1	12/05/2019 10:35:20 AM	12/06/2019 02:34:23 PM
172.18.1.192	00:50:56:9a:eb:0f	true	Server	Linux	Zone1	12/05/2019 10:35:20 AM	12/06/2019 02:34:23 PM
172.18.1.192		true			zone2	12/05/2019 02:45:21 PM	12/06/2019 12:47:40 PM
172.18.1.191	00:50:56:ae:01:96	true	Server	Linux	Zone1	12/05/2019 10:35:20 AM	12/06/2019 02:34:21 PM
172.18.1.191		true			zone2	12/05/2019 02:45:20 PM	12/06/2019 12:48:40 PM

Records 1 - 50 of 218

The dashboard provides these device attributes:

- **Active** - True/False status indicating whether the device responded to a Lumeta probe
- **Device Type** - Descriptor of the device such as server, router, printer
- **DNS Name** - Name given to device by Domain Name System
- **First Observed** - Timestamp of when the device first responded to a probe from Lumeta
- **IP Address** - The unique IPv4 or IPv6 device identifier
- **Last Observed** - Timestamp of when the device last responded to a probe from Lumeta
- **LocationCode** - Indicates the country, city in UN/ LOCODE, and custom locations such as CA TOR OF1 indicates: CA=Canada TOR=Toronto OF1=Office 1
- **MAC Address** - The unique device identifier
- **OS** - Operating system running on the device
- **State** - Categorizes IP address assignment permanence (e.g., static, DHCP-reserved, gateway)
- **Zonename** - Name of the zone in which the device was discovered

Network Management Integrations

Network management integrations ensure that the deployed networks you manage through a single browser interface all show up. When you enforce device security policies, deploy software and apps, and perform remote, live troubleshooting on managed devices, these integrations validate that you're handling all the devices in a zone in their entirety.

Integrated Network Managers

Meraki

Dashboard

None - Results augment device details

► Spotlight on Meraki



Meraki, a division of Cisco, is a web-based network management system. Customers purchase Meraki-brand routers, switches, firewalls and even cameras, deploy them on their network and then manage them via a website. This integration is another Lumeta discovery technique. From Meraki, Lumeta pulls router, switch and firewall information, including the interface tables of those devices, along with the MAC/IP addresses of all endpoints. This data augments Lumeta device details for those devices and displays in Lumeta analytics.

The responses from Meraki are used to enhance the interface information displayed in Lumeta Device Details, including:

- **Network** - Including additional Layer 3 switch data
- **Devices** - Additional information from Meraki has been added re: MX* model security appliances
- **Interface** - Including port information from Meraki
- Meraki source identifier called out in Lumeta Device Details.
- Meraki-inflected device fingerprints, identification, and confidence-rankings.
- Meraki-sourced devices and CIDRs can be added to Lumeta Target List and Lumeta Eligible List.

Device Details

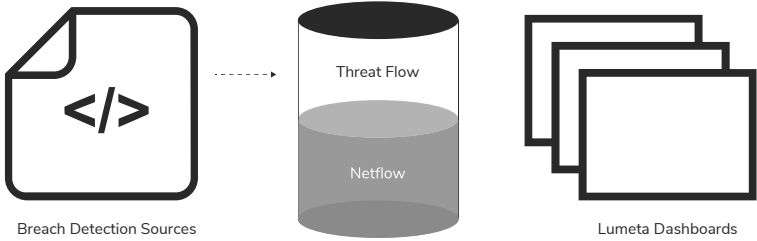
Enter IP, MAC, Custom Attribute, Cloud Instar

172.31.30.8  

Device Info	Attribute	Value
Device Profile	vendor	Meraki
Attributes	serial	JYJ
	networkName	ay
Interfaces	name	-AP1
Connected Hosts - Layer 3	model	MR33
Leak Response	merakiNetworkId	437
	lng	022
Notifications	lat	362
Alternate IPs	firmware	wireless-25-13
WMI Services	externalSource	Meraki Management Station
Cisco pxGrid	deviceType	Access Point

Breach Detection Integrations

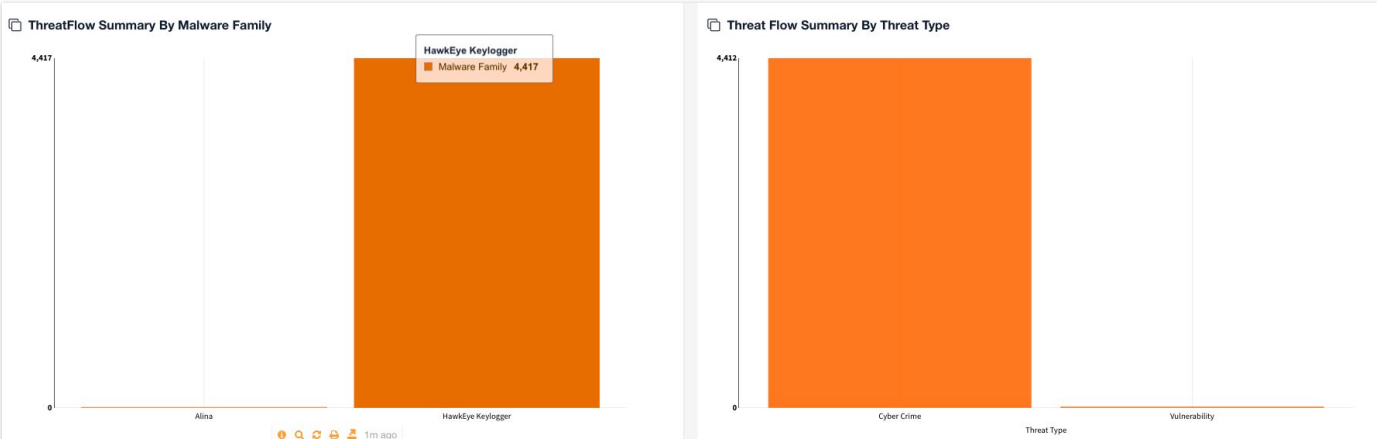
Lumeta breach detection integrations find the activity of malware in your network. They identify which devices on your network have been compromised by known bad actors. When you connect a breach detection integration such as Accenture's iDefense, Lumeta correlates data from two sources: netflow data and real-time streams of data providing information on potential cyber threats and risks. Compromised network assets including their attributes are reported in Lumeta.



Integrated Breach Detectors	Dashboard
Emerging Threats (open source)	Breach Detection
Gigamon NetFlow	Breach Detection
iDefense	Breach Detection - iDefense
ISC Ports	Breach Detection
TOR	Breach Detection

► Spotlight on iDefense

Lumeta provides actionable lists of zombie devices and threat flows in your network by correlating a closed-source threat intelligence feed from iDefense IPs against your network's IPs. Lumeta ingests a single source of netflow data or multiple sources that have first been bundled via a netflow aggregator such as Gigamon.



Risk Management Integrations

Lumeta amplifies the value of a Risk Managers such as FireMon Security Manager. FireMon Security Manager can better assess risk, prioritize remediation, and minimize the attack surface of the networks it manages.

Integrated Risk Managers	Dashboard
FireMon Security Manager	FireMon Management
Rapid7	Rapid7 Management

► Spotlight on Security Manager

FireMon offers a complete end-to-end solution for device visibility, leak path detection, network device clean-up, and compliance reporting using Lumeta and Security Manager. Attributes of devices Lumeta has profiled as being a unique router, Layer 3 switch, or firewall are pushed to Security Manager. Security Manager then compares these device records to those it manages already. A Security Manager administrator can apply rules, correct misconfigurations, and make the Lumeta-discovered devices policy-compliant—all on the FireMon platform.

Security Stack Alerting Integrations

Applications in the Security Stack Alerting space such as Splunk have created a “security stack ecosystem” that is aware of and responsive to change notifications.

The Splunk integration fortifies this ecosystem by providing it with real-time alerts and event notifications ingested from Lumeta.

- Lumeta publishes real-time “messages” on network changes to Splunk “topics.”
- Systems comprising the security stack “subscribe” to the topics.
- The “subscribers” respond to the event notifications, alerts, and change notifications they receive automatically via security stack systems.

Integrated Security Stack Managers	Dashboard
Splunk (3.3.6x)	(3.3.6x)
Service Now (3.3.6x)	(3.3.6x)
McAfee DXL	McAfee DXL Management

► Spotlight on Splunk

The Lumeta integration with Splunk fortifies the notifications that reach Splunk, enabling you to find out more of what is happening in your business so that you can take meaningful action on it quickly.

User Identification Integrations

User Identification integrations such as Cisco pxGrid ingest user session data. For organizations that want to ensure that NAC is active on all of their network assets, this information is important. Lumeta uses the Cisco ISE pxGrid to identify users and user sessions. It creates tables for Sessions, Identity Groups, Security Groups and Endpoints. For each discovered IP address, it discovers in real-time: Username, Session state, NAC server IP and port, RADIUS attribute-value pairs.

Integrated User Identification Managers	Dashboard
Cisco pxGrid	Cisco pxGrid

► **Spotlight on Cisco pxGrid**

Lumeta enables the exchange of context with Cisco products via a Cisco pxGrid server to validate endpoint, identity group, security group, and session data.



FireMon is the #1 network security automation solution for hybrid cloud enterprises. FireMon delivers persistent network security for multi-cloud environments through a powerful fusion of real-time asset visibility, compliance and automation. Since creating the first-ever network security policy management solution, FireMon has delivered command and control over complex network security infrastructures for more than 1,700 customers located in nearly 70 countries around the world. For more information, visit www.firemon.com.

