App Notes on Asset Manager Integrations

If your hybrid enterprise manages risk with a blend of EDR, HVM, IPAM, and breach management solutions, FireMon Asset Manager is the glue your platform needs. Asset Manager 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. Asset Manager 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. Asset Manager feeds the integrated applications better device data and enhances what they know.

The 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 Asset Manager with your security applications today to achieve the full value of your network security ecosystem.

What is an Asset Manager Integration?

An integration in the context of the Asset Manager solution is analogous to a plugin, add-on, or extension. It joins Asset Manager to other parts of your network-security platform, enabling the two to exchange information. Asset Manager does not replace these applications—it just makes them work better. It does this by making Asset Manager's authoritative index of device data, connections, and networks available to the integrated platform. Feeds are attached through the Asset Manager API and through various integrated data connectors. Some of these connectors identify vulnerable networks and devices by matching Asset Manager-discovered data with ingested threat intelligence. Others identify endpoints lacking agents or unknown to your network manager. Still others 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 Asset Manager supplies the missing pieces, eliminating blind spots.

Configuring an integration is as easy as supplying Asset Manager 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 Asset Manager, indexed, and displayed in dashboards. Data attributes ingested from them are used to enhance the device profiles. Discovery and profile data from Asset Manager is also shared to the management consoles of partner applications.

The overarching value and most important thing to know about Asset Manager 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 Asset Manager HVM integrations enable your organization to:

1) Identify devices in your network that are not managed by Qualys or Tenable SecurityCenter

2) Push metadata about those devices to integrated vulnerability management systems

3) Extend the capabilities of your vulnerability management platform by feeding it Asset Manager’s authoritative data set.

Integrated Host Vulnerability Managers	**Dashboard**
Qualys	Qualys Management
Tenable	Tenable.io Management Dashboard Tenable.sc Management Dashboard
Rapid7 InsightVM Integration	Rapid7 Management Dashboard

Spotlight on Tenable

The Tenable integration tells you which hosts on your enterprise network are either undefended by Tenable or unknown to Asset Manager. By comparing Asset Manager's comprehensive index of all 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 Asset Manager is only what you request, not an exhaustive collection of all the device details and attributes that Tenable manages. The enables Asset Manager 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, Asset Manager queries the integrated applications at the frequency you configure to identify the endpoints:

1) only the integrations are managing

2) only Asset Manager is managing

3) endpoints both are managing

Asset Manager also pushes unmanaged devices to the integration partner so that agents can be installed on them.

Integrated Endpoint Detection and Response Managers	**Dashboard**
VMware Carbon Black	Carbon Black Management Dashboard
Trellix ePO Integration	Trellix ePO Management Dashboard

Spotlight on Trellix ePolicy Orchestrator

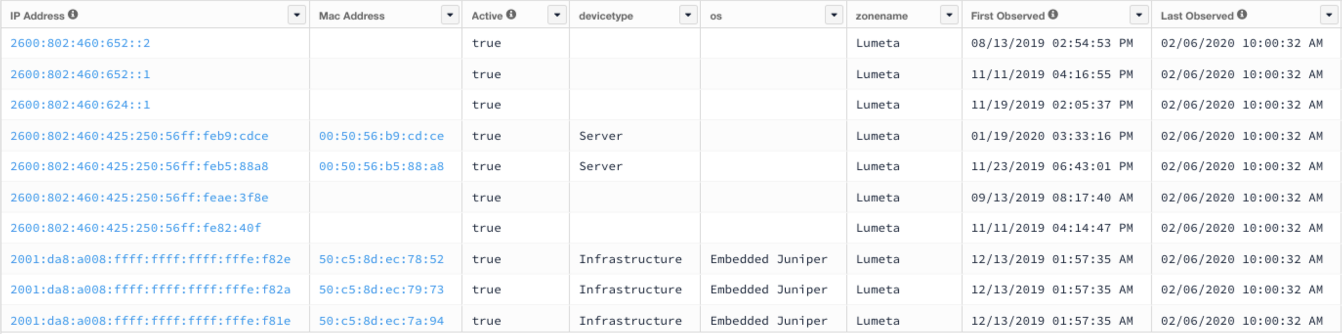
The Trellix ePolicy Orchestrator integration provides Trellix ePO customers with a way to ensure that Trellix's ePO agent is installed comprehensively on all network devices in one or more network segments. The integration reconciles Trellix findings with Asset Manager findings, uncovering:

1) assets lacking the Trellix ePO agent

2) assets to which visibility is blocked

3) assets with comprehensive management

The devices listed in this Asset Manager dashboard widget are missing Trellix's ePO agent, which is required element in the customer's network. The end-customer would be unaware of these policy violations were it not for Asset Manager.



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:fffe: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:fffe: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:fffe: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 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 to Asset Manager. When you activate the Infoblox IPAM integration, Asset Manager queries Infoblox, correlates the query results against what Asset Manager "knows," generates responses, and pushes metadata about discovered devices to Infoblox. Infobox is one of several Asset Manager integrations that not only pulls data from the integrated application, but also pushes data to it.

Integrated IP Address Managers	**Dashboard**
BlueCat	BlueCat Management Dashboard
Infoblox NIOS DDI	Infoblox Management Dashboard

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.

The dashboard provides these device attributes:

- **Active** - True/False status indicating whether the device responded to a Asset Manager 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 Asset Manager
- **IP Address** - The unique IPv4 or IPv6 device identifier
- **Last Observed** - Timestamp of when the device last responded to a probe from Asset Manager
- **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.

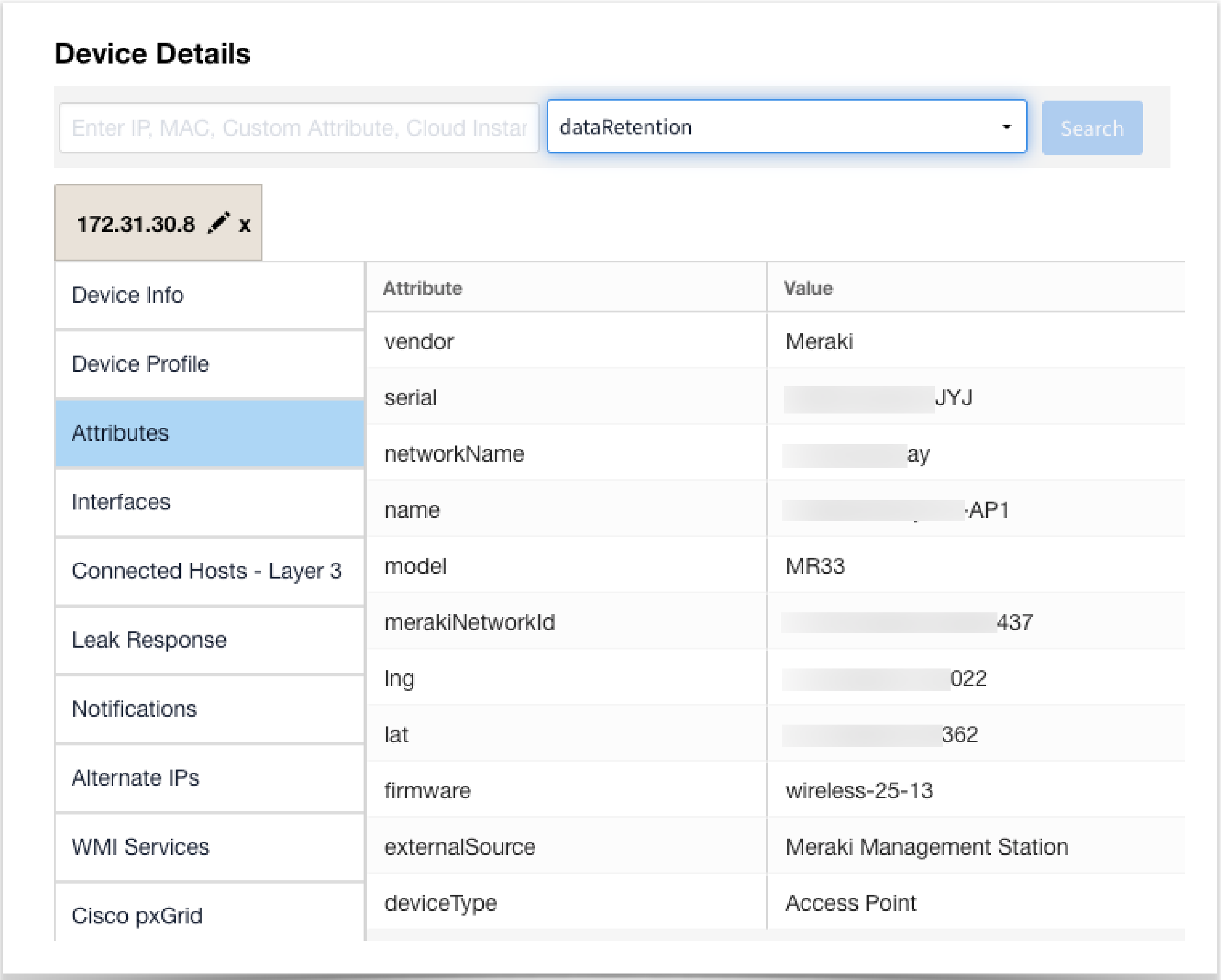
Integrated Network Managers	**Reports**
Cisco Meraki Integration	Reports Introduction

Spotlight on Meraki

Meraki, a subsidiary 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 Asset Manager discovery technique. From Meraki, Asset Manager 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 Asset Manager device details for those devices and displays in Asset Manager analytics.

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

- Network - Including additional L3 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 Asset Manager Device Details.
- Meraki-inflected device fingerprints, identification, and confidence-rankings.
- Meraki-sourced devices and CIDRs can be added to Asset Manager Target List and Asset Manager Eligible List.

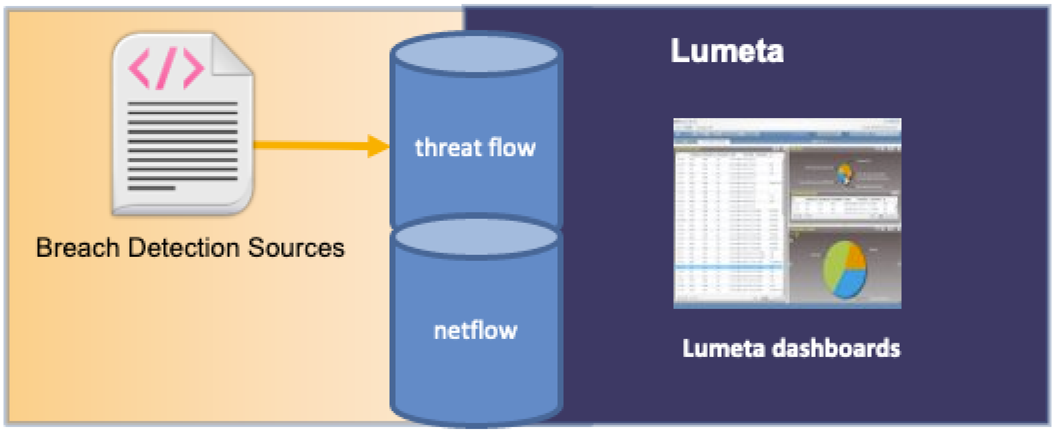


Device Details

Attribute	Value
vendor	Meraki
serial	[redacted]JYJ
networkName	[redacted]ay
name	[redacted]-AP1
model	MR33
merakiNetworkId	[redacted]437
lng	[redacted]022
lat	[redacted]362
firmware	wireless-25-13
externalSource	Meraki Management Station
deviceType	Access Point

Breach Detection Integrations

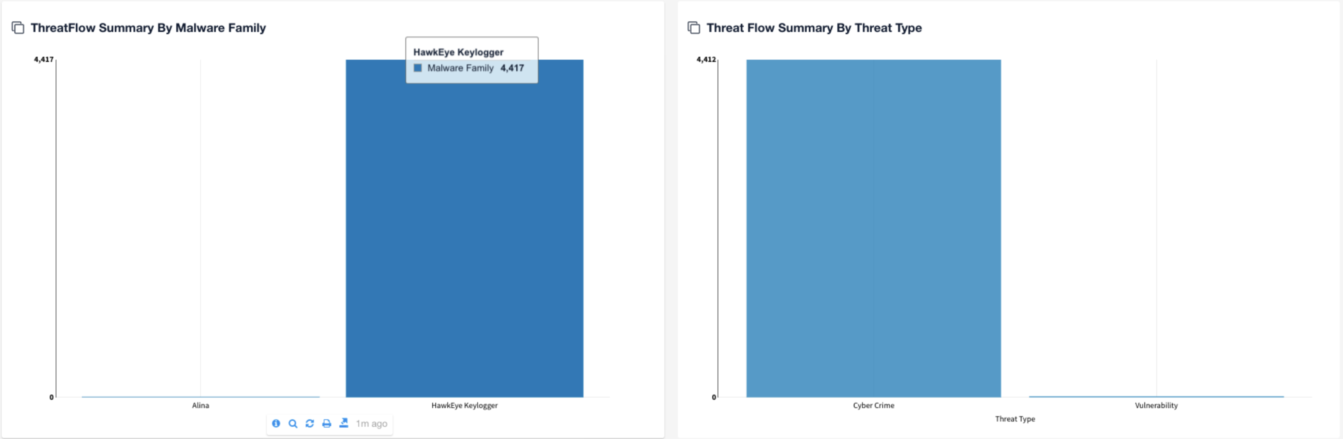
Asset Manager breach-detection integrations find the activity of malware in your network. They identify which devices on your network have been compromised by known bad actors. When you connect a breach detection integration such as iDefense, Asset Manager correlates data from two sources: netflow data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



Integrated Breach Detectors	Dashboard
Proofpoint Emerging Threats	Breach Detection
NetFlow	Breach Detection
iDefense	Breach Detection - iDefense Dashboard
SANS ISC	Breach Detection
TOR	Breach Detection

Spotlight on iDefense

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. Asset Manager 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

Asset Manager 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 Dashboard
Rapid7 InsightVM Integration	Rapid7 Management Dashboard

Spotlight on Security Manager

FireMon offers a complete end-to-end solution for device visibility, firewall clean-up, and compliance reporting using Asset Manager and Security Manager. Attributes of devices Asset Manager 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 Asset Manager-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. Asset Manager highlights missing syslog notifications and supplies it to the partner application.

Integrated Security Stack Managers	Dashboard

Splunk	Asset Manager's Dashboards in Splunk
ServiceNow Integration Overview	ServiceNow Integration Dashboards

Spotlight on Splunk

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

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

- Asset Manager 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.