FireMon Management Dashboard

Now you can share information between Asset Manager and Security Manager (SM) via API and create a group within Security Manager of Asset Manager-discovered devices it does not manage (i.e., non-managed devices in SM). Security Manager refers to devices imported from Asset Manager as "synthetic routers," and includes the data as part of the device's definition.

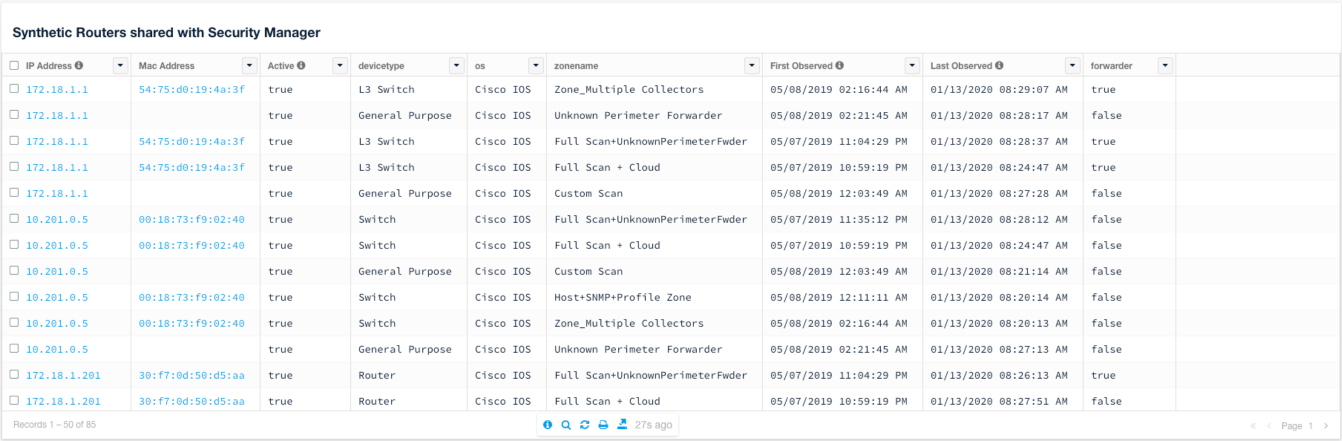
- Information on devices that profile as a unique router, switch or firewall in Asset Manager are fed to Security Manager, provided SM does not already know about the devices.
- Data points like device vendor, operating system, and model are conveyed, along with the description "Discovered by Asset Manager."
- Interface and routing information that Asset Manager discovers along with the device is also transmitted to Security Manager.

To amplify management capabilities, first configure the SIP Integration, and then review the FireMon Management dashboard, located on Asset Manager's Dashboards > Integrations menu.

The Risk Analyzer and Security Manager dashboards are introduced here:

Security Manager

The Synthetic Routers shared with Security Manager table identifies routers, Layer 3 switches and firewalls discovered in real-time by Asset Manager and pushed to Security Manager as "synthetic routers." Only devices that are new or “unknown” to Security Manager are transmitted there automatically. In the context of Security Manager, these newly ingested devices are called "synthetic routers."

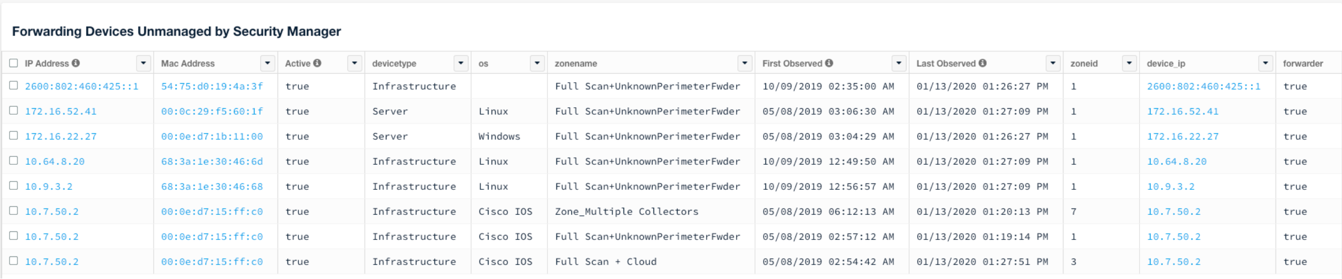


Synthetic Routers shared with Security Manager

☐ IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed	forwarder
☐ 172.18.1.1	54:75:d0:19:4a:3f	true	L3 Switch	Cisco IOS	Zone_Multiple Collectors	05/08/2019 02:16:44 AM	01/13/2020 08:29:07 AM	true
☐ 172.18.1.1		true	General Purpose	Cisco IOS	Unknown Perimeter Forwarder	05/08/2019 02:21:45 AM	01/13/2020 08:28:17 AM	false
☐ 172.18.1.1	54:75:d0:19:4a:3f	true	L3 Switch	Cisco IOS	Full Scan+UnknownPerimeterFwder	05/07/2019 11:04:29 PM	01/13/2020 08:28:37 AM	true
☐ 172.18.1.1	54:75:d0:19:4a:3f	true	L3 Switch	Cisco IOS	Full Scan + Cloud	05/07/2019 10:59:19 PM	01/13/2020 08:24:47 AM	true
☐ 172.18.1.1		true	General Purpose	Cisco IOS	Custom Scan	05/08/2019 12:03:49 AM	01/13/2020 08:27:28 AM	false
☐ 10.201.0.5	00:18:73:f9:02:40	true	Switch	Cisco IOS	Full Scan+UnknownPerimeterFwder	05/07/2019 11:35:12 PM	01/13/2020 08:28:12 AM	false
☐ 10.201.0.5	00:18:73:f9:02:40	true	Switch	Cisco IOS	Full Scan + Cloud	05/07/2019 10:59:19 PM	01/13/2020 08:24:47 AM	false
☐ 10.201.0.5		true	General Purpose	Cisco IOS	Custom Scan	05/08/2019 12:03:49 AM	01/13/2020 08:21:14 AM	false
☐ 10.201.0.5	00:18:73:f9:02:40	true	Switch	Cisco IOS	Host+SNMP+Profile Zone	05/08/2019 12:11:11 AM	01/13/2020 08:20:14 AM	false
☐ 10.201.0.5	00:18:73:f9:02:40	true	Switch	Cisco IOS	Zone_Multiple Collectors	05/08/2019 02:16:44 AM	01/13/2020 08:20:13 AM	false
☐ 10.201.0.5		true	General Purpose	Cisco IOS	Unknown Perimeter Forwarder	05/08/2019 02:21:45 AM	01/13/2020 08:27:13 AM	false
☐ 172.18.1.201	30:f7:0d:50:d5:aa	true	Router	Cisco IOS	Full Scan+UnknownPerimeterFwder	05/07/2019 11:04:29 PM	01/13/2020 08:26:13 AM	true
☐ 172.18.1.201	30:f7:0d:50:d5:aa	true	Router	Cisco IOS	Full Scan + Cloud	05/07/2019 10:59:19 PM	01/13/2020 08:27:51 AM	false

Records 1 – 50 of 85

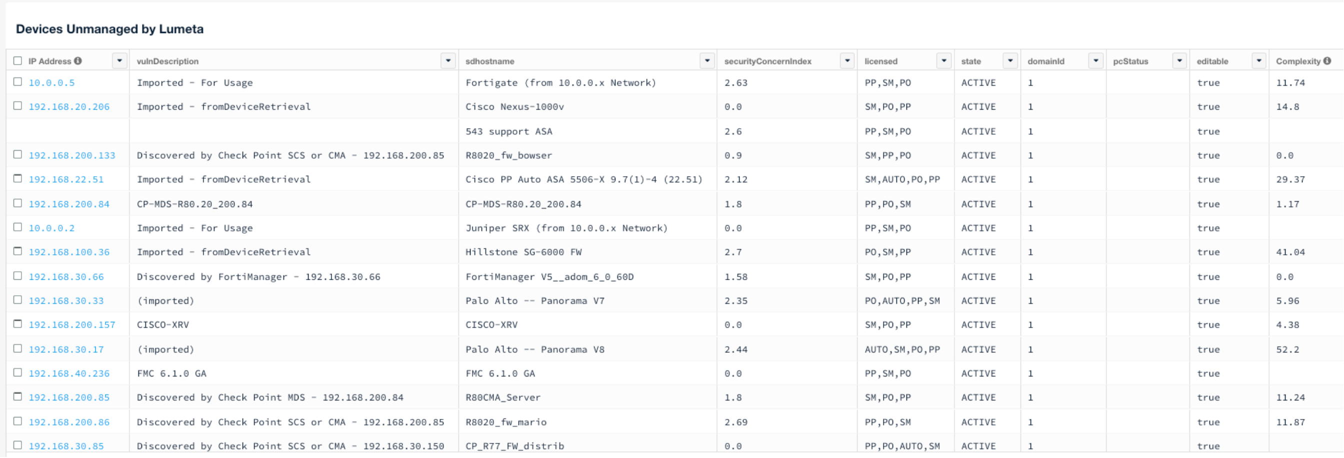
Forwarding Devices Unmanaged by Security Manager are forwarding devices Asset Manager found that do not profile as routers, switches, or firewalls. Asset Manager does not *automatically* push these findings to Security Manager. If the customer wants these findings in Security Manager, they must be added manually.



Forwarding Devices Unmanaged by Security Manager

☐ IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed	zoneid	device_ip	forwarder
☐ 2600:802:460:425::1	54:75:d0:19:4a:3f	true	Infrastructure		Full Scan+UnknownPerimeterFwder	10/09/2019 02:35:00 AM	01/13/2020 01:26:27 PM	1	2600:802:460:425::1	true
☐ 172.16.52.41	00:0c:29:f5:60:1f	true	Server	Linux	Full Scan+UnknownPerimeterFwder	05/08/2019 03:06:30 AM	01/13/2020 01:27:09 PM	1	172.16.52.41	true
☐ 172.16.22.27	00:0e:d7:1b:11:00	true	Server	Windows	Full Scan+UnknownPerimeterFwder	05/08/2019 03:04:29 AM	01/13/2020 01:26:27 PM	1	172.16.22.27	true
☐ 10.64.8.20	68:3a:1e:30:46:6d	true	Infrastructure	Linux	Full Scan+UnknownPerimeterFwder	10/09/2019 12:49:50 AM	01/13/2020 01:27:09 PM	1	10.64.8.20	true
☐ 10.9.3.2	68:3a:1e:30:46:68	true	Infrastructure	Linux	Full Scan+UnknownPerimeterFwder	10/09/2019 12:56:57 AM	01/13/2020 01:27:09 PM	1	10.9.3.2	true
☐ 10.7.50.2	00:0e:d7:15:ff:c0	true	Infrastructure	Cisco IOS	Zone_Multiple Collectors	05/08/2019 06:12:13 AM	01/13/2020 01:20:13 PM	7	10.7.50.2	true
☐ 10.7.50.2	00:0e:d7:15:ff:c0	true	Infrastructure	Cisco IOS	Full Scan+UnknownPerimeterFwder	05/08/2019 02:57:12 AM	01/13/2020 01:19:14 PM	1	10.7.50.2	true
☐ 10.7.50.2	00:0e:d7:15:ff:c0	true	Infrastructure	Cisco IOS	Full Scan + Cloud	05/08/2019 02:54:42 AM	01/13/2020 01:27:51 PM	3	10.7.50.2	true

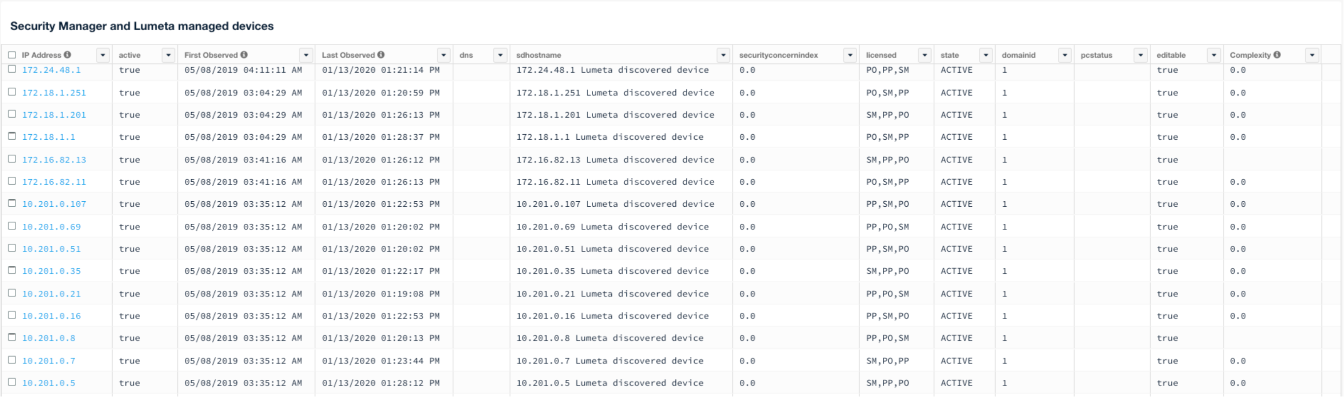
The Devices Unmanaged by Asset Manager are those devices that Asset Manager pulls from Security Manager. Ideally, this table will be empty, indicating that all devices managed by Security Manager have also been indexed by Asset Manager. The presence of records in this widget indicates a lack of visibility: Maybe a firewall is blocking discovery, maybe there’s a misconfiguration, a necessary protocol is missing, or there’s a poorly placed Scout component.



Devices Unmanaged by Lumeta

IP Address	vulnDescription	sdhostname	securityConcernIndex	licensed	state	domainId	pcStatus	editable	Complexity
10.0.0.5	Imported - For Usage	Fortigate (from 10.0.0.x Network)	2.63	PP,SM,PO	ACTIVE	1		true	11.74
192.168.20.206	Imported - fromDeviceRetrieval	Cisco Nexus-1000v	0.0	SM,PO,PP	ACTIVE	1		true	14.8
		543 support ASA	2.6	PP,SM,PO	ACTIVE	1		true	
192.168.200.133	Discovered by Check Point SCS or CMA - 192.168.200.85	R8020_fw_bowser	0.9	SM,PP,PO	ACTIVE	1		true	0.0
192.168.22.51	Imported - fromDeviceRetrieval	Cisco PP Auto ASA 5506-X 9.7(1)-4 (22.51)	2.12	SM,AUTO,PO,PP	ACTIVE	1		true	29.37
192.168.200.84	CP-MDS-R80.20_200.84	CP-MDS-R80.20_200.84	1.8	PP,PO,SM	ACTIVE	1		true	1.17
10.0.0.2	Imported - For Usage	Juniper SRX (from 10.0.0.x Network)	0.0	PP,SM,PO	ACTIVE	1		true	
192.168.100.36	Imported - fromDeviceRetrieval	Hillstone SG-6000 FW	2.7	PO,SM,PP	ACTIVE	1		true	41.04
192.168.30.66	Discovered by FortiManager - 192.168.30.66	FortiManager V5__adom_6_0_60D	1.58	SM,PO,PP	ACTIVE	1		true	0.0
192.168.30.33	(imported)	Palo Alto -- Panorama V7	2.35	PO,AUTO,PP,SM	ACTIVE	1		true	5.96
192.168.200.157	CISCO-XRV	CISCO-XRV	0.0	SM,PO,PP	ACTIVE	1		true	4.38
192.168.30.17	(imported)	Palo Alto -- Panorama V8	2.44	AUTO,SM,PO,PP	ACTIVE	1		true	52.2
192.168.40.236	FMC 6.1.0 GA	FMC 6.1.0 GA	0.0	PP,SM,PO	ACTIVE	1		true	
192.168.200.85	Discovered by Check Point MDS - 192.168.200.84	R80CMA_Server	1.8	SM,PO,PP	ACTIVE	1		true	11.24
192.168.200.86	Discovered by Check Point SCS or CMA - 192.168.200.85	R8020_fw_mario	2.69	PP,PO,SM	ACTIVE	1		true	11.87
192.168.30.85	Discovered by Check Point SCS or CMA - 192.168.30.150	CP_R77_FW_distrib	0.0	PP,PO,AUTO,SM	ACTIVE	1		true	

The final widget—Security Manager *and* Asset Manager-Managed Devices—is the full result of the Asset Manager-Security Manager integration. Devices on a network that both Security Manager *and* Asset Manager know about presented here, indicating that there are "no blind spots" and the customer has "full, visibility and coverage."

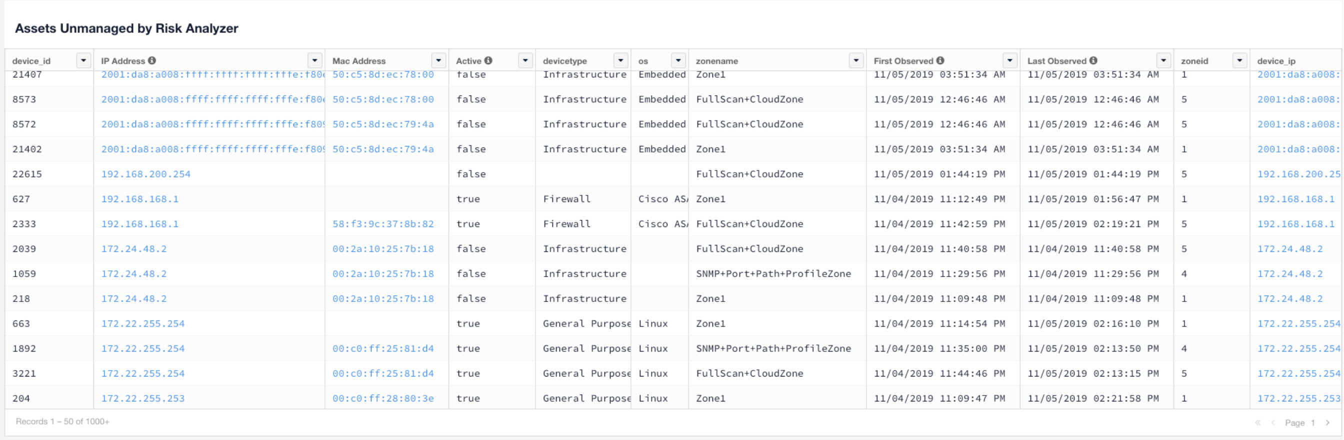


Security Manager and Lumeta managed devices

IP Address	active	First Observed	Last Observed	dns	sdhostname	securityconcernindex	licensed	state	domainid	pcstatus	editable	Complexity
172.24.48.1	true	05/08/2019 04:11:11 AM	01/13/2020 01:21:14 PM		172.24.48.1 Lumeta discovered device	0.0	PO,PP,SM	ACTIVE	1		true	0.0
172.18.1.251	true	05/08/2019 03:04:29 AM	01/13/2020 01:20:59 PM		172.18.1.251 Lumeta discovered device	0.0	PO,SM,PP	ACTIVE	1		true	0.0
172.18.1.201	true	05/08/2019 03:04:29 AM	01/13/2020 01:26:13 PM		172.18.1.201 Lumeta discovered device	0.0	SM,PP,PO	ACTIVE	1		true	0.0
172.18.1.1	true	05/08/2019 03:04:29 AM	01/13/2020 01:28:37 PM		172.18.1.1 Lumeta discovered device	0.0	PO,SM,PP	ACTIVE	1		true	0.0
172.16.82.13	true	05/08/2019 03:41:16 AM	01/13/2020 01:26:12 PM		172.16.82.13 Lumeta discovered device	0.0	SM,PP,PO	ACTIVE	1		true	
172.16.82.11	true	05/08/2019 03:41:16 AM	01/13/2020 01:26:13 PM		172.16.82.11 Lumeta discovered device	0.0	PO,SM,PP	ACTIVE	1		true	0.0
10.201.0.107	true	05/08/2019 03:35:12 AM	01/13/2020 01:22:53 PM		10.201.0.107 Lumeta discovered device	0.0	PP,SM,PO	ACTIVE	1		true	0.0
10.201.0.69	true	05/08/2019 03:35:12 AM	01/13/2020 01:20:02 PM		10.201.0.69 Lumeta discovered device	0.0	PP,PO,SM	ACTIVE	1		true	0.0
10.201.0.51	true	05/08/2019 03:35:12 AM	01/13/2020 01:20:02 PM		10.201.0.51 Lumeta discovered device	0.0	PP,SM,PO	ACTIVE	1		true	0.0
10.201.0.35	true	05/08/2019 03:35:12 AM	01/13/2020 01:22:17 PM		10.201.0.35 Lumeta discovered device	0.0	SM,PP,PO	ACTIVE	1		true	0.0
10.201.0.21	true	05/08/2019 03:35:12 AM	01/13/2020 01:19:08 PM		10.201.0.21 Lumeta discovered device	0.0	PP,PO,SM	ACTIVE	1		true	0.0
10.201.0.16	true	05/08/2019 03:35:12 AM	01/13/2020 01:22:53 PM		10.201.0.16 Lumeta discovered device	0.0	PP,SM,PO	ACTIVE	1		true	0.0
10.201.0.8	true	05/08/2019 03:35:12 AM	01/13/2020 01:20:13 PM		10.201.0.8 Lumeta discovered device	0.0	PP,PO,SM	ACTIVE	1		true	
10.201.0.7	true	05/08/2019 03:35:12 AM	01/13/2020 01:23:44 PM		10.201.0.7 Lumeta discovered device	0.0	SM,PO,PP	ACTIVE	1		true	0.0
10.201.0.5	true	05/08/2019 03:35:12 AM	01/13/2020 01:28:12 PM		10.201.0.5 Lumeta discovered device	0.0	SM,PP,PO	ACTIVE	1		true	0.0

Risk Analyzer

The top set of dashboard widgets shows assets Asset Manager knows about, but Risk Analyzer does not. This means that SIP is not defending the assets listed in the Assets Unmanaged by Risk Analyzer widget. Consider exporting these from Asset Manager, and importing them to Risk Analyzer to complete its coverage.



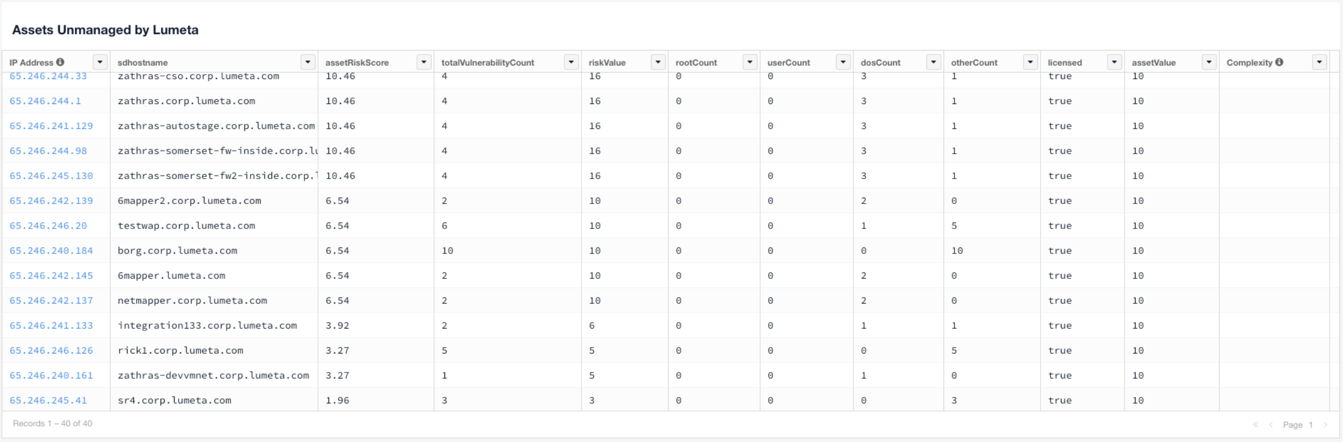
Assets Unmanaged by Risk Analyzer

device_id	IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed	zoneid	device_ip
21407	2001:da8:a008:ffff:ffff:ffff:fffe:f80	50:c5:8d:ec:78:00	false	Infrastructure	Embedded	Zone1	11/05/2019 03:51:34 AM	11/05/2019 03:51:34 AM	1	2001:da8:a008:
8573	2001:da8:a008:ffff:ffff:ffff:fffe:f80	50:c5:8d:ec:78:00	false	Infrastructure	Embedded	FullScan+CloudZone	11/05/2019 12:46:46 AM	11/05/2019 12:46:46 AM	5	2001:da8:a008:
8572	2001:da8:a008:ffff:ffff:ffff:fffe:f80	50:c5:8d:ec:79:4a	false	Infrastructure	Embedded	FullScan+CloudZone	11/05/2019 12:46:46 AM	11/05/2019 12:46:46 AM	5	2001:da8:a008:
21402	2001:da8:a008:ffff:ffff:ffff:fffe:f80	50:c5:8d:ec:79:4a	false	Infrastructure	Embedded	Zone1	11/05/2019 03:51:34 AM	11/05/2019 03:51:34 AM	1	2001:da8:a008:
22615	192.168.200.254		false			FullScan+CloudZone	11/05/2019 01:44:19 PM	11/05/2019 01:44:19 PM	5	192.168.200.25
627	192.168.168.1		true	Firewall	Cisco AS	Zone1	11/04/2019 11:12:49 PM	11/05/2019 01:56:47 PM	1	192.168.168.1
2333	192.168.168.1	58:f3:9c:37:8b:82	true	Firewall	Cisco AS	FullScan+CloudZone	11/04/2019 11:42:59 PM	11/05/2019 02:19:21 PM	5	192.168.168.1
2039	172.24.48.2	00:2a:10:25:7b:18	false	Infrastructure		FullScan+CloudZone	11/04/2019 11:40:58 PM	11/04/2019 11:40:58 PM	5	172.24.48.2
1059	172.24.48.2	00:2a:10:25:7b:18	false	Infrastructure		SNMP+Port+Path+ProfileZone	11/04/2019 11:29:56 PM	11/04/2019 11:29:56 PM	4	172.24.48.2
218	172.24.48.2	00:2a:10:25:7b:18	false	Infrastructure		Zone1	11/04/2019 11:09:48 PM	11/04/2019 11:09:48 PM	1	172.24.48.2
663	172.22.255.254		true	General Purpose	Linux	Zone1	11/04/2019 11:14:54 PM	11/05/2019 02:16:10 PM	1	172.22.255.254
1892	172.22.255.254	00:c0:ff:25:81:d4	true	General Purpose	Linux	SNMP+Port+Path+ProfileZone	11/04/2019 11:35:00 PM	11/05/2019 02:13:50 PM	4	172.22.255.254
3221	172.22.255.254	00:c0:ff:25:81:d4	true	General Purpose	Linux	FullScan+CloudZone	11/04/2019 11:44:46 PM	11/05/2019 02:13:15 PM	5	172.22.255.254
204	172.22.255.253	00:c0:ff:28:80:3e	true	General Purpose	Linux	Zone1	11/04/2019 11:09:47 PM	11/05/2019 02:21:58 PM	1	172.22.255.253

Records 1 – 50 of 1000+

« ‹ Page 1 ›

Asset Manager cannot "see" the assets listed on the Assets Unmanaged by Asset Manager widget. This indicates that your Scouts cannot "see" into the network on which they are located. Check your Scout deployment. Perhaps the device is off-network. This set presents devices Risk Analyzer knows about, yet Asset Manager does not.

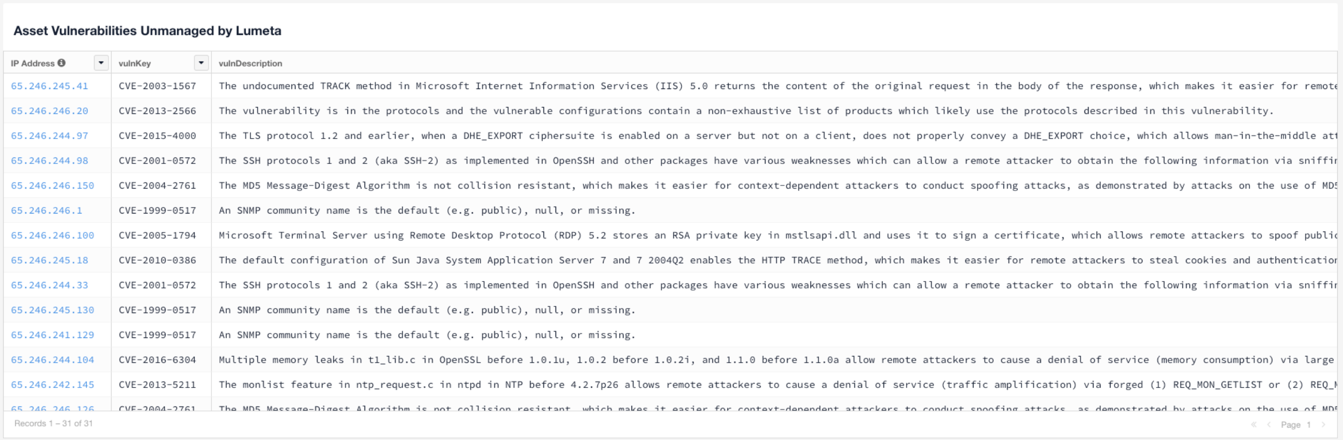


Assets Unmanaged by Lumeta

IP Address	sdhostname	assetRiskScore	totalVulnerabilityCount	riskValue	rootCount	userCount	dosCount	otherCount	licensed	assetValue	Complexity
65.246.244.33	zathras-cso.corp.lumeta.com	10.46	4	16	0	0	3	1	true	10	
65.246.244.1	zathras.corp.lumeta.com	10.46	4	16	0	0	3	1	true	10	
65.246.241.129	zathras-autostage.corp.lumeta.com	10.46	4	16	0	0	3	1	true	10	
65.246.244.98	zathras-somerset-fw-inside.corp.lu	10.46	4	16	0	0	3	1	true	10	
65.246.245.130	zathras-somerset-fw2-inside.corp.l	10.46	4	16	0	0	3	1	true	10	
65.246.242.139	6mapper2.corp.lumeta.com	6.54	2	10	0	0	2	0	true	10	
65.246.246.20	testwap.corp.lumeta.com	6.54	6	10	0	0	1	5	true	10	
65.246.240.184	borg.corp.lumeta.com	6.54	10	10	0	0	0	10	true	10	
65.246.242.145	6mapper.lumeta.com	6.54	2	10	0	0	2	0	true	10	
65.246.242.137	netmapper.corp.lumeta.com	6.54	2	10	0	0	2	0	true	10	
65.246.241.133	integration133.corp.lumeta.com	3.92	2	6	0	0	1	1	true	10	
65.246.246.126	rick1.corp.lumeta.com	3.27	5	5	0	0	0	5	true	10	
65.246.240.161	zathras-devvmnet.corp.lumeta.com	3.27	1	5	0	0	1	0	true	10	
65.246.245.41	sr4.corp.lumeta.com	1.96	3	3	0	0	0	3	true	10	

Records 1 – 40 of 40

This set presents asset vulnerabilities Risk Analyzer knows about, yet Asset Manager does not.

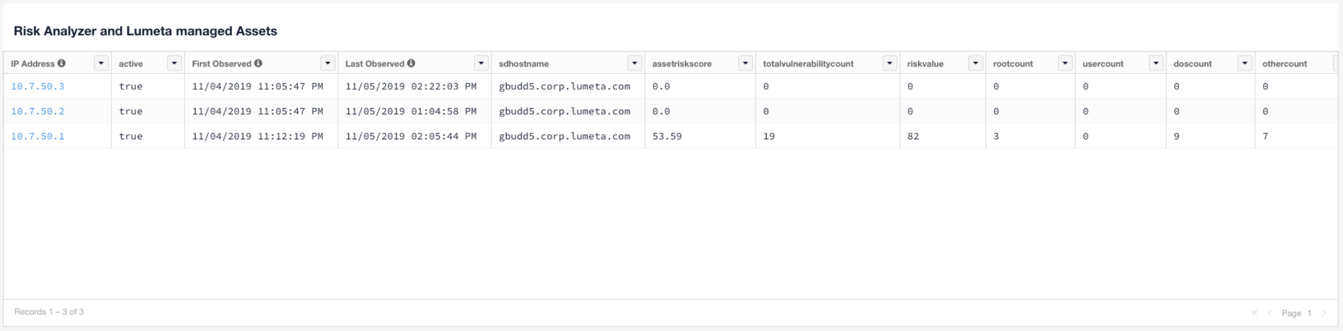


Asset Vulnerabilities Unmanaged by Lumeta

IP Address	vulnKey	vulnDescription
65.246.245.41	CVE-2003-1567	The undocumented TRACK method in Microsoft Internet Information Services (IIS) 5.0 returns the content of the original request in the body of the response, which makes it easier for remote
65.246.246.20	CVE-2013-2566	The vulnerability is in the protocols and the vulnerable configurations contain a non-exhaustive list of products which likely use the protocols described in this vulnerability.
65.246.244.97	CVE-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle att
65.246.244.98	CVE-2001-0572	The SSH protocols 1 and 2 (aka SSH-2) as implemented in OpenSSH and other packages have various weaknesses which can allow a remote attacker to obtain the following information via sniffin
65.246.246.150	CVE-2004-2761	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5
65.246.246.1	CVE-1999-0517	An SNMP community name is the default (e.g. public), null, or missing.
65.246.246.100	CVE-2005-1794	Microsoft Terminal Server using Remote Desktop Protocol (RDP) 5.2 stores an RSA private key in mstlsapi.dll and uses it to sign a certificate, which allows remote attackers to spoof public
65.246.245.18	CVE-2010-0386	The default configuration of Sun Java System Application Server 7 and 7 2004Q2 enables the HTTP TRACE method, which makes it easier for remote attackers to steal cookies and authentication
65.246.244.33	CVE-2001-0572	The SSH protocols 1 and 2 (aka SSH-2) as implemented in OpenSSH and other packages have various weaknesses which can allow a remote attacker to obtain the following information via sniffin
65.246.245.130	CVE-1999-0517	An SNMP community name is the default (e.g. public), null, or missing.
65.246.241.129	CVE-1999-0517	An SNMP community name is the default (e.g. public), null, or missing.
65.246.244.104	CVE-2016-6304	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large
65.246.242.145	CVE-2013-5211	The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_M
65.246.246.126	CVE-2004-2761	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5

Records 1 – 31 of 31

These panels will show any assets managed by both Asset Manager and Risk Analyzer.



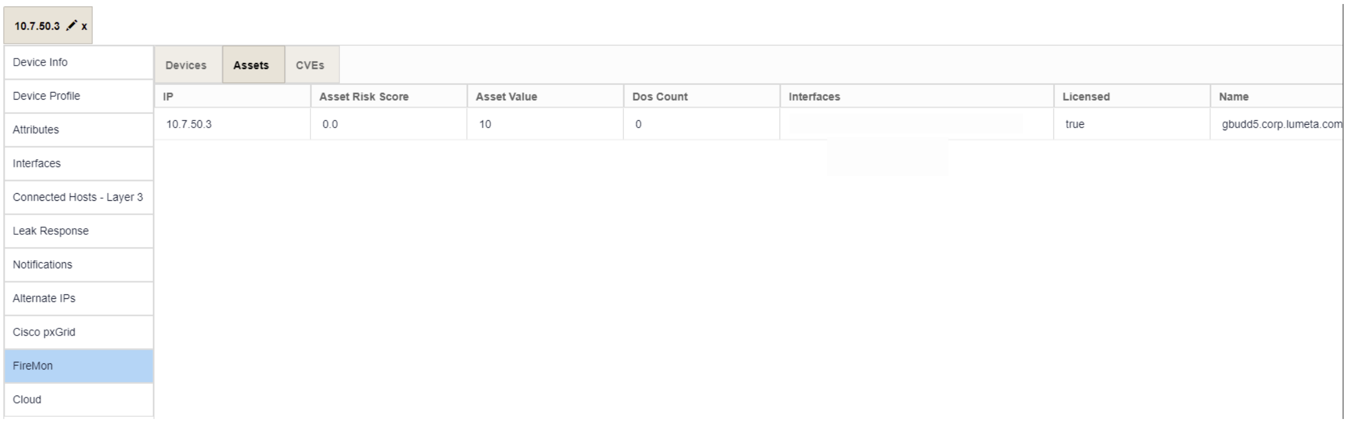
Risk Analyzer and Lumeta managed Assets

IP Address	active	First Observed	Last Observed	sdhostname	assetriskscore	totalvulnerabilitycount	riskvalue	rootcount	usercount	doscount	othercount
10.7.50.3	true	11/04/2019 11:05:47 PM	11/05/2019 02:22:03 PM	gbudd5.corp.lumeta.com	0.0	0	0	0	0	0	0
10.7.50.2	true	11/04/2019 11:05:47 PM	11/05/2019 01:04:58 PM	gbudd5.corp.lumeta.com	0.0	0	0	0	0	0	0
10.7.50.1	true	11/04/2019 11:12:19 PM	11/05/2019 02:05:44 PM	gbudd5.corp.lumeta.com	53.59	19	82	3	0	9	7

Records 1 – 3 of 3

SIP Device Details

The risk score, asset values and other device details associated with SIP-managed devices.



IP	Asset Risk Score	Asset Value	Dos Count	Interfaces	Licensed	Name
10.7.50.3	0.0	10	0		true	gbudd5.corp.lumeta.com