Lumeta Leak Discovery + Security Manager

Organizations cannot manage or patch devices that have not been detected. And a lack of network visibility means devices go undetected and are unknown, leak paths go unchecked, and the environment is likely compromised by policy and segmentation violations.

This application note describes FireMon's end-to-end solution for leak path detection, firewall clean-up, and compliance reporting using the Lumeta Leak Discovery feature and FireMon Security Manager.

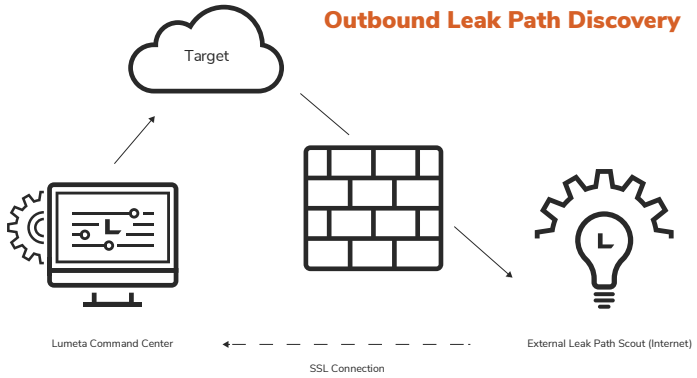
What is a Leak and Leak Discovery

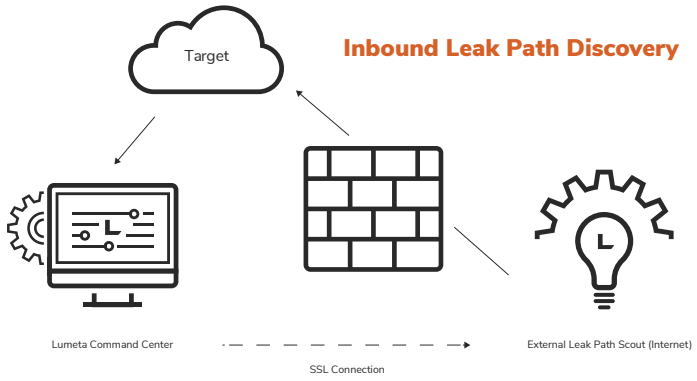
A ***leak*** is an unauthorized inbound or outbound connection route to the internet or to sub-networks. A leak goes through the network perimeter or between secure zones. For example, it may take the form of an unsecured forwarding device exposed to the internet, or it could manifest as a forgotten open link to a former business partner. Leak paths can be especially difficult to detect in cloud environments, where there is less network visibility and fewer security controls.

Leak Discovery is Lumeta's indirect method of uncovering potential leak paths in a zone. It identifies Layer 3 stateless connections and reports network devices that were reachable via a particular, prohibited port. Leak Discovery is typically used between internal segments of a network to test the defenses of secure zone configurations to ensure enclaves are secure. It is also used to determine if any of the devices on targeted networks have connectivity to the internet. Leak discovery is capable of spotting leaks in the network infrastructure such as router and firewall configuration issues.

How does Leak Discovery Work?

In Leak Discovery, two Lumeta devices work together to provide spoofed source addresses for leak testing. This process is performed with all discovered IP addresses to determine which hosts are leaking. Specialized markers are used within the discovery packets to ensure that Leak Scouts identify packets involved in Leak Discovery.





Mobile devices that come onto a network only periodically, would be discovered nevertheless in Lumeta's rounds of continuous monitoring and would be included in the scope of Leak Discovery and continuously monitored for risks.

In the event a device is not reachable after three rescan intervals, Lumeta designates it as inactive and removes it from the rounds of Leak Discovery collection.

What's the Process?

Leak Discovery is performed as follows:

1. Position a Leak Scout and its attendant collector within an enclave-of-interest (e.g., inside that zone's firewall). For example, to test for leaks between internal network enclaves, a Lumeta Command Center would be connected to a Leak Scout deployed inside one of the enclaves.

2. Configure Host Discovery and Leak Discovery on Lumeta and let them run.

Leak Discovery leverages Host Discovery as collectors configured to perform Leak Discovery "understand" where to go function by ingesting the results of Host Discovery. A leak collector receives its discovery scope from Host; it does not autonomously target devices. For this reason, Host and Leak Discovery tabs are enabled at this point in the process.

3. Analyze the results.

This would involve determining the direct source of any leak paths found, which is often a misconfigured firewall. It would also involve validating that the associated forwarding and filtering devices' vulnerabilities are benign in nature and not a violation of your company's security policies.

Communication Considerations

Communication between a Command Center (CC) and a Scout performing Leak Discovery (aka Leak Scout) takes place over an encrypted SSL connection on TCP port 443, as it does for all Lumeta communications. When the CC needs to communicate with the Leak Scout to deliver an instruction, it creates an HTTPS session over TCP port 443 to the Leak Scout. Once the instruction is executed, the Leak Scout no longer stores the instruction or the data. If there is a firewall between the CC and the Leak Scout, TCP port 443 must be open and return packets must be permitted.

Perimeter Controls and Stateful Inspection

A firewall is designed to block unauthorized network access while permitting authorized communications based on a set of rules and other criteria. Most routers include rudimentary access control lists which in some cases include simple stateful inspection. These perimeter controls should stop leaks from occurring. In addition, firewalls and routing devices can (and should) be used to examine the correct progression of the state of a connection, especially session establishment. In the context of Leak Discovery, Lumeta is specifically requesting the devices being tested (e.g., hosts) to "reply." However, firewalls and other devices tracking a packet's state will not have seen a request, and therefore should drop any replies. In the event stateful inspection is off, misconfigured, or unavailable on the routing device, the device will push the reply packet out to the Leak Scout and this stateless reply will be recorded and returned to the Command Center for reporting. All intermediary devices must cooperate in the communication process to ensure a leak is properly tracked. For example, if a discovery packet is sent to a host and a router is blocking its reply, this host will not be targeted for leak discovery.

Lumeta

Lumeta is a real-time visibility and risk management solution that enables cloud, network, and security teams to find unknown networks, devices, and connections. Through active, passive, and indirect methods, Lumeta uses a unique, patent-pending technology to recursively discover a network's state. Customers gain visibility into their entire infrastructure, including cloud instances and assets, and IPv4/IPv6 connections and devices. Lumeta provides authoritative data about the network and its devices in real-time and at a fine level of granularity. It synthesizes device responses, performs analyses to surface risk, and alerts both systems and people with the power to remediate so they can take action immediately.

Lumeta amplifies the value of asset-, breach-, EDR-, HVM-, alert-, risk- and network-management applications by supplying them with better foundational data. It delivers superior results and superior security intelligence: The broadest reach and most comprehensive network coverage in the industry, authoritative visibility, enterprise-grade user management, and a visual way to grasp the significance of events, trends, security gaps, threats, and misconfigurations. Use it alongside your firewalls and integrate it with your security applications to achieve the full value of your network security ecosystem.

Security Manager

Security Manager provides comprehensive network security policy management for complex hybrid cloud environments. Security Manager's unmatched scalability reduces risk and complexity with single-pane, real-time visibility and control to help enterprises achieve continuous compliance, optimize vulnerability management, and automate with confidence.

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.

Synthetic Routers shared with Security Manager

IP Address	Mac Address	Active	devicetype	os	zonename	First Observed	Last Observed	forwarder
10.13.1.2		true	Router	Cisco IOS	Internal	11/12/2019 10:59:20 AM	01/21/2020 07:02:48 AM	false
10.101.7.47		false	General Purpose	Windows	Internal	11/12/2019 10:57:06 AM	01/14/2020 07:07:07 AM	false
10.101.3.93		false	General Purpose	Windows	Internal	01/10/2020 06:43:55 AM	01/14/2020 07:08:10 AM	false
10.101.16.31		false	Switch		Internal	11/12/2019 10:56:09 AM	01/14/2020 07:16:10 AM	false
10.101.10.121		false	Printer	Embedded JetDirect	Internal	11/12/2019 11:04:12 AM	01/14/2020 07:07:08 AM	false
10.2.1.2		false	Switch	Cisco IOS	Internal	11/12/2019 10:36:40 AM	01/14/2020 07:19:40 AM	false
10.4.0.3		false	Switch	Cisco IOS	Internal	11/12/2019 10:36:40 AM	01/14/2020 06:57:48 AM	false
172.18.1.251		true	Switch	Cisco IOS	Internal	11/12/2019 10:36:40 AM	01/21/2020 07:02:48 AM	false

Results in FireMon Lumeta

The results of Lumeta's integration with Security Manager displays in both Lumeta and in Security Manager. In Lumeta, the **Synthetic Routers Shared with Security Manager** widget reports all routers, Layer 3 switches and firewalls discovered in real-time by Lumeta and pushes them to Security Manager. Devices that are new or "unknown" to Security Manager are transmitted automatically. Once in Security Manager, these newly ingested devices are called "synthetic routers." The devices in this widget have been identified as forwarding devices and have been profiled as infrastructure devices.

The **Forwarding Devices Unmanaged by Security Manager** widget displays the records of forwarding devices Lumeta found that do not profile as routers, switches, or firewalls. An analysis to determine why would typically follow. If the Security Manager admin determines that any or all of these devices should be managed within Security Manager, they are added. Otherwise, they are not. Lumeta deliberately does not push these findings to Security Manager automatically.

The **Devices Unmanaged by Lumeta** are devices Lumeta pulls from Security Manager. Ideally, this table will be empty, indicating that all devices managed by Security Manager have also been indexed by Lumeta. The presence of records in this widget indicates a lack of visibility due to a number of potential factors: a firewall is blocking discovery, there's a misconfiguration, a necessary protocol is missing, or there's a poorly placed Leak Scout component.

Results in FireMon Security Manager

All Lumeta-discovered routers, Layer 3 switches and firewalls that Security Manager did not know about are ingested by Security Manager and labeled "Lumeta-discovered devices." Lumeta must profile a device in order for it to be pushed as a synthetic device. Non-profiled forwarding devices will not be pushed to Security Manager. A description of each device including its type, vendor, and model are provided. You might see, for example, that the device is a Layer 3 switch, the vendor is Cisco, and the model number is 4507. Security Manager also provides interface and route details on the device.

Lumeta-discovered devices are also mapped in Security Manager. Each device that's new to Security Manager is highlighted in blue and all interfaces associated with the device display adjacent to the map. These newly found devices can be associated with a device pack to handle rule compliance and clean-up. A hole in the network map and a lack of understanding in the organization's understanding of their network is eliminated.

By providing real-time visibility through Lumeta, and network security policy management through Security Manager, FireMon enables customers to bring all their previously unknown network infrastructure under management.