One of the biggest detriments to achieving PCI compliance and preventing data loss is the inability to find the unknown, rogue and shadow IT networks, endpoints and various leaks that are more common than most organizations realize. What you don't see is what attackers commonly exploit for a successful breach. Lumeta Spectre also provide real-time visual drill-down mapping, analytics and alerts for the entire infrastructure as it is mapped and even as changes occur.

Opptimize a Vulnerability Management Program

Lumeta Spectre can provide early warning for attackers attempting a breach by identifying anomalous network behaviours common to the majority of attacks, like ransomware through the analysis of the unique real-time network context we gather and monitor to quickly pinpoint at risk areas and prioritize any issues for remediation. Spectre includes the ability to ingest third-party threat intelligence feeds to correlate with the network data collected. Lumeta also works with Qualys and Tenable to provide the most up-to-date asset list of potentially vulnerable systems

Continuous Monitor & Test Networks

Lumeta Spectre indexes all the network elements and any attached endpoints (within minutes of its insertion on the network) and provide immediate alerting via syslog, email or on screen, for a true view of the network - what endpoints are connected to the network, and how what address space is in use supporting of a new business initiative or simply out of human error. Once agains, Lumeta Spectre is the only solution that can find any unknown, unmanaged, rogue or shadow IT networks and connected endpoints that other solutions cannot simply find using traditional network and security discovery and monitoring. This capability is critical to ensure that PCI compliance is being achieved and client data is protected.

Maintain a Robust Information Security Policy

Lumeta Spectre provides real-time cyber situational awareness enabling network and security teams to not only identify all your IP-enabled critical infrastructure but also monitor for changes or unusual behaviors - without installing any agent software - providing early detection for preventing a successful breach supporting security policy creation. Lumeta Spectre is the key central solution to organization's security stack with the ability to ingest and feed information to integration partners' solutions such as Cisco, Infoblox, McAfee, and more.

Lumeta's Alignment with PCI DSS

The PCI DSS defines 12 requirements for securing payment card data within 6 control objectives. Lumeta Spectre plays a significant role in addressing 6 requirements within 4 of the control objectives. The following section details how Spectre addresses specific PCI DSS requirements and sub-requirements within each of the 4 control objectives.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The PCI DSS requires companies that store, process or transmit Primary Account Numbers (PANs) to install and maintain firewall configurations that protect cardholder data. To protect cardholder data, it is essential to document and test connections to and from the cardholder data environment.

Requirement 1.1.1.
Spectre also runs ongoing mapping to verify that the firewalls are restricting traffic as intended and to identify any unknown/unmanaged devices including IoT or connections that are circumventing the firewalls. Spectre provides an automated way to streamline the resource-intensive process of manually examining firewall rule sets to verify compliance all in real-time.

Lumeta Spectre uses a unique "always on" technique to produce an authoritative network summary – a recursive cycle of targeting, indexing, tracing, monitoring, profiling, and displaying a network's state meeting and exceeding **Requirement 1.1.2,** which mandates requiring a current diagram that shows all connections. **Requirement 1.1.5** mandates that a list of services and ports available on a device be documented. Spectre examines all network devices in real-time for active ports in its Host. The results are delivered through web reports, real-time alerts or can be easily exported for use in a vulnerability management system.

To support **Requirement 1.3.2,** Spectre demonstrates the effectiveness of the DMZ by demonstrating that there are no leaking devices inside the network – leaks are unauthorized connectivity to or from the public Internet. Spectre shows leaking devices in both reports and its visual analytics module (interactive mapping).

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
To gather data supporting Requirement 2.1.1, Spectre, in its Service Discovery module, will survey all routing devices for their default SNMP configurations. This allows clients to examine wireless access points for any vendor-supplied default configuration settings.

Spectre produces reports on these devices that provide the IP address of the misconfigured device and the values of those configuration settings.

Maintain an Enhanced Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications
Requirement 6.1 mandates that a process be in place to insure that all devices are up to appropriate patch levels. Lumeta Spectre discovers hosts and devices in real-time on a network that were unknown and therefore unmanaged using multi-protocol discovery. These unknown and unmanaged devices or hosts are usually not under change control and often represent areas of likely vulnerability. By pinpointing these assets and exporting them to common vulnerability management tools, such as those offered by Qualys and Tenable, Lumeta Spectre automates the vulnerability management and remediation processes. Only by discovering a complete set of networks and identifying all connected endpoint sin real-time can an organization be sure that it is properly patching ALL of its connected IP devices including IoT.

Continuously Monitor and Test Networks in Real-Time

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 10 requires an organization to understand network connectivity in order to effectively to track and monitor access to cardholder system resources from inside or outside the organization's network. Lumeta's Spectre mapping reveals knowledge gaps in clients' understanding of how traffic actually flows on the network, and whether hosts have direct visibility to or from the Internet. This can result from a poorly configured security device or a completely unsecured connection. By adding the network perspective, Spectre aligns defense configurations with security policies in real-time protecting cardholder data from attack. In addition, most PCI resources are protected by segmentation policies. Lumeta Spectre, through its comprehensive knowledge of the entire enterprise network, even extending into the cloud, can provide insight into segmentation violations caused by unauthorized activity or misconfigurations that need to be corrected.

Requirement 11: Regularly test security systems and processes

The DSS states that to meet Requirements 11.1 and 11.2, companies must test network connections annually and must run network vulnerability scans at least quarterly. Lumeta Spectre exceeds this requirement with continuous mapping of IP devices on the network, providing an automated means to test network connectivity and identify vulnerabilities as they are created by network connectivity – specifically unauthorized connections to the public Internet (known as "Internet leaks" or "leak paths"). Lumeta maps the entire network using internal and external sensors to detect and report on Internet leaks. Collecting and reporting in real-time providing ongoing security posture of the organization from a network perspective. Spectre provides notification of leaking devices through its reports, alerts, visual analytics (interactive mapping) or an export of the leaking devices' profile data.

Maintain an Information Security Policy Requirement 12: Maintain a policy that addresses information security

Complying with the PCI DSS Requirement 12 requires organizations to establish sound security policies and practices and monitor that they are enforced by the network. By uncovering the complete set of network facts regarding connected assets and the configuration of network defenses, Spectre's output is a critical benchmark for measuring and demonstrating the alignment of PCI DSS policy and, we often find of unauthorized connectivity, unmanaged network assets and an undefined network perimeter. Measuring these risks is critical to the ongoing security posture called for in PCI DSS. Lumeta recommends that organizations establish Network Assurance programs to add the network perspective to system and data security measures. Many of our clients use the Lumeta Network Index (LNI) as a means to measure the effectiveness of policy and controls using a risk scorecard. Lumeta Spectre is the only solution to map the entire network in real-time enabling vastly improved security operations in locating and managing unknown and unmanaged IP devices and leak paths.

LUMETA
DETECT WITH A HIGHER SENSE

LUMETA CORPORATION 300 ATRIUM DRIVE
SUITE 302 SOMERSET NJ 08873 USA +1.732.357.3500

www.lumeta.com