
DATASHEET

# Real-Time Vulnerability Management Across the Entire Enterprise

## Lumeta Spectre and Qualys Integration

Device and network vulnerabilities throughout the enterprise can be targeted for exploitation, which may result in unauthorized entry into a network, exposure of confidential information, violation of privacy provisions, or paralysis of business operations. Not knowing about a vulnerability that actually exists in your network places your networks and endpoints at serious risk.

Most successful attacks are preventable with a properly implemented and effective vulnerability management program. A successful vulnerability management program needs to encompass the entire network – all connections and devices within the network – to provide a comprehensive assessment of the enterprise.

Integration of the Lumeta Spectre cyber situational awareness solution with Qualys Vulnerability Management (VM) brings together comprehensive network visibility and vulnerability scanning, enabling a more complete picture of security posture within an organization's enterprise and, therefore, an improved ability to quickly remediate identified risk.

### HIGHLIGHTS

Lumeta Spectre not only discovers and track 20% to 40% unknown, rogue and shadow IT infrastructure, but also monitor in real-time beyond what any other solution can do by using patented passive and active listening techniques. Lumeta Spectre provides unmatched context into dynamic network elements, endpoints, virtual machines and even cloud-based infrastructure married with threat intelligence to offer Cyber Situational Awareness. Customers that deploy Spectre in conjunction with Qualys VM are able to reduce operational risk and gain control of IP-enabled systems. The combination of Spectre and Qualys provides automated discovery, identification, and protection of network assets that had previously represented security vulnerabilities across a more comprehensive view of the enterprise network.

Lumeta Spectre excels at discovering an organization's connected network space (including hidden and unknown networks and devices), providing a clear definition of the network. Qualys VM excels at detecting vulnerabilities on any device connected to the network. When these two solutions join forces, gaps in vulnerability management coverage are eliminated, allowing an organization to get a true assessment of its security posture.

**The Capabilities and Benefits of the Lumeta-Qualys Integration**

The integration combines the reach of Spectre's network and endpoint discovery with the depth of Qualys' vulnerability scanning of devices to deliver comprehensive vulnerability management. In simple terms, Spectre maps all the residences in a town allowing Qualys VM to go door to door asking questions.

**Step 1: Track Inventory and Categorize Network Assets Extending in the Cloud**

You can't measure risk if you don't know what you have on your network. In order to fix vulnerabilities, you must first understand what assets you have in your network. Discovering an accurate inventory of your assets helps you determine the areas that are most susceptible to attacks.

Spectre gives users the capability to perform a full discovery of your networked assets on a global scale without limitations within even cloud environments, enhancing Qualys VM's vulnerability scanning function. Identifying your inventory and categorizing assets establishes an evaluation baseline.

**Step 2: Scan All of Your Systems to Find Vulnerabilities**
Check hosts (any combination of IP numbers, ranges of IPs, and asset groups) to find any vulnerabilities that may exist on your network.

What should you scan? Hosts and devices that may introduce risk to the enterprise, including Web Servers, SMTP/POP Servers, FTP Servers, Firewalls, Databases, eCommerce, LDAP Servers, Load Balancing Servers, Switches and Hubs, Desktops, Mobile Devices, Virtual Machines, Cloud Instances.

You also need to scan hosts and devices on business partners, in particular those with connections back to your network. Some business regulations require scans for business partners to ensure the confidentiality, integrity, and availability of personally identifiable information – whether for customers, employees, or partners.

**Step 3: Remediate Vulnerabilities**
Eliminate network and endpoint weaknesses that leave your business exposed and at risk. A post-scan report reveals actual vulnerabilities and states what you need to fix in order of priority.

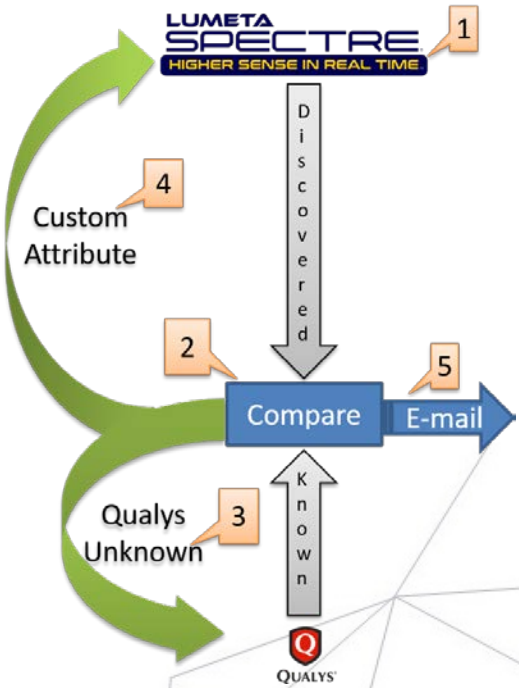
**Step 4: Repeat**
New devices appear constantly on a network in this day of enterprise mobility, Internet of Things (IoT), virtualization and cloud computing. You need to incorporate steps 1-3 in real-time as new devices are attached to the network.

Also, new vulnerabilities appear every day due to flaws in software, faulty configuration of applications and IT gear, and (dare we say it?) good old human error. Whatever their source, vulnerabilities don't go away by themselves. Their detection, removal, and control require comprehensive vulnerability management.

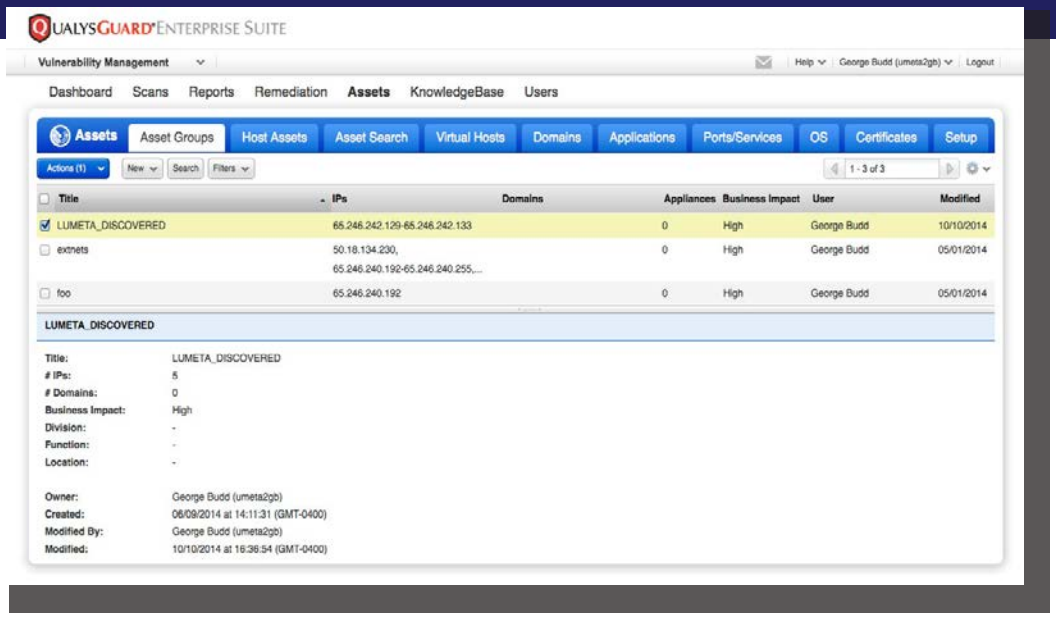
**How Does It Work?**
The Lumeta-Qualys connector gets installed, configured and runs on Spectre, and then connects to a Qualys instance. The connector allows users to compare IPs discovered by Spectre against those known by Qualys VM, creating an asset group in Qualys VM for future scanning.

**The integration between Lumeta Spectre and Qualys VM works as follows:**

1. **User launches an Spectre network discovery with our patented Recursive Network Indexing**
2. **The connector compares IPs discovered by Spectre against known/ subscribed IPs in Qualys VM**
3. **The connector creates an asset group and adds previously unknown IPs in Qualys VM**
4. **The connector tags each IPs within Spectre indicating whether or not it is known/subscribed by Qualys VM**
5. **The connector sends an email alerting users of discovered devices, including those which have been added to Qualys VM asset group**




*Workflow of the integration between Lumeta Spectre and Qualys Vulnerability Management*




*The connector compares IPs discovered by Spectre against known/subscribed IPs in Qualys, and then creates an asset group of previously unknown IPs in Qualys*

### *About Qualys*

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions with over 6,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100.The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications. Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA) and Council on CyberSecurity. For more information, please visit www.qualys.com.

### *About Lumeta Corporation*

Lumeta's cyber situational awareness solutions provide unmatched visibility into networks that even extend into the cloud and connected endpoints. Our ability to discover rogue and shadow networks and endpoints, including VMs even in the darkest corners of an organization's infrastructure is the first piece of the puzzle that sets us apart from the myriad of companies with lots of promises in preventing breaches. When we take that unique level of visibility and combine that with threat intelligence we achieve a new level of what we call Cyber Situational Awareness to help security and network teams identify potential malicious or harmful activity on the network and have the context and intelligence to detect and stop threats before a breach. As part of your overall security program, including protecting endpoints from compromise, Lumeta Spectre is a critical piece for contributing to the success of your security program.

Lumeta optimizes other network and security product investments with accurate and fact-based network intelligence. Headquartered in Somerset, New Jersey, Lumeta has operations throughout the world.