

About Lumeta® and IPsonar®

Lumeta empowers large enterprise and government with global network visibility, allowing clients to understand how network change affects security, availability, and compliance. Lumeta IPsonar® is the industry's only network discovery product which discovers every asset on a network, including assets not currently under management and maps the connectivity between assets and networks to help with issues like Mergers & Acquisitions, IT Compliance, Cybersecurity, Critical Infrastructure Protection, Data Leak Prevention, and Large-scale Network Transformations and Roll-outs.

Lumeta spun out of Bell Labs in 2000 where famed Bell Labs scientists that first mapped the Internet with the technology that was a foundation of IPsonar. As a testament to the product's speed and scalability, we use it every day to map the entire Internet – in just three hours.

Lumeta IPsonar's leading network discovery technology analyzes the connectivity between assets and networks, uncover risk patterns, and automate the enforcement of network policies. Lumeta IPsonar uses active network discovery provides an accurate picture by visualizing every device and path connected to the network -- optimizing vulnerability management and intrusion detection and prevention and enhancing network monitoring and change management processes.

With this level of network assurance, IT organizations can harden security, improve business continuity, and deploy new services without impacting its ability to deliver existing services.



IPsonar Host Topology Visualization

New product module supports stealthy device identification, guest network and extranet security, VLAN compliance and Virtual Machine identification

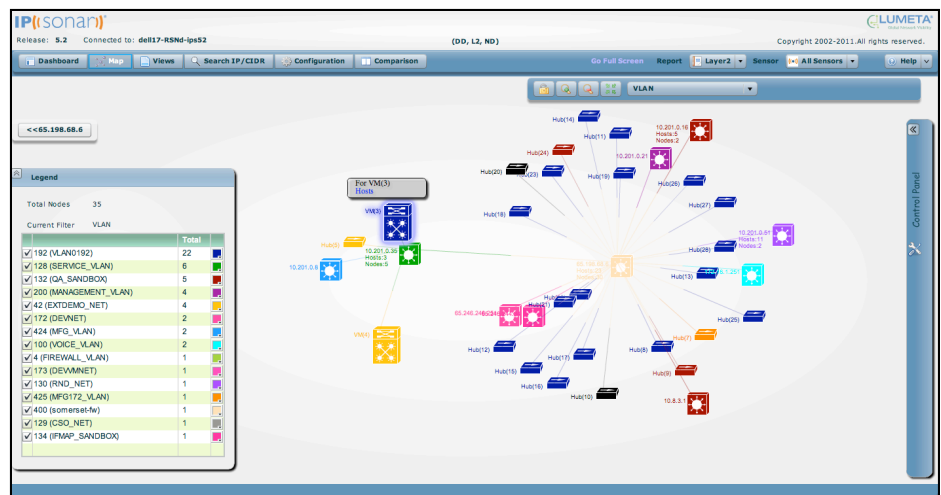
IPsonar's Host Topology Visualization module provides increased visibility into the network and advancing the product's multi-layered active network discovery capabilities. The added module provides a greater layer of drill-down accuracy to IPsonar's network topology visualization, supporting network and data center secure design, VLAN mapping, virtual machines, stealthy device identification, and guest network and extranet security through rich connectivity information.

Network & Data Center Hardening

Because of the exponential growth of IP-connected devices, and the increasing pace at which connectivity is required to change to support the needs of the business, network awareness and visibility has come to the forefront of network security and operations priorities. Cyber security measures to harden the network and data center infrastructures against attack are more important than ever.

Uncover Stealthy Devices

Cyber security measures to harden the network and data center infrastructures against attack are more important than ever. Despite the common evasion or obfuscation techniques used by "stealthy" devices - or those that exhibit forwarding and filtering behavior, and which often go undetected by traditional network monitoring solutions - IPsonar can detect these devices that are routing but do not respond to the typical network probes. The latest version of IPsonar employs Host Topology Visualization to uncover detailed information to identify stealthy devices on the network, enabling proactive network security.



IPsonar's Host Topology Visualization VLAN Mapping & Compliance

Guest Network & Partner Extranet Management

Through its industry-leading correlation of multi-layer active network discovery data, IPsonar defines the true connectivity of the environment based on multiple protocols to ensure accuracy in the device findings. IPsonar's active network discovery is agentless, allowing for easier and faster deployment than agent-based discovery tools. Agentless discovery also gives IPsonar the unique ability to provide visibility into rich device information including device type, vendor, model number, OS version, and more.

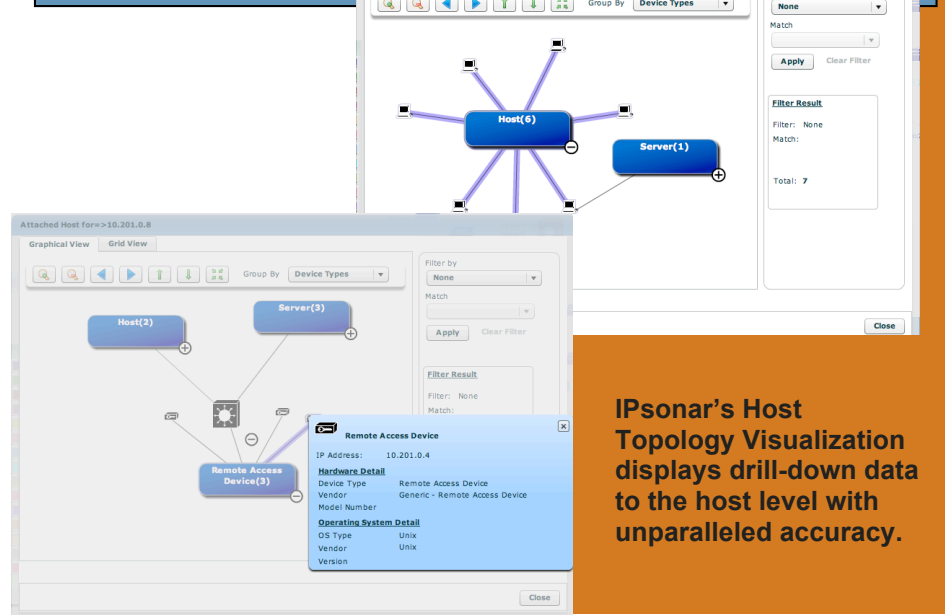
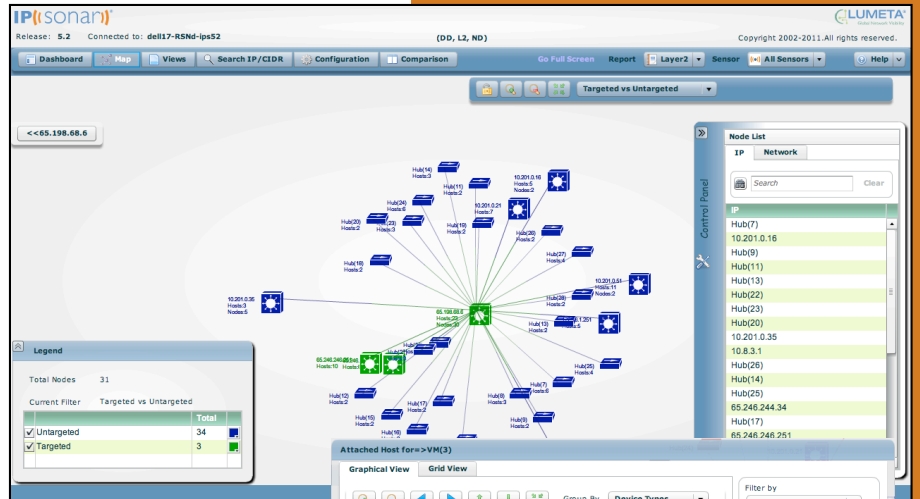
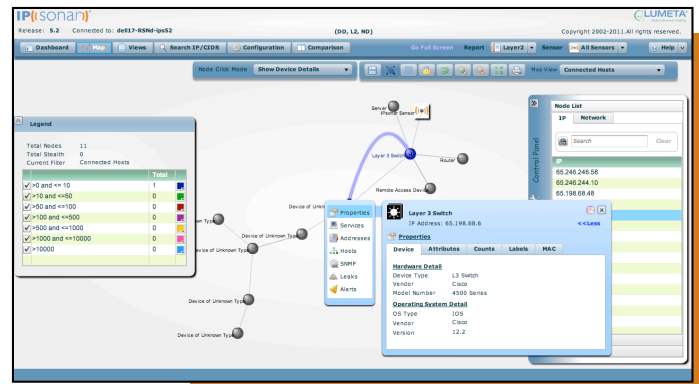
VLAN Mapping & Compliance

IPsonar's Host Topology Visualization module maps virtual local area networks (VLANs) across large enterprise networks. Utilizing VLANs as a method for segregating network traffic is common and cost effective. However, VLAN security is largely dependent on proper segmentation and controls. Therefore, organizations need to verify the configurations and controls in place in order to allay concerns related to VLAN security.

Many regulations and policies have specific security requirements related to VLANs, including the Payment Card Industry Data Security Standard (PCI DSS). Reliance on the simple segmentation of VLANs alone is not robust enough. Adequate security controls will require that traffic is restricted around VLANs carrying customer data, and that wireless networks use separate VLANs. IPsonar's Host Topology Visualization module allows users to map VLANs across the enterprise, providing an active snapshot of VLAN connectivity to verify policy compliance.

Virtual Machine Identification

IPsonar's Host Topology Visualization module also includes Virtual Machine Identification, enabling organizations to discover and monitor relationships between physical devices and virtual machines. Virtual Machine information is intuitively integrated with Layer 3 network information, extending the identification to determine where that physical device exists on the network.



IPsonar's Host Topology Visualization displays drill-down data to the host level with unparalleled accuracy.

Host Topology Visualization expands IPsonar's active discovery and network visibility to meet the current and future needs of our clients. This latest addition continues Lumeta's commitment to comprehensive network situational awareness, addressing new elements of data center and virtual security, as well as expanding the depth of information we gather on connections down to the host level.