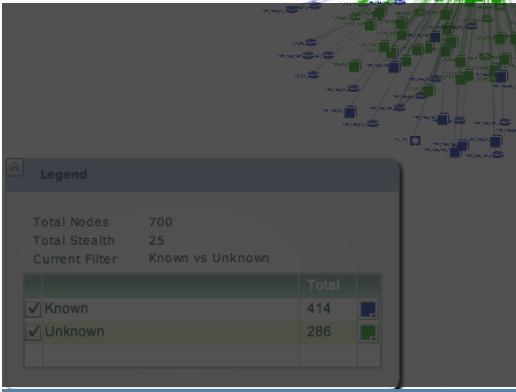


IPsonar

Active Network Discovery for comprehensive visibility of the routed and switched infrastructure. Widely deployed on across the world's largest networks. Time-tested in the most sensitive and geographically distributed organizations.



IPsonar provides visibility into every IP asset, host, node, and connection on the network, performing an active probe and mapping everything that's on the network, resulting in a comprehensive view of the entire routed infrastructure.

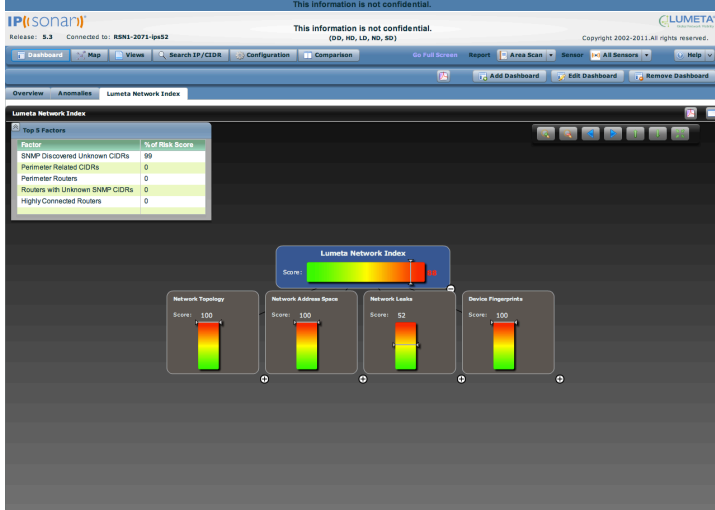
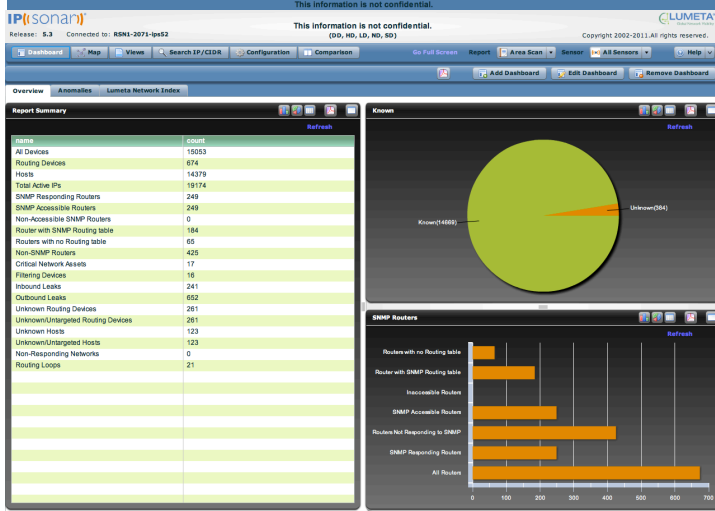
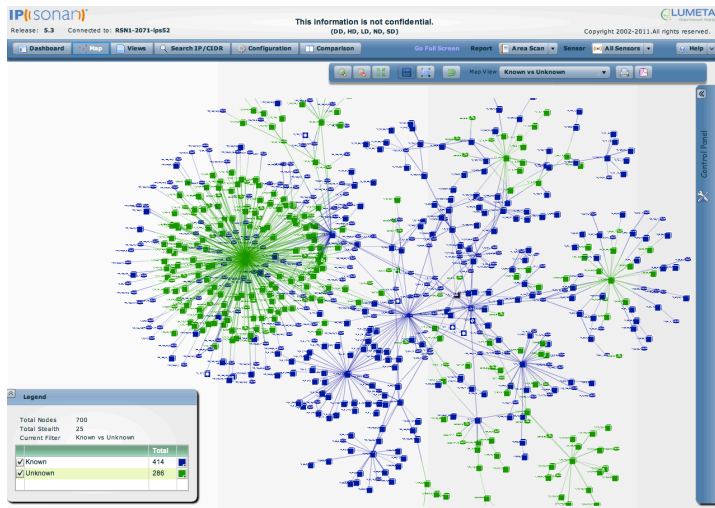
Today's distributed, ever-changing IT environments require complete visibility into the network in order to maintain security, compliance and availability.

Lumeta® IPsonar® is the industry's the most widely deployed network discovery solution for large, geographically distributed organizations. Lumeta's patented, award-winning network assurance technology discovers and maps every IP asset, host and node on the network, giving CIOs, CSOs and CISOs a clear view of risks and policy violations arising from network changes. Such changes include the addition of new devices, modifications in remote access, changes resulting from IT consolidations, and infrastructure updates.

Over a dozen U.S. federal government agencies, five of the ten largest pharmaceutical companies, three of the five largest energy companies, and many other industry-leading organizations rely on Lumeta to maximize the value and efficacy of IT investments in vulnerability management, information protection and control, IP address management, IT asset management, and compliance.

Lumeta's clients rely on IPsonar to:

- Find more of what they need to know with a complete, comprehensive network topology;
- Balance change with security, availability and compliance;
- Measure network risk from a global network perspective;
- Provide an accurate view of what's connected to the network;
- Identify previously unknown devices and internet leaks;
- Validate policy compliance across the enterprise;
- Eliminate gaps between security policy and operational reality; and
- Optimize deployment and enhance the value of IT security and network management tools.



IPsonar’s credential-less and agent-less approach minimizes disruption to operations and scales to handle the largest networks. IPsonar is lightweight and safe for use on large networks even during production hours, operating at the level of network “noise” and using only properly formed packets to elicit benign responses.

IPsonar’s patented network leak detection solution reveals unauthorized connections between the enterprise and another network, between segregated subnets, as well as unwanted connectivity between the network and the Internet, determining whether connectivity is outbound, inbound or both. IPsonar’s network leak detection capabilities are unparalleled in the industry, with the unique ability to find unknown connections into other organizations, such as legacy partner connections or divestiture connectivity. Network leak detection provides intelligence for active network defense, enabling cybersecurity response before costly downtime or material weaknesses wreak havoc on the enterprise.

IPsonar allows users to set policy guidelines based on regulatory requirements or internal guidelines, and to automate the measurement of the true state of the network against those policies. IPsonar also provides real-time alerting on policy violations that break risk thresholds, even where the violation occurs on an asset or connection that was previously unmanaged or unknown, enabling a proactive approach to network security and management.

IPsonar’s powerful dashboards can be configured to present the most relevant data more effectively. For instance, dashboards can be created for IT audit and regulatory preparation or for executive management reporting.

With a bi-directional open API, and configurable custom attributes, Lumeta IPsonar provides users the ability to seamlessly integrate active network discovery data into existing IT and Security lifecycle, leveraging IPsonar’s network discovery reporting and powerful network mapping engines as a front end to operational network visualization.

Lumeta IPsonar is delivered on an appliance-based system, including sensors, scan servers and reporting servers. The number of systems required and licensing costs depends on the size, complexity and segmentation of the network to be scanned. Lumeta IPsonar can also be run as a service. Lumeta offers an extensive suite of professional services, training and educational certifications.

Lumeta IPsonar

Active Network Discovery, Mapping and Leak Detection for Large Distributed, Highly Complex & Sensitive Enterprise Networks

The Phases of IPsonar Discovery

IPsonar actively scans the network to collect all data related Network, Host, Leak, and Device Discovery. Users can accurately visualize what is on the network, drill down to analyze potential areas of risk, and identify appropriate corrective actions.

Network Discovery

Organizations must understand the entire network during times of change, assuring that all assets are under management to avoid intrusion and service outages. For that reason, IPsonar identifies and measures relationships between known and previously unknown network assets, including connections, routers, and firewalls. The solution:

- Applies multi-protocol discovery to penetrate deep into the network, identifying forwarding and filtering devices
- Traces data paths through a network, to see if assets communicate properly
- Flags “stealth” assets that do not respond to queries, pinpointing resources that may not be under management
- Isolates the impact of firewall and router access control lists (ACLs), assuring they are operating in compliance to policy
- Provides a route-based network topology from an application connectivity perspective

Host Discovery

Unknown IP addresses exist in every large network, often undiscovered until an outage, breach, or audit issue. IPsonar reveals all network addresses, helping IT executives align areas of visibility with areas of responsibility. The solution:

- Conducts a census of all IP addresses using multi-protocol discovery, identifying the true perimeter of the network
- Flags addresses unrecognized by official network inventories for remediation
- Enables organizations to harden defenses around the network perimeter and secure zones to enforce policies

Leak Discovery

Leaks are devices with unauthorized inbound or outbound connectivity to the Internet or sub-networks (e.g., unsecured routers exposed to the Internet or open links to former business partners). The more complex a network, the more likely it is that leaks exist. IPsonar is crucial in the proactive fight against leaks, revealing all unauthorized connections and identifying whether access is outbound, inbound, or both. The solution:

- Pinpoints forwarding and filtering devices, enabling IT staff to assure these resources are in compliance with security policies
- Flags inbound and outbound connectivity to secure zones, such as those developed to protect customer data or carry sensitive communications
- Identifies resources a “hop” beyond the network, showing executives to which organizations they are connected

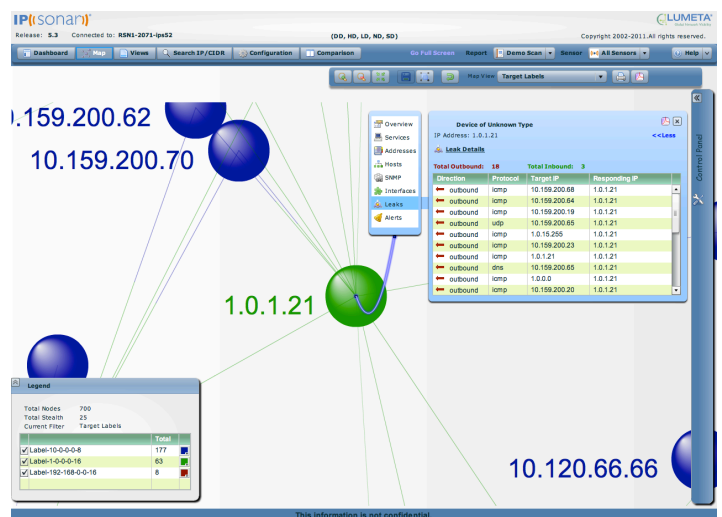
Device Discovery

IPsonar provides rich data on all networked devices, delivering a uniquely comprehensive data set on all devices at the network and transport levels, in addition to providing application-layer visibility. Detailed device information obtained by active network discovery gives users a real-time glimpse into device type information, vendor, model number, OS version, and more all of which can be easily integrated into to other IT and security lifecycle tools, such as network management systems.

The product ships with a pre-configured library of more than 150 vendors, dozens of devices types, and common operating systems and OS versions, all regularly refreshed through a live update feature. Customers can also enhance or customize this library easily to suit their individual infrastructure.

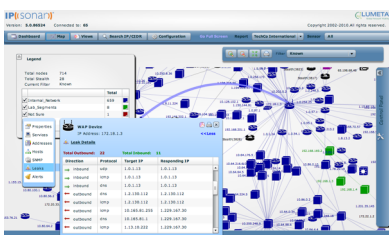
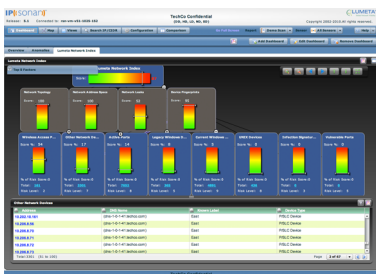
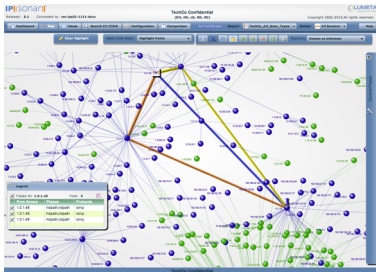
The solution:

- Identifies Internet services and proprietary IP applications active on hosts and devices, pinpointing resources for which tested ports are active
- Flags improperly secured wireless access points for remediation—improving security without requiring staff to scan airwaves or deploy antennae-based monitors
- Determines which operating systems and versions network devices are running
- Extracts information from standard packets (ICMP echo requests and high-port UDP packets); no application-layer transactions
- Facilitates consolidation by noting devices that run network-based services, such as printers and storage appliances



An IPsonar network map showing a device with a number of Outbound and Inbound Network Leaks.

Lumeta offers the industry's most comprehensive and proven network discovery & visibility solutions. Lumeta IPsonar provides comprehensive network visibility for active network defense.



Scalable to the World's Largest Networks with Multi-tier Enterprise Architecture

Because it is a network appliance, Lumeta's IPsonar requires no installation or disruption to operations in order to completely scan a network - no matter how far-flung or numerous the resources are. IPsonar is made to handle large data sets as easily as it does small data sets. Thus, IPsonar is a true enterprise application, able to work efficiently in both large and small deployments.

IPsonar's three-tiered architecture is proven at the world's most complex networks and has been used to scan the entire Internet:

- **Sensors.** Accurate, complete network scanning is achieved through the use of network entry points called Sensors. These entry points are portable, providing flexibility to address even the most fast-changing networks.
- **Scan Servers.** These resources are positioned at appropriate points in the network to assure that business applications and even the lowest-speed network links are unaffected by IPsonar network traffic. Multiple scans can be run simultaneously.
- **Report Servers.** Functioning as the data repository, Report Servers separate report generation from scanning to further reduce IPsonar's operational footprint. A single remote Report Server can support multiple Scan Servers.

IPsonar uses a pre-loaded, hardened configuration to simplify and assure security. Communication between IPsonar appliances is via HTTPS (SSL) and available in several configurations, so no changes to firewalls or network access control are required. The user interface supports signed digital certificates.

The number of systems required, and software-licensing costs depend on the size, complexity and segmentation of the network to be scanned. Lumeta IPsonar can also be run as a service. Lumeta offers an extensive suite of professional services, training and educational certifications.

Integration

With a bi-directional open API, and configurable custom attributes, Lumeta IPsonar provides users the ability to seamlessly integrate active network discovery data into existing IT and Security lifecycle, leveraging IPsonar's network discovery reporting and powerful network mapping engines as a front end to operational network visualization.

Lumeta's IPsonar fully integrates its data into third-party applications, providing organizations with the information needed to ensure complete network availability, security, and compliance. IPsonar's open API is designed to enable integration with any application and the solution's network discovery results are fully extensible to a range of third-party solutions and easily translated into actionable information.

Lumeta Corporation

300 Atrium Drive, 3rd Floor
Somerset, New Jersey 08873

+1.732.357.3500
www.lumeta.com