

**IP**((sonar))<sup>®</sup>



# Global Network Visibility

## Key Benefits

### **Balance compliance and change.**

Periodically monitor compliance to assure new mandates and evolving resources do not compromise compliance efforts. Resolve issues before audits. Create objective reports.

**Maintain service availability.** View the changing network to create project plans that minimize adverse impact to service. Integrate scan results to network management tools, for faster, more accurate problem diagnosis.

**Strengthen security.** Identify and automatically prioritize known and previously unknown security vulnerabilities. Use results to maximize performance of intrusion detection and access management tools. Validate that remedial actions are implemented.

**Validate policy compliance.** Align IT's area of responsibility with its area of network visibility. Scan resources and assure compliance across headquarters, division, remote, and partner networks.

**Unlock savings.** Gain intelligence to plan consolidation and optimization efforts. Pinpoint and remove inefficiencies, such as remnants of divested units or poorly engineered branch networks.



## IPsonar®: Creating Global Network Visibility

Enterprises and government agencies are evolving their networks to improve service levels and reduce costs. Yet even simple network adjustments increase the potential for service outages, security breaches, and compliance violations.

Balancing change with availability, security, and compliance requires comprehensive network visibility based on concrete facts. Armed with this information, IT managers can confidently make the right decisions about network risk and availability. This is network assurance.

IPsonar, Lumeta's flagship network assurance product, is the only technology that provides global network visibility and measures risk from a network perspective. IPsonar maps every asset on a network—including assets not currently under management—to visually analyze the connectivity between assets and networks, uncovering risk patterns and policy weaknesses.

IPsonar extends the value of network management and security investments by prioritizing bottlenecks and vulnerabilities due to poorly configured or previously unknown devices. Thus, issues can be resolved before they result in costly downtime or material weaknesses.

IPsonar is delivered as an appliance to minimize installation overhead, and is built on a robust three-tier enterprise architecture that ensures scanning is efficient and non-intrusive. As a network appliance, IPsonar requires no installation or disruption to operations in order to completely scan a network—no matter how dispersed or numerous the resources are. The solution completes scans typically within 72 hours. Results are fully extensible to other network management and security systems, for example, SIM systems or asset management solutions, so clients can accelerate processes such as vulnerability and change management.

## The Phases of IPsonar Discovery

IPsonar actively scans the network to collect all data related Network, Host, Leak, and Device Fingerprint 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 results. 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
- ▶ Spots hard-to-find leaks such as unauthorized cable/DSL routers, multi-homed servers, and NAT/PAT proxies that covertly forward network traffic



*The same technology used to map the Internet, pictured above, allows the world's most security conscious organizations to measure risk from a global network perspective.*

*“Lumeta has been in production at the bank for several years, and we continue to add licenses as we build out our infrastructure or add devices due to M&A activity. The data and capabilities that Lumeta provides are critical for maintaining the security and integrity of our enterprise network.*

*One of our goals is to keep Wachovia out of the newspapers by ensuring that we do everything we can to protect our customers' data.”*

*– Peter Makohon, VP of Corporate Information Security, Wachovia Corporation*

## Device Fingerprint Discovery

Assessing risk requires more than a census of assets and their interdependencies. To determine whether assets are non-compliant or vulnerable to a specific threat, IT organizations must have fingerprinting capabilities that enable them to understand attributes such as a server's operating system or whether a device or host has a particular service enabled. Both fingerprinting and leak discovery are necessary components to focus patch management efforts on high-risk hosts and devices with direct exposure to the Internet.

IPsonar's fingerprinting capabilities enable the organizations to detect services, wireless access points, and operating system information—without disrupting operations IPsonar:

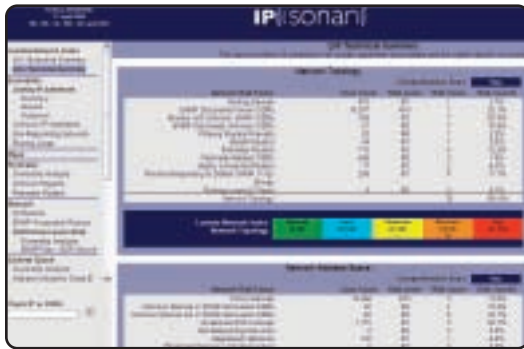
- ▶ Identifies Internet services and proprietary IP applications active on hosts and devices, pinpointing resources for which tested ports are active
- ▶ Flags improperly secured wireless access points for remediation—improving security without requiring staff to scan airwaves or deploy antennae-based monitors
- ▶ Determines which operating systems 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, network-based faxes, and storage appliances
- ▶ Exports details to security tools, optimizing host-level vulnerability assessments and accelerating patch management

## Measuring Risk: The Lumeta Network Index

To quantify and mitigate network risk, organizations require regularly updated visibility into the changing global network with information that results in meaningful and actionable information. IPsonar's Lumeta Network Index (LNI) provides this information through a simple executive scorecard based on analysis of more than 34 variables.

Clients develop a network risk profile, measuring baseline deviations as conditions change. The result is an objective dashboard that provides a clear understanding of network risk based on evolving operational reality. Over time, organizations can easily see whether risk is increasing or decreasing relative to the state of the network.

The LNI also identifies and prioritizes major contributing factors to an organization's risk score, so executives can focus efforts where they will have the greatest impact.



IPsonar offers comprehensive Web-based reports, including an Executive Summary, a technical overview (top), and a set of predefined maps for visual analysis of data (above).

*"To accurately know what's on our network, we needed an intelligent tool capable of mapping our entire network and quantifying risk, and found it with IPsonar. In fact, IPsonar is a key component of our M&A strategy because we're able to instantly assess the impact of network consolidation,"*

— Raymond Ray, Group Infrastructure and Security Manager, Smiths Group



# GLOBAL NETWORK VISIBILITY

*“IPsonar provides enhanced visibility into the previously unknown parts of a company’s network, with a scalability and level of detail distinctive from the auto-discovery capabilities available in the fault- and performance-management products available today.”*

– Dennis Drogseth, Enterprise Management Associates

## IPsonar Administration

Advanced management and security options are built into IPsonar. Optional support for scanning and implementation is provided by the professional services organization.

### Advanced Management Options

- ▶ Schedule Scans (Windowing)
- ▶ Monitor Active Scans
- ▶ Tactical Scans
- ▶ User Management
- ▶ System Management
- ▶ Remote Patch Management

### Advanced Security Options

- ▶ PKI Authentication
- ▶ Security Auditing
- ▶ Secure Session Management
- ▶ Tamper Management
- ▶ Network Time Protocol

## Multi-tier Enterprise Architecture

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 portable entry points provide the flexibility to address even the fastest-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.

## API Integration

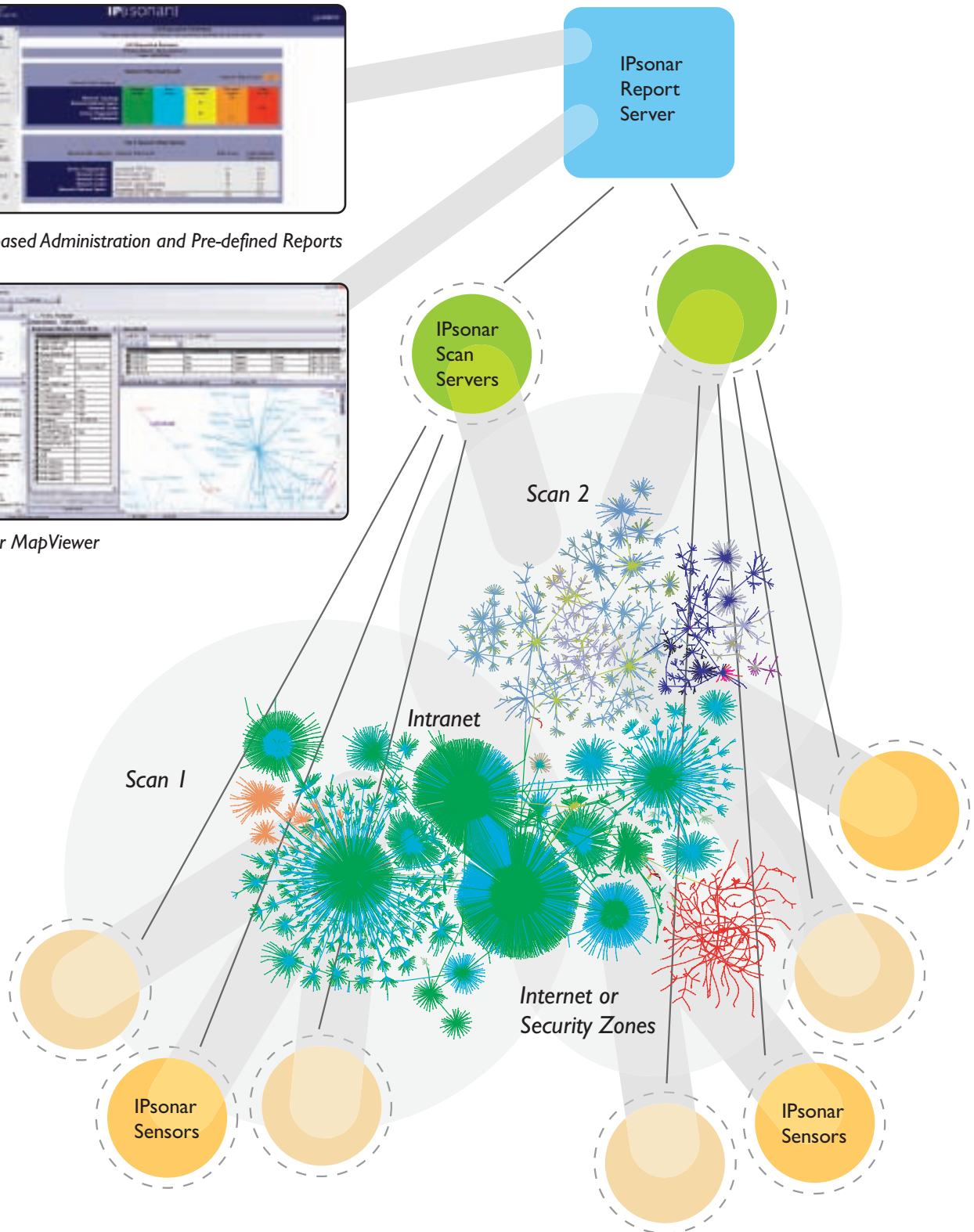
Lumeta understands that organizations have made substantial investments in a variety of network solutions. That is why IPsonar integrates closely with solutions like Foundstone, ArcSite, and Qualis, enabling organizations to leverage their previous investments while discovering information that can help make existing network investments even more efficient. Through public APIs, users can quickly export data about connectivity and possible security or compliance issues and handle them proactively, before they become full-blown problems.



Web-based Administration and Pre-defined Reports



IPsonar MapViewer



IPsonar's multi-tier architecture allows users to conduct multiple simultaneous scans across a complex network. Portable entry points, known as IPsonar sensors, can be flexibly deployed at various points on the network to facilitate efficient network discovery. These sensors forward network information to IPsonar scan servers, which synthesize distributed scan data for reporting. The IPsonar report server correlates scan data for presentation to the end user.

## About Lumeta Corporation

Lumeta empowers large enterprise and government agencies with global network visibility, allowing them to understand how network change affects security, availability, and compliance.

Lumeta's IPsonar is the industry's only network assurance solution that discovers and maps every asset on a network, including assets not currently under management. This capability enables IT professionals to analyze the connectivity between assets and networks, uncover risk patterns, and automate the enforcement of network policies.

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.

For more information about how Lumeta can help you secure your network in the face of change, please email [info@lumeta.com](mailto:info@lumeta.com) or call +1.732.357.3500

[www.lumeta.com/ipsonar](http://www.lumeta.com/ipsonar)



Corporate Headquarters  
220 Davidson Avenue  
Somerset, NJ 08873

PHONE 732.357.3500  
866.LUMETA7 (586.3827)

FAX 732.564.0731

US Federal Headquarters  
8260 Greensboro Drive  
Suite 425  
McLean, VA 22102

PHONE 866.LUMETA7 (586.3827)

European Headquarters  
New Broad Street House  
35 New Broad Street  
London EC2M 1NH  
United Kingdom

PHONE +44 (0) 207.194.8040