

Key Benefits

Ease of use.

IPsonar® features an open API which allows organizations to create simple or complex queries against the IPsonar database with minimal implementation time.

Unrivaled flexibility.

The unique data IPsonar discovers can be integrated with any application, such as asset management, network management, and inventory management solutions.

Automated management.

Lumeta IPsonar's API enables users to initiate scans and run reports remotely, automating network management and security processes.

Extensive querying capabilities.

IPsonar's API enables a wide range of queries, resulting in the quick and efficient collection of volumes of data, such as hundreds of thousands of IP addresses.

Simplified troubleshooting.

Trouble tickets can be generated based on scan data, with a follow-on scan automated to ensure proper remediation.

Greater data processing capabilities.

IPsonar's API allows organizations to pipe-line requests – one query can be created, while another is being processed and a third is being analyzed.

IPsonar: Open Integration to Optimize Discovery for the IT lifecycle

An organization's security posture can be impacted by a plethora of variables – unauthorized network connections, ineffective security controls, infrastructure modifications, unmanaged network devices – the list goes on and on. In an effort to combat such threats and obtain true network security, organizations typically implement a range of security and network management solutions from multiple vendors. While these point solutions can be effective in delivering one piece of the overall network security picture, organizations today require a comprehensive, integrated network defense solution in order to effectively mitigate risks.

Lumeta understands that organizations have made substantial investments in a variety of network solutions. Lumeta IPsonar closely integrates with solutions enabling organizations to leverage their existing investments while discovering information that can help make current network investments even more valuable.

IPsonar fully integrates its data into applications, such as Host Vulnerability Management tools and Network Management platforms, providing the world's most security-conscious organizations with the data needed ensure comprehensive network availability, security and compliance. The product's open API gives organizations the flexibility to quickly aggregate, associate and export real-time information for a more holistic and comprehensive security approach. Partner organizations can deliver a more powerful solution to customers by leveraging this open API – providing organizations with choice and control about how to efficiently and cost-effectively support end-to-end security needs.

Leveraging IPsonar's Visibility to Meet Customers' Needs

IPsonar's automated network discovery capabilities allow organizations to quickly discover information to make existing network investments more efficient and secure, and by exporting data through IPsonar's API, organizations can take that a step further and better utilize network solutions organization-wide.

IPsonar API helps partner organizations bridge the gap between provided information and the true state of the network, resulting in comprehensive solutions that extend a partner's ability to:

- ▶ Manage and assess risks related to network changes
- ▶ Optimize IT processes
- ▶ Ensure a secure infrastructure
- ▶ Implement new technologies, reliably and cost-effectively

Proven Integration

IPsonar's open API integrates with any network management or network security application and the product's network scan results are completely extensible to a range of third-party solutions that benefit:

- ▶ Systems Integrators and Service providers: Identifies and measures relationships about unknown assets that need to be managed, including connections, routers and firewalls
- ▶ Security Management vendors: IPsonar identifies and prioritizes known and unknown security vulnerabilities to maximize performance of intrusion detection tools and validate that remedial actions are implemented.
- ▶ Network Management vendors: IPsonar provides an accurate view of the changing network to help maintain service availability and enable faster, more accurate problem diagnosis.
- ▶ Asset Management vendors: IPsonar creates an accurate baseline of network assets, providing visibility into all managed and unmanaged network changes to maximize access management tools.

IPsonar: Open API Results in Intelligent Actions

IPsonar's open API is designed to enable integration with any application that would value from leveraging the product's network visibility, whether at a macro- or micro-level. The API provides organizations with a straightforward, simple way to translate IPsonar's extensive network data into actionable information.

IPsonar supports a new SOAP API – Open API – which makes it easy for programmers to effectively extract data that can be used by organizations to proactively manage the state of network security and apply security policies and processes to ensure defense-in-depth and compliance.

IPsonar has 13 individual API calls, each of which provide varying levels of granularity and a powerful, yet flexible, mechanism to request a comprehensive set of network facts such as:

Device Details

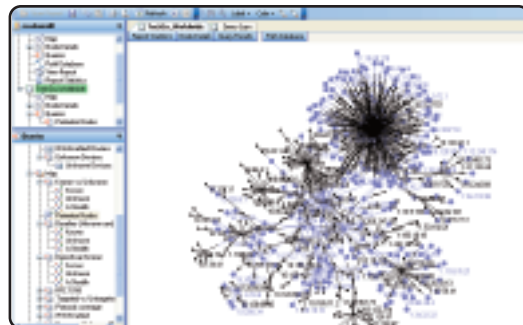
- ▶ Devices with active ports or no active ports
- ▶ Devices with wireless discovery data
- ▶ Devices which are filtering traffic
- ▶ Devices that have an outbound leaking port
- ▶ Devices with a specific OS version

Device-Specific Data

- ▶ Is this device a host?
- ▶ What devices are connected to this device?
- ▶ Is this a known device?
- ▶ Was this device discovered by SNMP?
- ▶ Is the device IPv6 enabled?

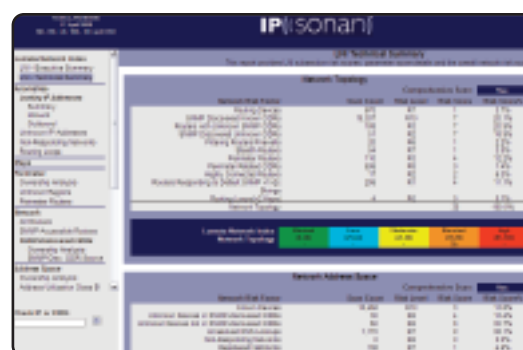
IP Address Data

- ▶ Filtering IP addresses
- ▶ Inbound and outbound leaking IP addresses
- ▶ Inbound and outbound leaking IP addresses by port and protocol
- ▶ Unique inbound and outbound leaking IP addresses
- ▶ IP addresses inactive on port



IPsonar MapViewer Data

- ▶ Users can export specific IPsonar network map data about the operational state of the changing network, such as unauthorized hosts, devices and connections, resource attributes and address space.



Lumeta Network Index

- ▶ Users can query the IPsonar executive scorecard data that analyzes network risk based on 34 variables.

Case Study: Seamless Integration with IF-MAP

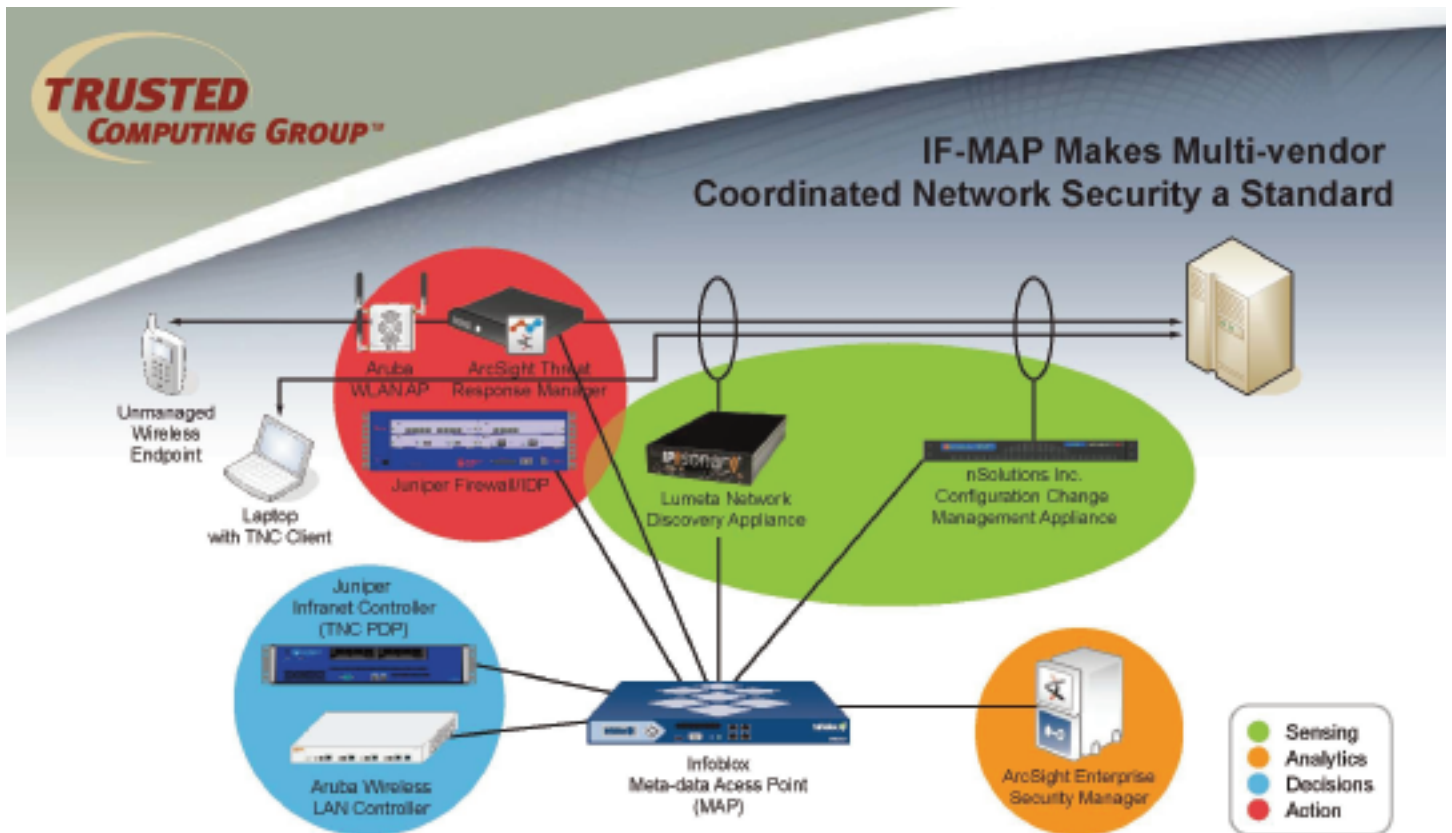
In order for organizations to respond in real-time to changes in security posture, maintain compliance and ensure continuous network service availability, they require in-depth network and security awareness and coordinated defenses among deployed networking and security solutions. To support a standardized, dynamic data exchange among a variety of applications, the Trusted Computing Group (TCG) introduced a powerful new protocol – IF-MAP (Interface for Metadata Access Point) – that enables data about network devices, policies, status, and behavior to be shared in real-time.

A member of TCG, Lumeta participates in its Trusted Network Connect (TNC) work group, which is focused on developing industry specifications that ensure secure interoperability across multi-vendor network security solutions. Lumeta’s IPsonar product supports TNC specifications, including the IF-MAP protocol.

The flexible API allows network administrators and managers to greatly expand the types of requests they can make and, therefore, the type of data they can extract from the IPsonar database.

"No one solution can secure the network; instead, what is required is a variety of solutions and components to continually monitor the network. By enabling the real-time exchange of data among products from multiple vendors, TNC, and specifically the new IF-MAP spec, is helping to enable systems that provide continual, coordinated defense-in-depth at a reasonable cost while enabling vendor choice"

– Stuart Bailey, founder and CTO of Infoblox and Trusted Network Connect work group specification editor



The extracted data can then be exported into any tool, including trouble ticketing, vulnerability, asset management, and inventory management solutions, among others.

Prior to the integration of Lumeta's API with the IF-MAP protocol, data had to be extracted and analyzed by network administrators. The latest version of IPsonar allows administrators to run all scans at predetermined times and the data mined from the scans can then be sent automatically to any number of tools.

Coordinated Network Security

IPsonar's Open API made the product an ideal fit for the IF-MAP protocol, enabling the product's global network visibility data to be automatically integrated with an organization's additional network and security components. As part of an IF-MAP deployment, IPsonar publishes information to the IF-MAP server which has a centralized database for storing information about network security events, devices, users, etc. Once the IF-MAP server receives the data, it automatically shares the information with other applications that leverage that data to coordinate security responses.

For example, IPsonar publishes information to the IF-MAP server about a leaking IP address. A Network Access Control solution would then subscribe to the IF-MAP server to learn about this network vulnerability and security policies would be adjusted and applied as needed. IPsonar's API also supports IF-MAPs extensive querying and searching capabilities, which allow users to extract any piece of metadata, from any IF-MAP client, in order to better understand network and device behavior.



Web-based Administration and Pre-defined Reports



IPsonar MapViewer

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.



Corporate Headquarters
220 Davidson Avenue
Somerset, NJ 08873

PHONE 732.357.3500
866.LUMETA7 (586.3827)

FAX 732.564.0731