

# Network Insight with Advisor

## NETWORK INSIGHT

### Network and Device Discovery, Visibility, Automation and Control

Digital technologies are radically changing the network landscape. Direct access to public and hybrid cloud applications from everywhere is expanding the network perimeter. SaaS is delivering a fast, efficient always-on customer experience. SD-WAN is powering remote user and branch access, while wireless, IoT and 5G are dynamically increasing network resource connectivity demands.

Responding to these changes is further complicated as data is created and managed by different teams at different times with different tools and data objectives. Manual, inefficient, error-prone processes, limited and suboptimal resource utilization and rework strain the OpEx budget and teams responsible for managing core network uptime and availability. Ultimately, if you cannot see what's on your network, you cannot manage it.

### Establish Authoritative IPAM

Infoblox Network Insight, a key component of the Infoblox DNS, DHCP and IPAM (DDI) solution suite, uses distributed probes and a central data consolidator to provide a continuous import of IP and network addresses, convert discovered assets into IPAM objects and sync them into a central authoritative IPAM database. This approach delivers precise visibility, accuracy and shorter, integrated workflows, improving operational efficiencies, resource utilization, lower operational costs and data confidence for workflow automation.

### Pinpoint Network Visibility

Network Insight reduces IT silos through shared access to the integrated, authoritative database of protocol, IP address, network infrastructure device, end-host, connectivity and port data. It reduces security and service interruption risk through the detection of rogue devices, errors and unmanaged devices and networks that go unseen in standard IPAM tools. Network Insight's comprehensive inventory of switch-ports makes port-resource management easy. Network Insight automates data collection and correlation for visibility, analysis, design validation, provisioning, troubleshooting, managing and delivering effective core network services.

## NETWORK INSIGHT KEY FEATURES

### Comprehensive, Tunable Network Discovery

Gathering current infrastructure and device data provides visibility and enables action on networks and devices not currently managed within your IPAM database. Comprehensive switch-port data supplies port resource management, "use next available port" and "port reservation" features. Tunable discovery supports "black out" schedules and switch-port operations by network needed to deliver critical uptime and response requirements.

### Authoritative Network Database

A single interface for viewing protocol, network infrastructure (layer-2 and layer-3 devices), endhost, connectivity, switch-port and all related IP data empowers IT. Reduce mean time to repair (MTTR), exclude the network as a root cause for issues and confidently automate processes.

## Drive Operational Efficiencies

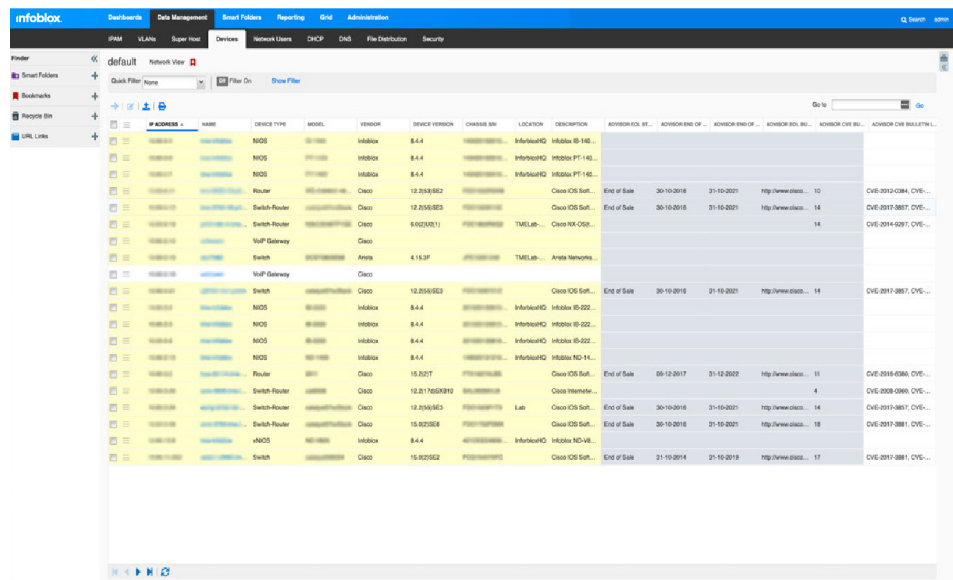
Streamline operations with integrated workflows. Provision, troubleshoot and remediate errors, and manage switch ports from a single UI. Aggregated network data improves decisionmaking and network operations by delivering contextual information, automation and control. Configurable, role-based administration enables IT teams to redeploy resources for more strategic, higher-value engagements.

## Automate and Control Workflows

Built-in controls ensure that your network is connected and running as designed. With Network Insight’s authoritative IPAM database, end-host, connectivity and core network services data, you can compare planned changes with discovered results, automate workflows across IT teams and reduce time, effort, errors and rework. Automatic IP address and port usage detection identifies conflicts and improves accuracy. Conflicts are flagged when a discovered IP address or reserved ports are associated to another endpoint outside the original reservation. Such accurate data supports “use next” for IP addresses and ports, making provisioning simple, reliable, automated and within your control.

## Manage with an Easy, Unified User Interface

Network Insight’s user interface is very easy to use and enables you to see everything on your network through a single pane of glass. Since Infoblox is founded on DNS, DHCP and IPAM data, the device tab displays all level-2 and level-3 devices along with all device and network attributes and parameters. By selecting a device, users can see the summary and forensic data of all the associated interfaces, networks, IP addresses, device location, ports, VLANs, users and end-hosts present on the network.



## Network Insight and the Reporting Appliance

Network Insight adds a wealth of network discovery data to the IPAM database. With Infoblox's Reporting and Analytics solution, this data is displayed in summary dashboards and more granular forensic reports to provide historical context for switch-port audit and compliance, real-time views and forward-looking predictive analytics. Built on the Splunk reporting and visualization engine, pre-built dashboards and reports are available and customizable to provide essential information for network management. Two such reports, Port Capacity Utilization by Device and Port Capacity Delta by Device, provide the type of historical information that helps network administrators optimize their switch-port resources.

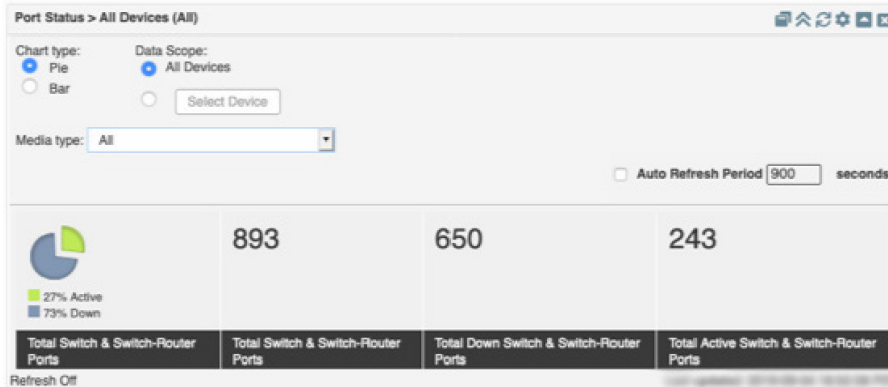


Figure 2: Port Status Dashboard, All Devices View

## Network Insight Summary

If you cannot see what's on your network, you cannot manage your network. Real-time discovery, historical and present visibility, future predictability and data access are essential. Network Insight is the catalyst for establishing an authoritative IPAM database. It provides tunable network discovery, a single repository for viewing network assets, DNS, DHCP and IPAM synchronization, integrated workflows, router and switch-port provisioning and management, conflict remediation and reporting and analytics. It's an indispensable tool for distributed discovery, IPAM integration, and network automation that will save you time, money and make your job easier.

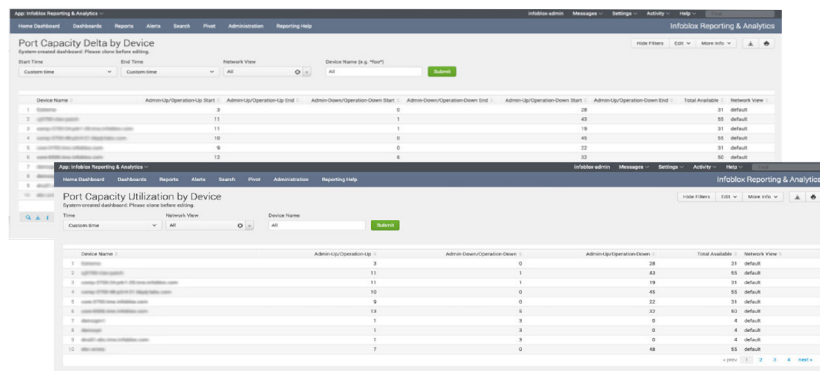


Figure 3: Port Capacity Delta and Utilization, Reporting View

### Reduce Service Interruption Risk

Easily validate network designs and quickly identify misconfigured networks, switches and misplaced servers.

### Scalability

Manage mergers and acquisitions (M&As) without network outages due to overlapping IP addresses, lost knowledge or missing network architecture documentation.

### Cross-Functional Collaboration

When security, server, and network teams share current authoritative data, they can make quick, reliable decisions, delegate tasks and eliminate departmental dependencies.

## NETWORK INSIGHT ADVISOR KEY FEATURES

### Network Insight Advisor

Provides an automated Security and Lifecycle Management service to Network Insight.

### Network Insight Integrated Discovery

Leverages Network Insight's accurate, automated, vendor-agnostic discovery, visibility, conversion of IP networks and addresses to managed assets.

### Security Advisories

Find devices and all applicable Security Bulletin vulnerabilities (e.g., PSIRTS and Common Vulnerabilities and Exposures (CVEs) for real-time alerting.

### Lifecycle Management

Detect obsolete network components based on vendor Lifecycle Management (e.g., "end-of-sale" or "end-of-support") announcements.

## NETWORK INSIGHT ADVISOR

Device Lifecycle, Security and Compliance Notification Service

### Ensure Device Security and Compliance

As networks diversify with solutions and vendors, the challenge of tracking security bulletins and field notices like Cisco PSIRTs and Juniper Bulletins becomes harder. The tedious, manual process of collecting and aggregating RSS feeds and emails and cross-tabulating vulnerabilities across a multitude of device models and OS versions can become overwhelming.

Network Insight Advisor automates this process to ensure your network is secure and up to date. By combining continuous rich device and network discovery with multi-vendor advisories, Advisor compares and assesses potential network device risks and alerts you to device vulnerabilities. Infoblox Advisor also helps plan future requirements by monitoring end-of-sale and end-of-support information.

### Engage Always-On Analysis of Security and Lifecycle Advisories

Network Insight Advisor eliminates manual time and effort by collecting and analyzing security advisory and other data from key sources and translating that data into usable alerts that are automatically streamed to the platform.

### Automate Timely Alerts on the Advisories and Devices that Matter

Instead of manually attempting to cross-reference individual advisories with different model and OS versions, Advisor delivers a curated feed of continuously updated rules and policies that highlight impacted devices in the context of your network. Customizable alerts identify devices that need further review, so your network and security experts can quickly isolate where remediation action is warranted and where action can be deferred.

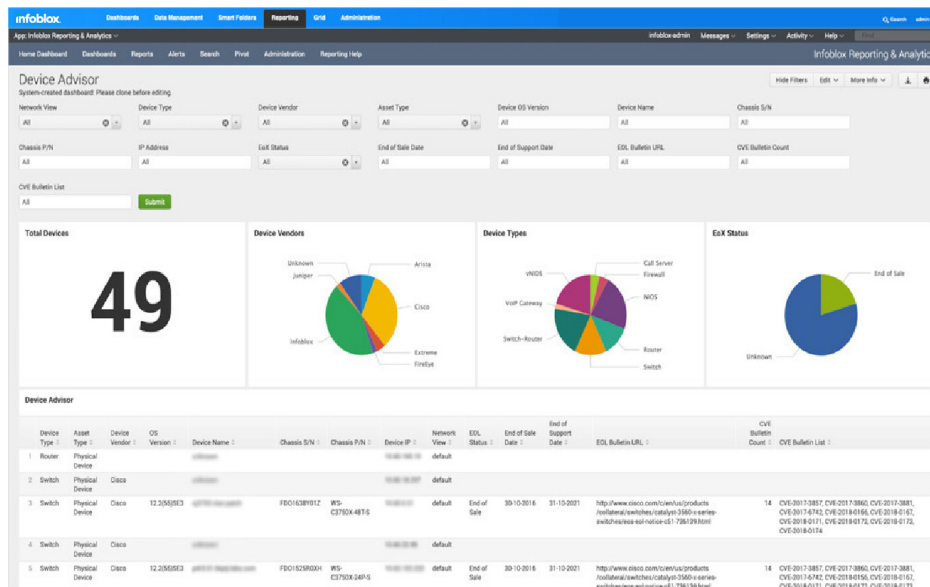


Figure 4: Device Advisor Dashboard, Reporting View

### Multi-Vendor Support

Enhance the value of your existing relationships and investments with most vendors supported out-of-the-box.

### Continuous Reporting

Identify vulnerable and obsolete equipment on an ongoing basis.

### Continuous Updates

Receive the latest announcements that apply to your infrastructure devices.

### DNS, DHCP and IPAM (DDI) Integration

Enrich the context of your DDI solution with end-of-life, service and security bulletins.

## NETWORK INSIGHT ADVISOR KEY BENEFITS

### Visibility

Identify vulnerable devices faster by providing immediate alerts of policy violations.

### Security

Automate discovery and alerting to reduce security risk and compliance issues.

### Reliability

Eliminate unnecessary manual processes and human errors by automating complex cross-tabulation.

### Automation

Track outdated and obsolete software and resolve problems faster via automated individual or bulk changes that with existing processes.

## Locate Unsupported Devices to Optimize Lifecycle Planning

Over time, particular device models and OS version combinations may no longer be supported by the manufacturer. When this occurs, a greater risk of vulnerability and compliance issues arise. Network Insight Advisor automatically detects and reports when devices and software are reaching lifecycle milestones (e.g., end-of-life or end-of-support) to keep you current and ahead of upcoming changes.

## Eliminate Device Vulnerabilities Quickly and Easily

Infoblox helps enterprises reduce network device and software vulnerability risks with a complete, automated solution including:

1. Automated discovery of network devices including vendor, model and OS version.
2. Continuous updates of advisories, PSIRTS, bulletins and end-of-sale/ support information fed into the platform.
3. Automated cross-tabulation of advisories to specific model/OS versions.
4. Alerts when vulnerabilities and non-supported devices are identified.
5. Historic reporting with Infoblox’s built-in reporting engine for trending and alerting.

## Network Insight Advisor Summary

Network Insight Advisor takes Network Insight, the market leading, integrated DDI multi-vendor discovery and switch-port management solution, and adds automated device Security, Lifecycle Notification and Compliance as an add-on service. By leveraging Network Insight’s extensive discovery engine, Advisor adds up-to-date risk and vulnerability information to improve compliance and operational security management. Infoblox Network Insight with Advisor provides you with the next level network discovery, visibility, automation, compliance and control solution that saves you time and money and simplifies your network management workload.

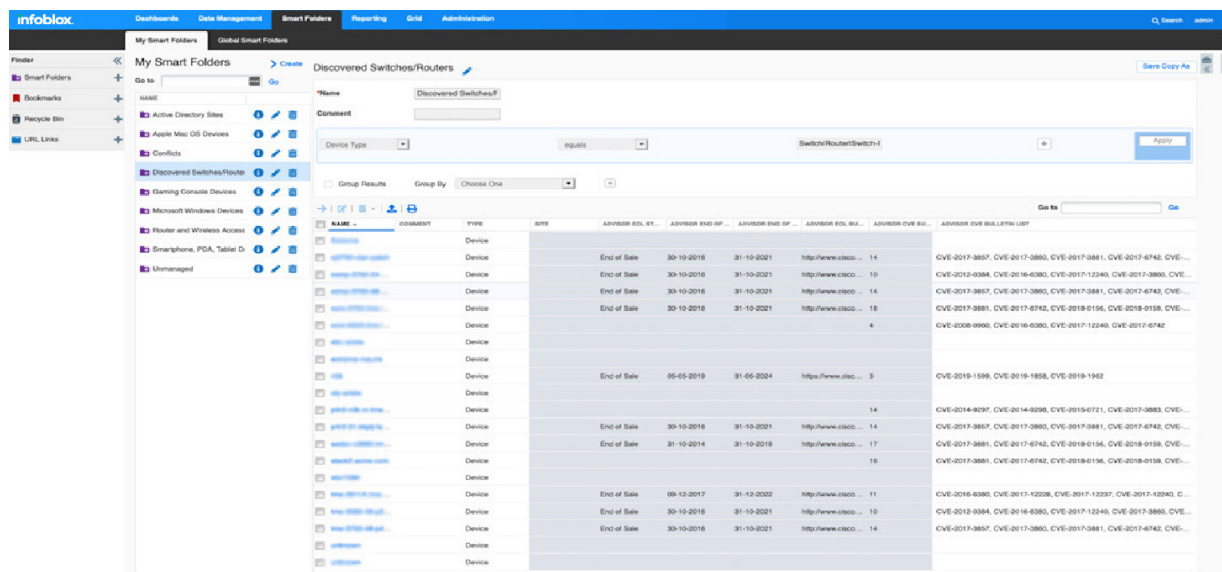


Figure 5: Discovered Switches/Routers, Smart Folders View



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

**Corporate Headquarters**  
2390 Mission College Blvd, Ste. 501  
Santa Clara, CA 95054

+1.408.986.4000  
[www.infoblox.com](http://www.infoblox.com)