

# AUTHORITATIVE IPAM QUICKSTART

## SUMMARY

Authoritative Internet Protocol Address Management (IPAM) QuickStart is an integration of network service tools that ensure identification and data accuracy for IP address planning, setup, control, tracking and reporting.

Network and Microsoft teams use it to automate discovery, visibility, sync and control of all IP network users, VMware and OpenStack endpoints, Active Directory Sites and Services and non-Windows assets. It detects rogue or compromised assets, resolves IP conflicts and automates workflow management across geo-diverse on-premises, wireless and SDN environments. It also offers multi-cloud interfaces (e.g., AWS, Azure, Google Cloud Platform, OpenStack and VMware) for DNS/IP provisioning, DDI policy-based automation and auditing in the hybrid cloud. Ecosystem integration with over 80 security vendors automates quarantine and scan of newly discovered assets and threat data sharing with endpoint, Network Access Control (NAC) and Security Information and Event Management (SIEM) tools. It also delivers full visibility through over 100 pre-built, customizable dashboards and reports, search, predictive analytics and Splunk-powered visualizations for next level endpoint, performance, security forensics, access logging, audit and control.

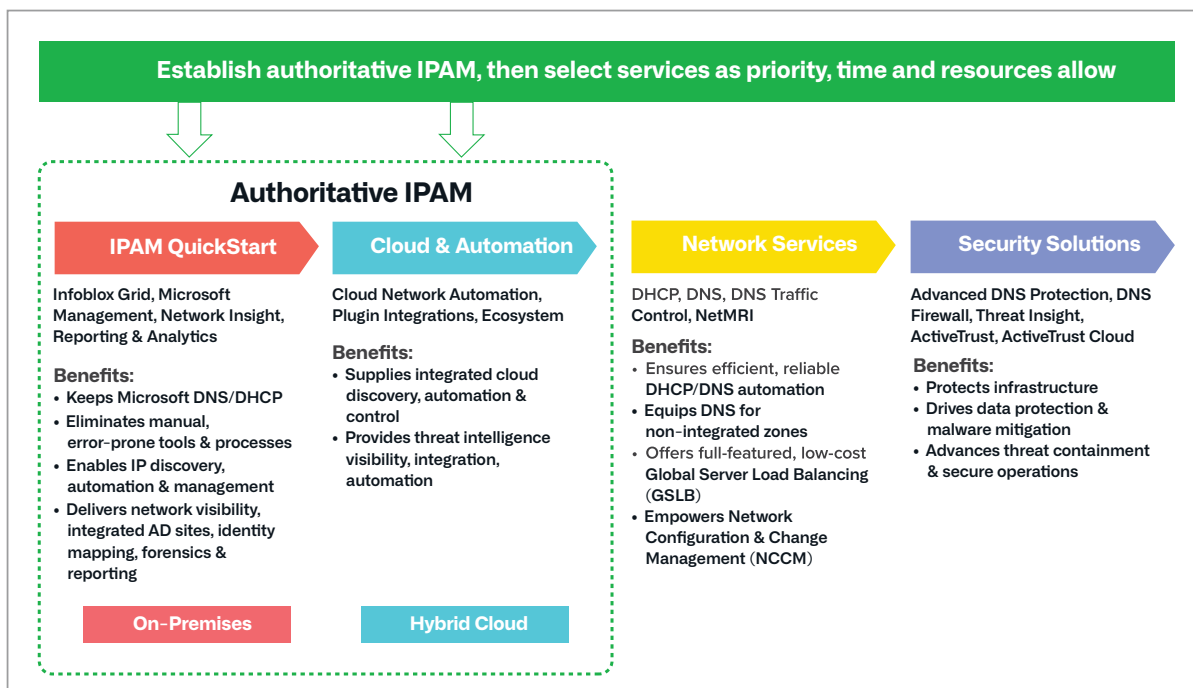


Figure 1: Infoblox solutions are built on authoritative IPAM on-premises or in the hybrid cloud to enable next level network discovery, visibility, automation and control.

## KEY COMPONENTS

- **Authoritative IPAM**

Automatically delivers accurate visibility into network asset types, attributes, availability, user context, network activity, location, network type (on-premises, hybrid cloud, wired, wireless, SDN), topology, vendor infrastructure and more.

- **Infoblox Grid**

Empowers physical, virtual or cloud-based DNS/DHCP/ IPAM (DDI) appliances embedded with IPAM, database and discovery of VMWare and OpenStack assets for reliable, automated, distributed, security-hardened, high availability and easy-to-manage core network services via a single pane of glass.

- **Microsoft Management**

Delivers an agentless DDI overlay that retains Microsoft protocols but eliminates IP conflicts, DHCP and network outages, allowing full discovery of Microsoft network endpoints, Active Directory (AD) Sites and Services and user/IP mapping for visibility, automation, orchestration, cross-team collaboration, reporting and control.

- **Network Insight**

Enables full, accurate and automated discovery, visibility, IPAM sync, switch port management, rogue and compromised asset detection, IP conflict resolution, reporting and analytics across geo-diverse on-premises, wireless and SDN environments for efficient, automated workflow management.

## AUTHORITATIVE IPAM –ACCURACY, VISIBILITY AND AUTOMATION

Authoritative IPAM accurately reflects the state of your network, provides contextual visibility (i.e., the who, what, why, when, how, where and which) of your network assets (e.g., IP addresses, subnets or VLANs) and enables you to replace manual, error-prone tools and processes with efficient, automated workflows.

### **Purpose –**

Ensuring network availability through accurate usage tracking of network assets was the original purpose of IPAM. If you allocate an IP address that is already in use, IP conflicts, network outages and escalations will result. Authoritative IPAM is the only way to avoid these outcomes. Network, Microsoft/Server Ops and Security teams gain considerable benefit by simply knowing that all network asset data is accurate and visible from a single console. Network Ops teams cannot perform proper capacity, asset/inventory or service management (e.g., ServiceNow) without having an accurate and complete view into the network. And Security teams cannot secure what they can't see. Authoritative IPAM is the solution.

### **Accuracy –**

Authoritative IPAM ensures accuracy by comparing IPAM database records with the actual network state to detect discrepancies, provide notification, reports and automated, policy-based remediation. Rather than manual user inputs and tracking, authoritative IPAM uses end-to-end workload automation to identify which assets are in use, and which are available for allocation.

### **Visibility –**

Beyond access to the IP address and subnet information, authoritative IPAM identifies a wealth of endpoint data. You'll know if the asset is a router, switch, firewall or end-host, the model, OS, vendor and which user is using the asset. You'll know when it appeared on the network and when it disappeared, and its exact location including the subnet, wireless AP, switch port, ESXi host or AWS VPC. You'll see if it's on-premises, wired, wireless, SDN, private, or in the public or hybrid cloud. And you'll have up-to-date insights on your ecosystem, infrastructure and network services vendors, no matter how complex or distributed. The end-result is that you'll gain clear, near-real-time summary and detailed visibility of everything on your network despite complexity, diversity or location.

## KEY COMPONENTS CONT.

- **Cloud Network Automation and Plugins**

Provides multi-cloud inter- faces, (e.g., VMware, OpenStack, Azure, AWS) IPAM discovery and visibility, DNS/IP provisioning, virtual server DDI policy-based automation, DDI auditing and reporting through a unified management interface.

- **Ecosystem Integration**

Automates quarantine and scans of newly discovered assets, near-real-time remediation and TrustSec policy via integrations with 80+ security vendors (e.g., McAfee, Cisco, Carbon Black, FireEye, etc.) and threat data sharing with endpoint, Network Access Control (NAC) and Security Information and Event Management (SIEM) tools.

- **Reporting and Analytics**

Delivers full plug and play visibility through 100+ pre-built, customizable dashboards and reports, search, predictive analytics and Splunk- powered visualizations for endpoint, performance, security forensics, access logging, audit and control.

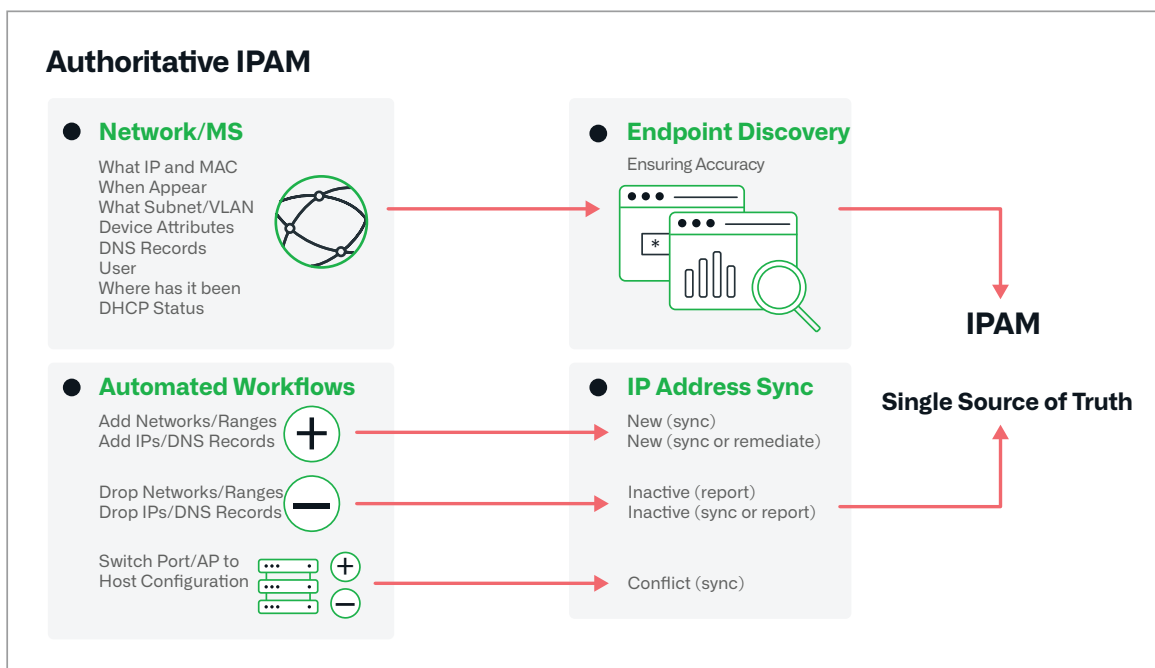


Figure 2: Infoblox authoritative IPAM, endpoint discovery, IP address sync and automated workflows deliver a single source of truth.

### Automation –

When you possess an accurate database of record, opportunities for automation are extensive. It enables automated end-to-end workload provisioning, deprovisioning and DNS, DHCP and IPAM (DDI) component syncing, NAC end-host identification and quarantine, end-host vulnerability scanning, ecosystem intel and threat sharing, alerting, reporting, analytics and more. This delivers greater accuracy, reliability, processing speed and cross-team collaboration while enabling skilled workers to be redeployed to higher-value assignments.

## IPAM QuickStart – A Deeper Look

IPAM QuickStart includes components you can select as your priorities, time and resources allow:

- **Infoblox Grid** – IP Address Management, database and discovery of VMware and OpenStack assets
- **Microsoft Management** – Discovery and management of Microsoft DHCP and DNS environments
- **Network Insight** – Discovery of on-premise wired, wireless and SDN environments
- **Cloud Network Automation** – Discovery of AWS, Azure, GGCP, OpenStack, VMware and advanced plugins (e.g., Ansible, Docker, Kubernetes)
- **Ecosystem** – Outbound API and outof-the-box Ecosystem integrations
- **Reporting and Analytics** – Near-real-time and historical dashboards, reports, alerts and predictive analytics

## INFOBLOX DISCOVERY—AUTHORITATIVE IPAM FOR ANY PLATFORM

The Foundation of a Secured, Controlled Network

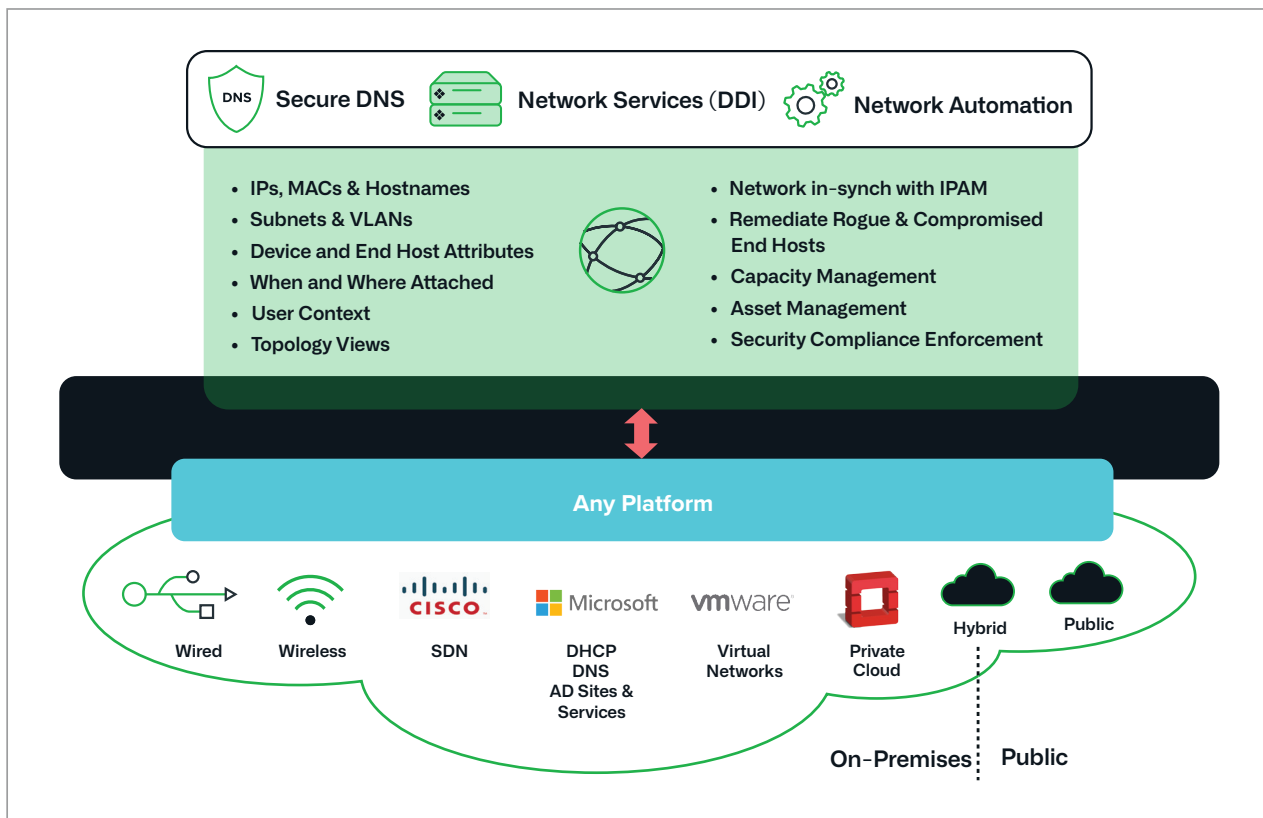


Figure 3: Infoblox authoritative IPAM works across Secure DNS, DDI and Network Automation to integrate IPAM services for any platform.

## VALUE OF AUTHORITATIVE IPAM—SECURITY, AVAILABILITY AND TRUE DATABASE OF RECORD

Functional Teams	Network Operations	Microsoft/Server	Security Operations
<b>Value Delivered</b>	Visibility into current and historical asset data, inventory, management and control	Visibility, collaboration and control across disparate Microsoft DHCP/DNS servers and Active Directory domain controllers from a single console	Consolidated near-real-time visibility into network infrastructure, users, devices, DNS threats, malicious events, contextual data, forensics and data sharing
<b>Questions Answered</b>	<ul style="list-style-type: none"> <li>• What network devices and hosts are on my network?</li> <li>• What subnets, VLANs and IP addresses are on my network?</li> <li>• How many free switch ports do I have?</li> <li>• What's in my device component inventory?</li> <li>• When did these network assets appear and where are they now?</li> <li>• To which ESX host and virtual switch is this VM attached?</li> <li>• To which Tenant, network and VPC does is this AWS VM attached?</li> <li>• To which EPG, Tenant, and Bridge Domain is this end-host attached?</li> </ul>	<ul style="list-style-type: none"> <li>• Which DHCP IP addresses are being used, who is using them, where are they on the network and what types of devices are they?</li> <li>• When did the device using this DNS record appear on the network, which VLAN is it on and to which switch port is it attached?</li> <li>• What are all my Active Directory domains, which sites are they found in and which subnets are used for replication?</li> <li>• What network devices and hosts are on my network?</li> </ul>	<ul style="list-style-type: none"> <li>• To which switch port or wireless access point is this compromised or rogue end-host attached?</li> <li>• Where has this end-host and user been on the network for the past 2 years?</li> <li>• What new assets on the network need to be quarantined or scanned?</li> <li>• What was discovered that we didn't know about? (i.e., unmanaged assets)?</li> </ul>

### SUMMARY: INFOBLOX GRID AND IPAM

Infoblox Grid and IPAM enables network accuracy, visibility and reliability:

- Provides automatic accurate, reliable, near-real-time data updates and status of network assets (e.g., IPs, subnets & VLANs) for visibility, control and guaranteed performance
- Detects discrepancies between the IPAM database and the true network state for alerting and remediation
- Allows distributed integrated appliances to deliver automated, highly available, security-hardened, easy-to-deploy and manage core network services via a single pane of glass

## INFOBLOX GRID AND IPAM

Infoblox physical or virtual appliances deliver core network services in a reliable, secure, easy-to-deploy and manage platform. The Infoblox Grid is created by linking appliances across a distributed enterprise. Rather than a separate management and reporting application overlay for individual appliances, Grid appliances are embedded with a sophisticated distributed database technology and linked together. This transforms the appliance network into a unified system with a single UI, high availability, hardened system security and integrated DDI database.

The Infoblox Grid simplifies and delivers IPAM as a manual or automated core network service for a more resilient network while delivering significant labor, time and workflow savings. Applications that need IP addresses can be served in a consistent, automated and error-free manner through the Infoblox IPAM interface:

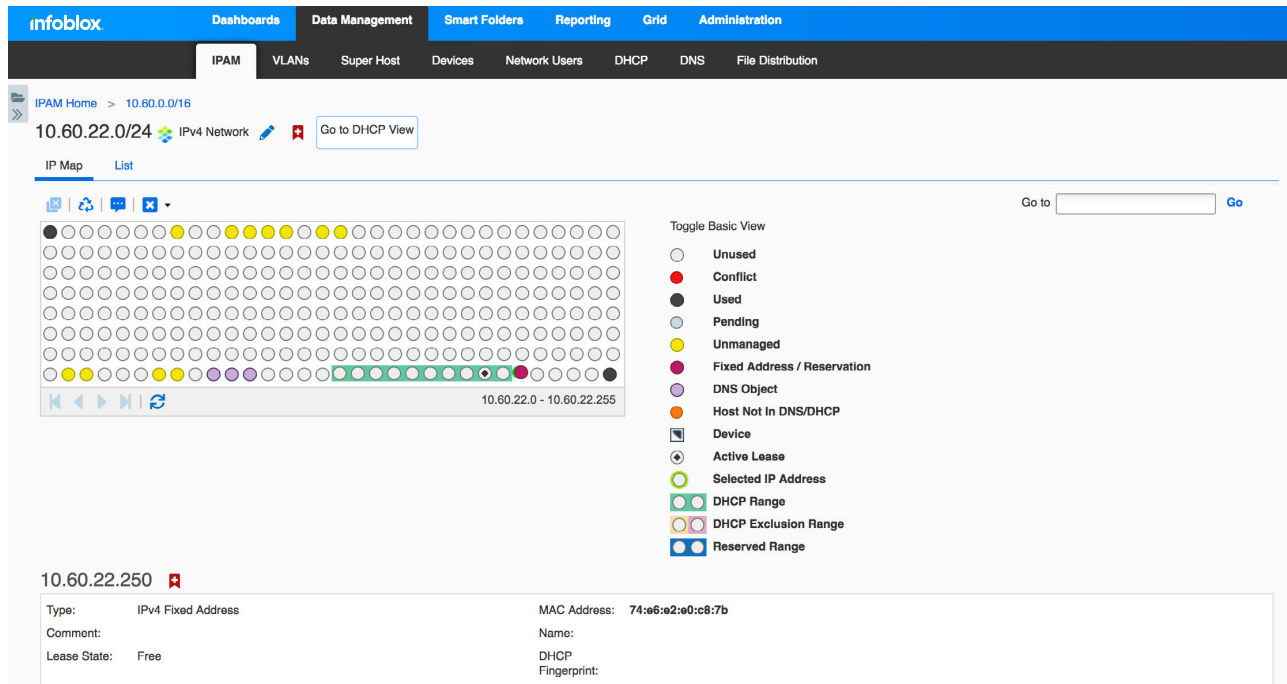


Figure 4: The Infoblox UI maps IP address data for a given DHCP range and delivers this information through a single management platform.

## SUMMARY: INFOBLOX MICROSOFT MANAGEMENT

Infoblox Microsoft Management is a DNS/DHCP protocols overlay that retains existing infrastructure and enhances investment:

- Central DNS/DHCP integration and management
- Agentless connection with no server impact
- Automated DDI component syncing and near-real-time data
- Cross-team collaboration
- User/IP identity-mapping
- Resource planning

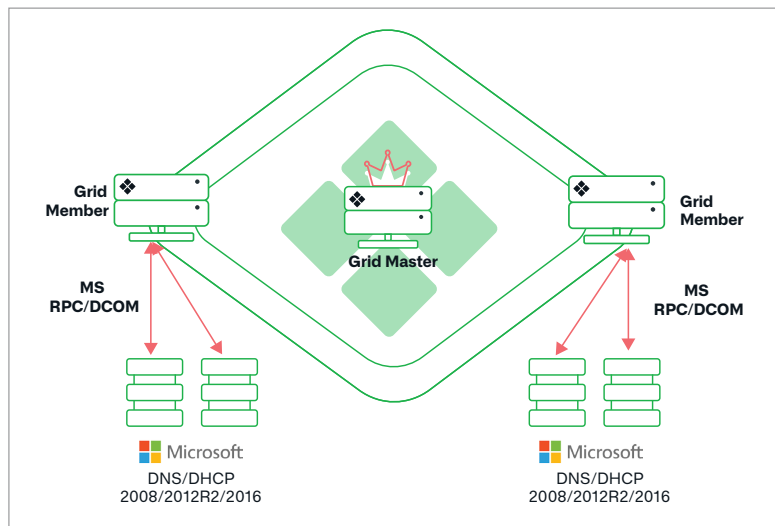


Figure 5: Infoblox Microsoft Management is an agentless overlay for Microsoft DNS/ DHCP that solves IP conflicts, DHCP issues and network outages.

## MICROSOFT MANAGEMENT

With the skyrocketing demand for IP addresses fueled by ever-increasing applications, personal devices, IoT, IPv6, virtualization and more, many organizations struggle to manage IPs efficiently to ensure delivery of highly available network services. The struggle is worse for organizations preferring to retain existing Microsoft-based DNS/DHCP servers, but find that more servers, added technology and an automated IPAM system are essential to keep pace with IP address management scalability, redundancy and security needs. Infoblox Microsoft Management solves these challenges. By keeping the existing Microsoft DNS/DHCP protocols, Infoblox Microsoft Management provides a non-intrusive overlay to enhance the value of the existing Microsoft investment. Since it uses RPC via DCOM for communication, no installed agents are required. Adding Microsoft Management adds full visibility to solve IP conflicts, DHCP availability issues and network outages. Here are a couple of key use cases:

### Hybrid Cloud, Central View of Microsoft DHCP:

Infoblox can be used in the private, public or hybrid cloud. Due to its deep, DNS integration, you can access Microsoft DHCP data to see things like address range, usage status, lease state and more, all from a central view:

### Hybrid Cloud, Central View of Microsoft Sites and Services:

Infoblox saves you time and makes your job easier by capturing Microsoft Active Directory domains, Sites, networks for replication, user data and more, bringing it all together in a single view:

## SUMMARY: INFOBLOX NETWORK INSIGHT

Infoblox Network Insight delivers on-premises discovery, visibility, IPAM sync, switch port management and control:

- Unveils deep discovery of network devices, end-hosts, subnets, interfaces, components and topology
- Detects and remediates IP conflicts and rogue and compromised assets
- Supplies continuous syncing of networks and IPs into IPAM
- Automates router and switch port provisioning and control

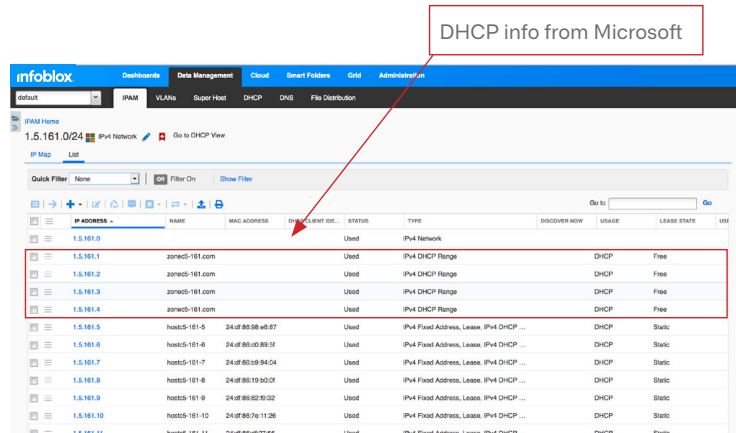


Figure 6: Infoblox captures and displays DHCP data from Microsoft protocols.

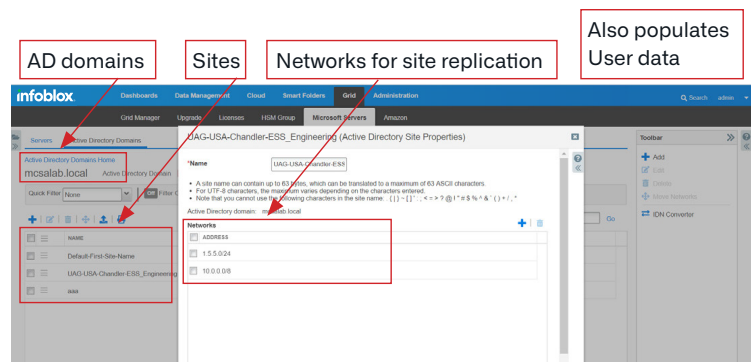
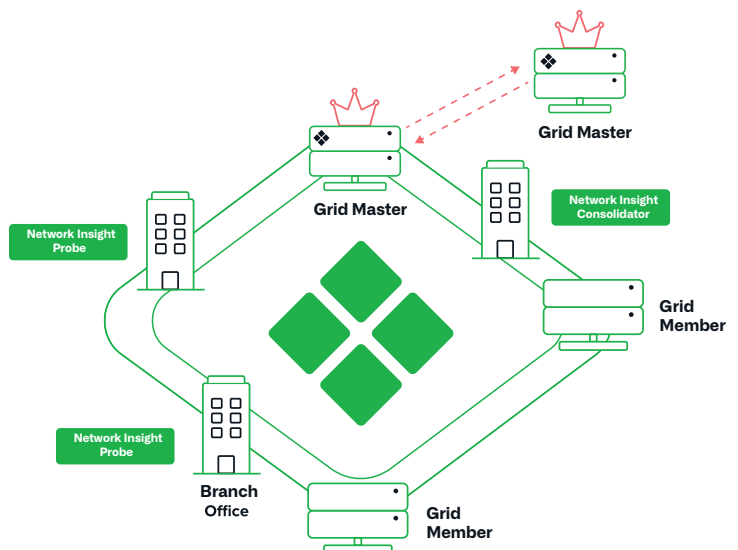


Figure 7: Infoblox Microsoft Management captures and presents Microsoft Sites and Services data through a central view.



## NETWORK INSIGHT

If you manage geo-diverse, on-premises, wireless and SDN environments, end-to-end accurate and automated end-point discovery is essential. The ability to see summary and detailed asset data, sync IP addresses, manage switch ports, detect compromised or rogue assets, resolve IP conflicts and ensure ongoing alerting and reporting are required best practices. Infoblox's deep DNS, authoritative IPAM and vendor integrations makes near-real-time data available on demand.

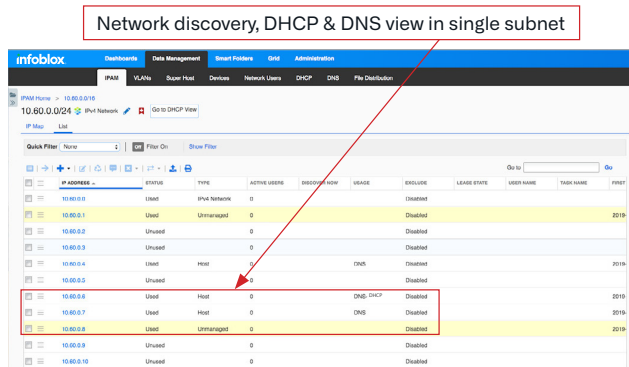


Figure 8: The Infoblox UI shows the depth of on-premises individual IP host discovery data captured by Network Insight/ NetMRI.

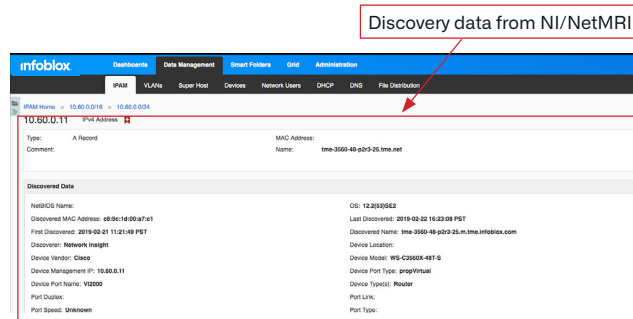


Figure 9: Infoblox network discovery delivers DHCP/ DNS single subnet data through Network Insight/NetMRI.

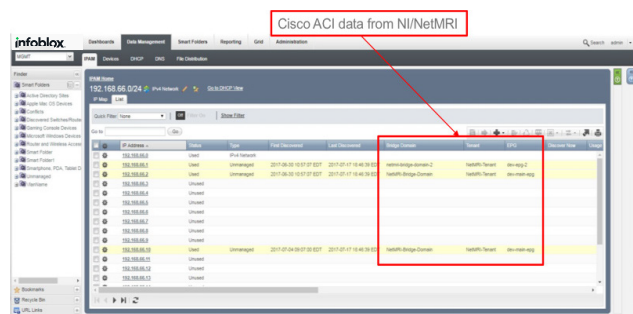


Figure 10: Infoblox includes many vendor integrations out-of-the box including this Cisco ACI integration that highlights data captured by Network Insight/NetMRI.

## SUMMARY: INFOBLOX CLOUD NETWORK AUTOMATION AND PLUGINS

Infoblox Cloud Network Automation delivers multi-cloud discovery, IPAM sync and control:

- IPAM discovery and visibility for traditional networks, private, and leading public and hybrid cloud platforms via a single pane of glass
- DNS, DHCP and IPAM policy-based automation for virtual servers
- DNS/IP provisioning via plugins with AWS, Azure, Google Cloud Platform, OpenStack, VMware and more
- Single Open RESTful management customization interface
- Fast, efficient clean-up of decommissioned instances
- Auditing and reporting across clouds for DHCP leases, DNS records and IP addresses

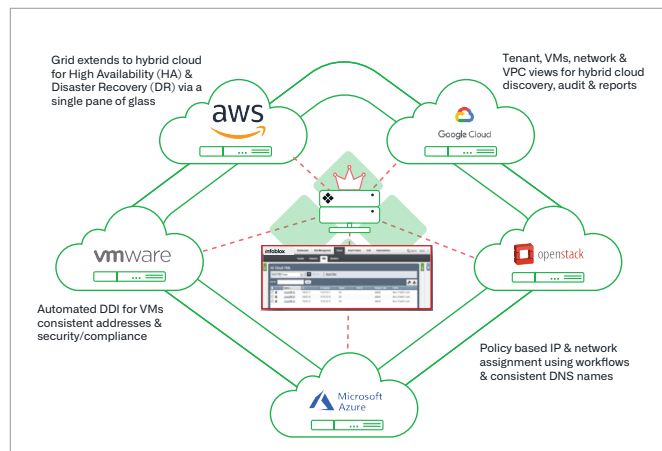


Figure 11: Infoblox offers a multi-cloud architecture for authoritative IPAM asset discovery, control, HA, DR, auditing and reporting.



## CLLOUD NETWORK AUTOMATION

Like Network Insight for on-premises environments, Cloud Network Automation delivers IPAM discovery and visibility for assets located in the private, public or hybrid cloud. It's an indispensable tool that provides multi-cloud discovery, sync and control for organizations with cloud initiatives. Not only does it supply visibility into AWS, Azure, Google Cloud, OpenStack and VMware platforms, it automates DNS/IP provisioning and deprovisioning, and coordinates allocation and release of IP addresses and DNS registrations with orchestration tools across servers, networks and storage. Authoritative IPAM ensures accurate DDI resource distribution across a hybrid environment—all from a single system. Automating manual processes can change workflows from days to seconds, increasing accuracy, reliability, coordination and efficiency. Plus, Infoblox has out-of-the box plug-in integrations with leading orchestration tools like Ansible, VMware vRA, CNI Kubernetes and more.

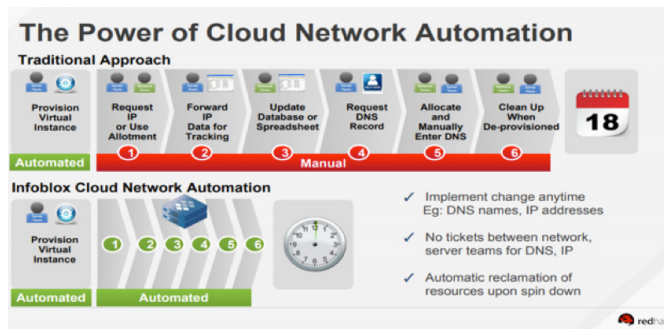


Figure 12: Cloud Network Automation saves time and cost, delivers greater reliability and improves processes and workflows.

## SUMMARY: INFOBLOX ECOSYSTEM

Ecosystem eliminates silos, enables faster incident response and supports near-real-time action through inbound and outbound API integrations with private, public and hybrid cloud partners, integrators and vendors:

- Automates quarantine and scans of newly discovered assets
- Provides near-real-time remediation and TrustSec policy by sharing threat data with endpoint, NAC, SIEM and other solutions
- Engages billions of indices via seamless 3rd party integrations with Cisco, Carbon Black, Qualys, FireEye, LogRhythm and 80+ more

VM Name	VM ID	IP Address	VM Availability Zone	Network	VM VPC	VM Region	Host ID
Azure VMAutomation01	VMAutomation01	10.100.103.182	us-east-1a	2	None	us-east-1	VMAutomation01
Azure VMAutomation02	VMAutomation02	10.100.99.2	us-east-1a	2	None	us-east-1	VMAutomation02
Azure VMAutomation03	VMAutomation03	10.100.103.182	us-east-1a	2	None	us-east-1	VMAutomation03
GCP gke-aws-ipv4-rev-default-pool...	7136000298...	172.25.1.5	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
GCP gke-aws-ipv4-rev-default-pool...	7136000292...	35.247.7.173	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
GCP gke-aws-ipv4-rev-default-pool...	37782668168...	35.247.83.222	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
GCP gke-aws-ipv4-rev-default-pool...	37782668168...	172.25.1.4	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
GCP gke-aws-ipv4-rev-default-pool...	633551121457...	35.247.30.129	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
GCP gke-aws-ipv4-rev-default-pool...	633551121457...	172.25.1.6	us-east-1a	2	None	us-east-1	gke-aws-ipv4-rev-default-pool...
Azure test-ipv4-02	VMAutomation01	10.2.1.4	us-east-1a	3	test-ipv4-02	us-east-1	test-ipv4-02

Figure 13: Cloud Network Automation provides a detailed central, multi-tenant view of cloud-discovered assets.

IP Address	Status	Type	Attached Device	Attached Device	Attached Device	Attached Device	Attached Device	Attached Device	Attached Device
10.60.16.0/24	Unused								
10.60.16.5	Unused								
10.60.16.7	Unused								
10.60.16.8	Unused								
10.60.16.9	Unused								
10.60.16.10	Unused								
10.60.16.11	Unused								
10.60.16.12	Used	Unmanaged	Cisco IOS Svr...	10.60.0.12	hme-3760-48-p...	csayip37xv3Stack	Q1-014	Cisco	Highash-ess-n...
10.60.16.13	Used	Unmanaged	Cisco IOS Svr...	10.60.0.12	hme-3760-48-p...	csayip37xv3Stack	Q1-022	Cisco	TMECluster-106...
10.60.16.14	Used	Unmanaged	Cisco IOS Svr...	10.60.0.12	hme-3760-48-p...	csayip37xv3Stack	Q1-023	Cisco	TMECluster-106...
10.60.16.15	Unused								

Figure 14: For NetOps and Security teams, Infoblox displays DNS and network discovery data for forensic insights into single IPs.

## ECOSYSTEM

Infoblox Ecosystem is a highly interconnected set of integrations that improve significantly the security, efficiency and ROI of third party and multi-vendor assets throughout the cybersecurity network. It enables security, increases agility and enhances situational awareness across networks of any scale or complexity. Integrations eliminate silos between network and security teams and provide consolidated visibility of on-premises, virtualized and cloud infrastructure. By automating workflows, the Ecosystem accelerates remediation of threat and network changes, enabling organizations to raise network security, performance, efficiency and cost control to the next level.

### How Ecosystem Works

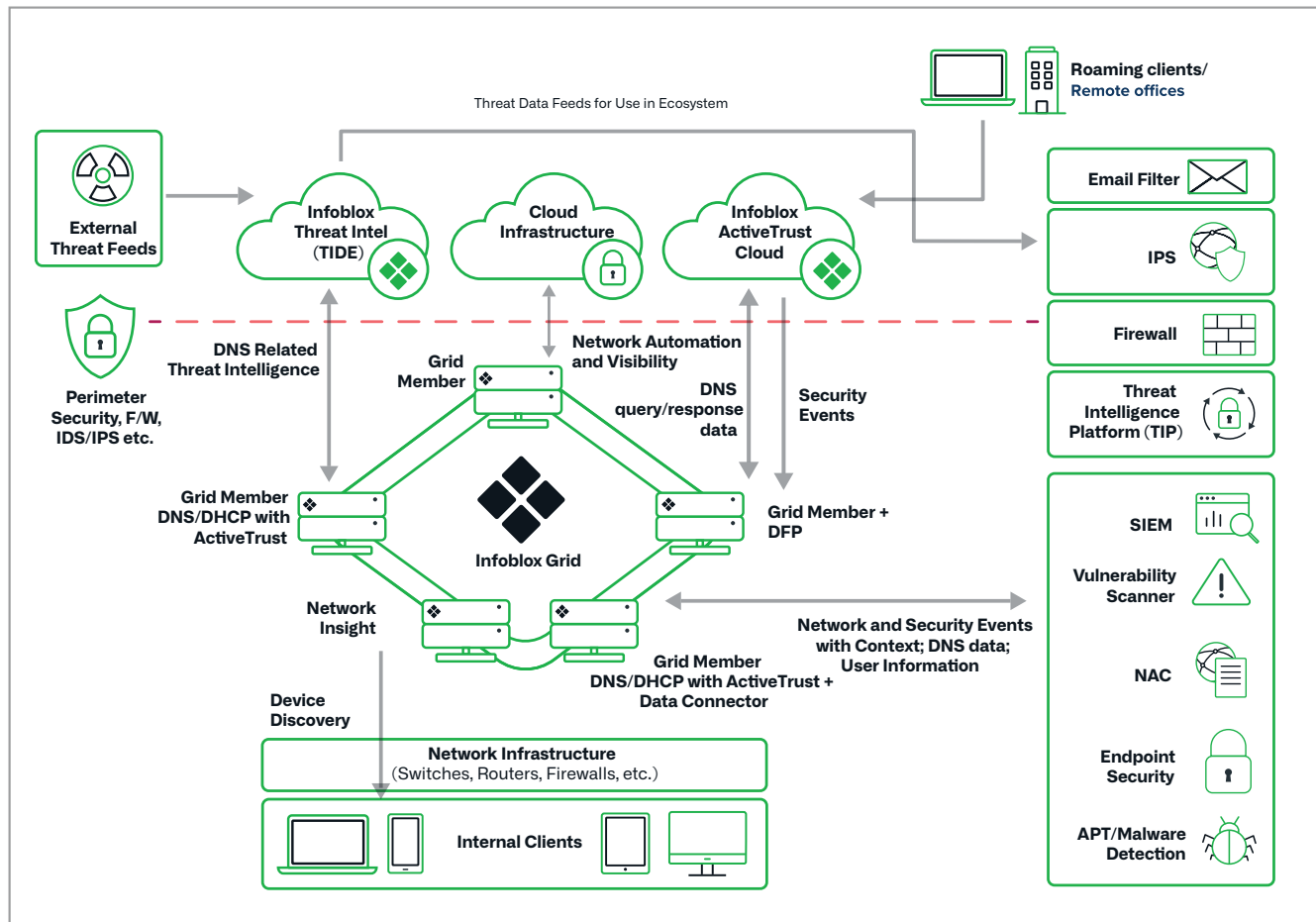


Figure 15: Infoblox Ecosystem automatically discovers, scans, remediates, updates policies and shares data with security tools and the security vendor community.

Automation is driven by accurate network database records, APIs and extensive security vendor integrations. Automation enables contextual data sharing and customization with security, configuration management database (CMDB) and service management tools.

## How Ecosystem Works

- Integrations with vendors like Ansible, VMware and Kubernetes reduce days of manual processes to seconds through end-to-end workload automation.
- Newly discovered assets are automatically scanned for vulnerabilities through vendors like McAfee, Qualys, Rapid7 and Tenable.
- Discovered rogue end-hosts are quarantined, near-real-time remediation is engaged, TrustSec policies are updated and contextualized data is shared with NetwAC and SIEM tools including Cisco ISE/pxGrid and McAfee.
- The Ecosystem discovers, scans, remediates, updates policies and shares data with the security vendor community—automatically—for greater protection and manageability.

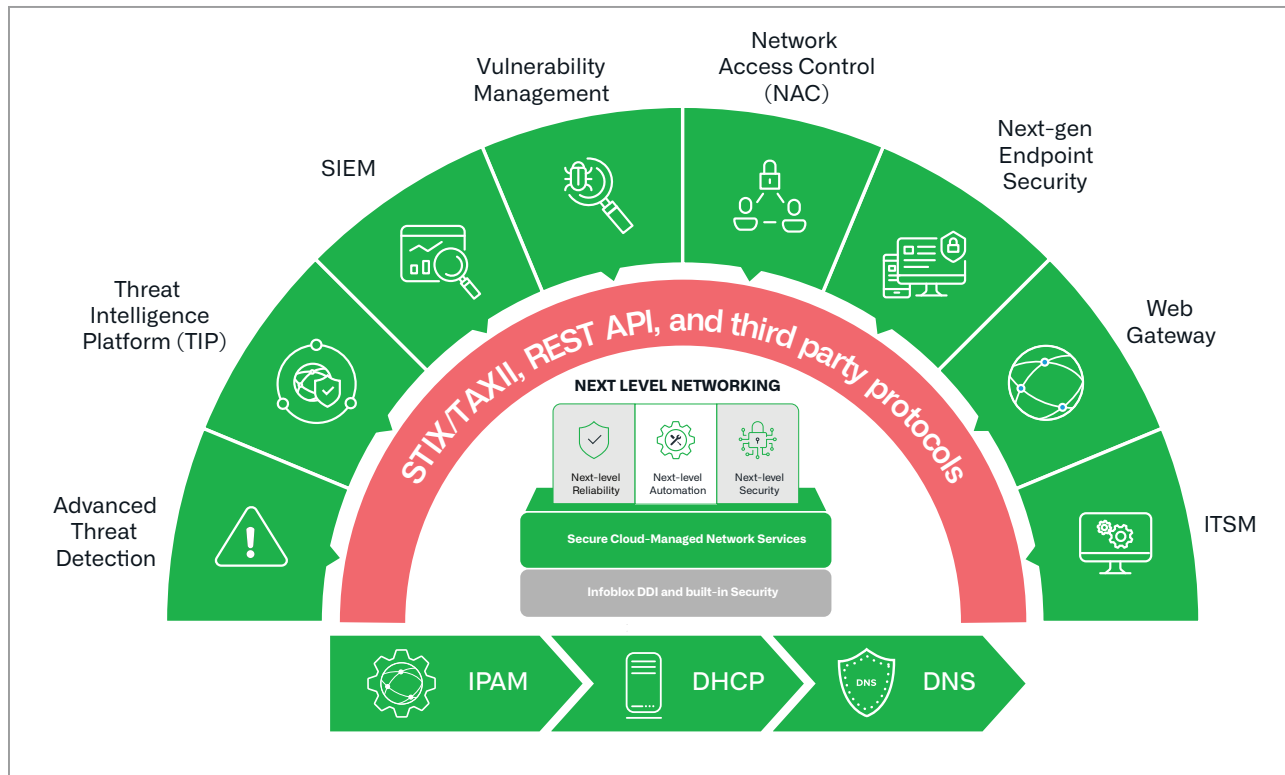


Figure 16: Infoblox Ecosystem delivers automated device fingerprinting, audit trail and contextualized data for prioritization, orchestration and rapid incident response.

## Ecosystem Integrations

The Infoblox API fuels integrations with over 80 security vendors and growing, processing an escalating 14 billion threat indices across a broad array of security tools. These include Advanced Threat Detection, Threat Intelligence Platform (TIP), Security Information and Event Management (SIEM), Vulnerability Management, Network Access Control (NAC), Next-Gen Endpoint Security, Web Gateway, and IT Service Management (ITSM)/IT Operations Management (ITOM)/Security Operations.

This Solution Note highlights two integrations, an automated Network Access Control (NAC) solution with Cisco ISE (Figure 17) and an automated end-host vulnerability scanning solution with Rapid7 (Figure 18). Infoblox has, and continues to develop, many other integrations with partners, integrators and vendors as shown in Figure 19. Please access the [Ecosystem](#) microsite on Infoblox.com for additional resources and information.

## Automated NAC and Quarantine

Since Authoritative IPAM can identify rogue and potentially compromised end-hosts, IPAM becomes a key notifier and publisher to NAC systems. For instance, Infoblox has an out-of-the-box integration with Cisco ISE/pxGrid. This allows Infoblox to publish discovered identity data to ISE to adjust TrustSec policies and notify ISE of end-hosts that require quarantine. Infoblox also subscribes to user data and quarantine status from ISE so this data is visible in the Infoblox UI.

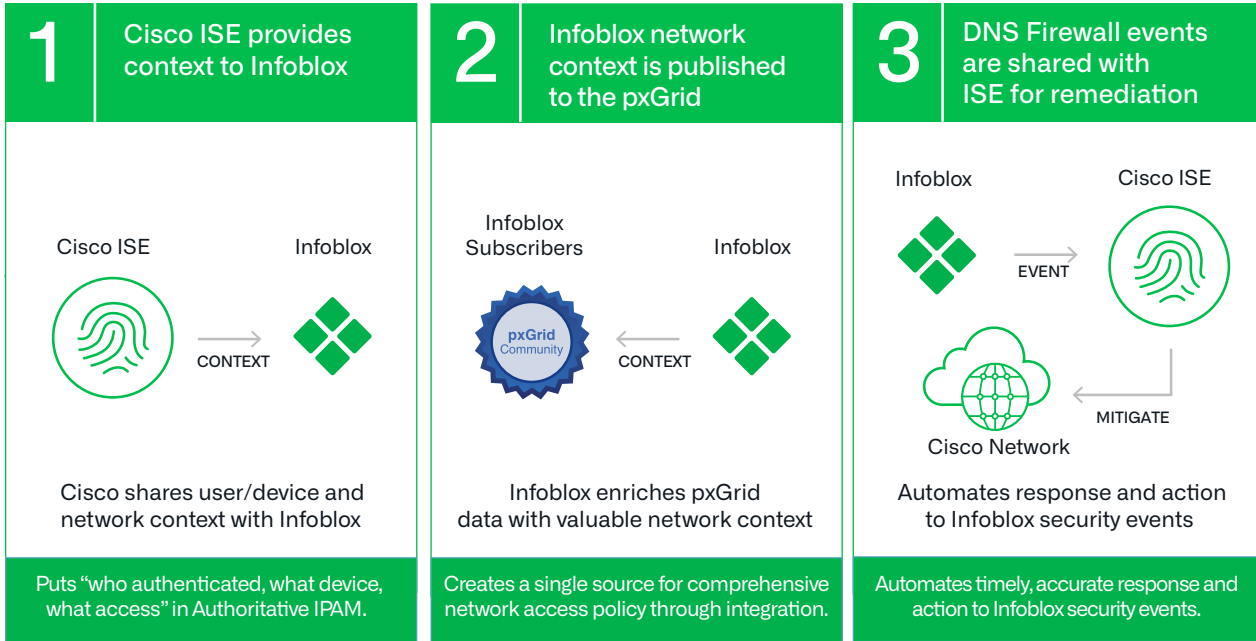


Figure 17: Infoblox shares rich IP address, DNS, DHCP and network data with NAC solutions like Cisco ISE for better policy decisions and faster incident response.

## Automated End-Host Vulnerability Scanning

Authoritative IPAM identifies when new subnets and IP addresses appear on the network. It classifies them as “known” or not and can potentially identify them as compromised. With a breadth of out-of-the-box integrations with vulnerability scanners including Rapid7, Qualys, Tenable and McAfee, along with the Infoblox outbound API, vulnerability scans of network assets can be automated. This shortens the time a potentially rogue or compromised asset can be on the network prior to scanning and remediation.

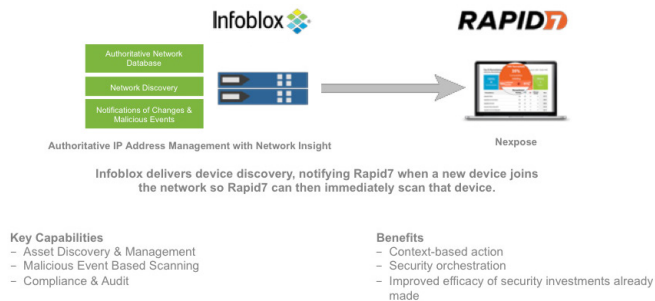


Figure 18: Infoblox makes vulnerability scanning more efficient through integrations like Rapid7 for greater audit, compliance and control.



Figure 19: The robust Infoblox API enables a broad array of integrations with the leading security partners, integrators and vendors to deliver an unmatched ecosystem advantage.

## REPORTING AND ANALYTICS

If you work on a network, you’re sitting on a wealth of business-impacting data flowing through your endpoints, clients and applications. But can you see it? Can you access and manipulate it? Are you actively leveraging it to make your network more secure, perform faster, more reliably and scale to meet changing business needs?

Built on Infoblox DDI and the Splunk reporting and visualization engine, Infoblox Reporting and Analytics delivers fast plug-and-play deployment, role-based access control, historical search, near-real-time alerting and predictive analytics to help you get the most from your data and network. It includes over 100 pre-built, customizable dashboards and reports, and provides the flexibility to adjust filters, create new dashboards, reports, set distribution lists, alerting thresholds and frequencies, and much more.

## SUMMARY: REPORTING AND ANALYTICS

Infoblox Reporting and Analytics delivers summarized, granular and predictive analytics for full network visibility:

- Provides fast plug-and-play deployment
- Enables deep visibility into network data on-premises and in the private, public and hybrid cloud through a central management platform
- Delivers real-time and historical search and predictive views via 100+ pre-built, customizable, Splunk-based dashboards, reports and alerts
- Empowers security forensics, audit & compliance via query logging
- Allows fast threat detection & remediation via ecosystem data sharing

Data is presented in summary view but thanks to the deep DNS-based integration, it's also accessible through granular query logging for security forensics and actionable, on-demand tracking to support audit, forecasting and control. Since query log data can place a considerable processing load on core network services, Infoblox provides a Data Connector that offloads much of the processing impact to keep services running at peak performance.

The following reporting dashboards are provided out-of-the-box with the Authoritative IPAM components even if you are using just Microsoft for DHCP and DNS:

<b>Discovery</b> <ul style="list-style-type: none"> <li>• End-Host History</li> <li>• IP Address Inventory</li> <li>• Network Inventory</li> <li>• Device Interface Inventory</li> <li>• Device Inventory</li> <li>• Device Components</li> <li>• Port Capacity Utilization By Device</li> <li>• Port Capacity Trend</li> <li>• Port Capacity Delta By Device</li> <li>• IPAMv4 Device Networks</li> </ul>	<b>DNS</b> <ul style="list-style-type: none"> <li>• Replies Trend</li> <li>• Update Trend</li> <li>• Query Rate by Member</li> <li>• Query Rate by Query Type</li> <li>• Daily Query Rate by Member</li> <li>• Daily Peak Hour Query Rate by Member</li> <li>• Domains Queried by Client</li> <li>• Domain Query Trend</li> <li>• Query Trend per IP Block Group</li> <li>• Top Clients</li> <li>• Top Clients by Query Type</li> <li>• Top Clients per Domain</li> <li>• Top Clients Query MX Records</li> <li>• Top NXDOMAIN</li> <li>• Top Requested Domain Names</li> <li>• Top SERVFAIL Errors Received</li> </ul>	<b>DHCP</b> <ul style="list-style-type: none"> <li>• Lease History</li> <li>• Message Rate Trend</li> <li>• Top Lease Clients</li> <li>• V4 Range Utilization Trend</li> <li>• V4 Usage Statistics</li> <li>• V4 Usage Trend</li> <li>• V4 Top Utilized Networks</li> </ul>
<b>IPAM</b> <ul style="list-style-type: none"> <li>• IPAMv4 Network Usage Statistics</li> <li>• IPAMv4 Network Usage Trend</li> <li>• IPAMv4 Top Utilized Networks</li> </ul>	<b>Cloud</b> <ul style="list-style-type: none"> <li>• VM Address History</li> <li>• License Pool Utilization</li> </ul>	
<b>SYSTEM</b> <ul style="list-style-type: none"> <li>• CPU Utilization Trend</li> <li>• Memory Utilization Trend</li> <li>• Traffic Rate Trend</li> <li>• Audit Log &amp; User Login History</li> </ul>	<b>Ecosystem</b> <ul style="list-style-type: none"> <li>• User Login History</li> <li>• Subscription Data</li> <li>• Publish Data</li> </ul>	
	<b>Prediction</b> <ul style="list-style-type: none"> <li>• Home Dashboard</li> <li>• System Capacity Prediction Trend</li> <li>• IPAM Prediction Trend</li> </ul>	

Figure 20: Infoblox includes over 45 pre-built, custom-izable IPAM dash-boards and reports for summary and forensic-level insights.

## Device Interface Inventory

Addresses: Audit/Compliance, Uptime & Performance (Sample Report 3.1)

- **What is it?**  
Tracks each device & interface inventory
- **Who Needs It?**  
Network & Microsoft Admins
- **Why is it Important?**
  - Discover, members & tracks devices & their interfaces
  - Provides critical information for audit, compliance & troubleshooting devices & their interfaces
- **How do You Get It?**  
Out-of-the-box (Requires Network Insight)
- **Where is it Located?**  
Device (Discovery) Dashboards
- **Data Presented?**  
Total Interfaces, Port Types, Admin Status, Operation Status, Trunk Status, Interface Inventory



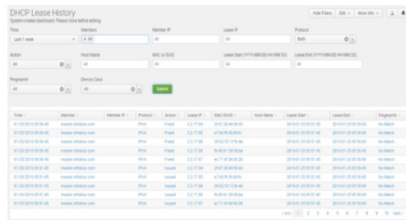
**Use Case:** An Admin must take inventory of device interfaces. A troubled device is discovered. What interface does it use? Are other devices with the same interface also having issues?

Figure 22: This report shows DHCP lease history for a given time to enable security forensics and audit.

## DHCP Lease History

Addresses: Audit/Compliance & Security (Sample Report 4.1)

- **What is it?**  
Shows DHCP history for a given timeframe
- **Who Needs It?**  
Network, Microsoft & Security Admins
- **Why is it Important?**
  - Provides a time-sequenced list of which MACs requested an IP address & when
  - Correlates systems to IPs
  - Aids audit, compliance & troubleshooting
- **How do You Get It?**  
Out-of-the-box
- **Where is it Located?**  
DHCP Dashboards
- **Data Presented?**  
Time, Member, Member IP, Protocol, Action, Lease IP, MAC/DUID, Hostname, Lease Start, Lease End, Fingerprint, Microsoft Server, Microsoft Server IP & Device Class



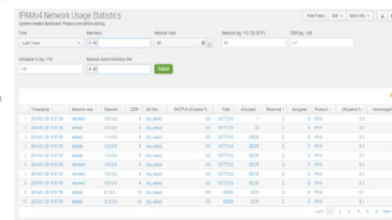
**Use Case:** A device was infected last month. Lease times are 24 hours. What IPs has it had in the last month?

Figure 21: Built on the Splunk reporting and visualization engine, this report displays device and interface inventory to support audit and performance troubleshooting.

## IPAMv4 Network Usage Statistics

Addresses: Capacity Planning (Sample Report 8.1)

- **What is it?**  
Shows utilization data for IPAMv4 networks
- **Who Needs It?**  
Network & Microsoft Admins
- **Why is it Important?**
  - Provides detailed views of usage based on individual networks & subnets
  - Helps Admins plan for network & subnet capacity & tracks usage over time
  - Prevents resource conflicts
- **How do You Get It?**  
Out-of-the-box
- **Where is it Located?**  
IP Address Management Dashboards
- **Data Presented?**  
Timestamp, Network View, Network, CIDR, AD Site, DHCPv4 Utilization %, Total, Allocated, Reserved, Assigned, Protocol, Utilization % & Unmanaged



**Use Case:** Enables Admins to proactively identify networks that are approaching full utilization.

Figure 23: As one of the all-time most utilized reports, the Infoblox IPAM Network Usage Statistics report aids in planning to identify which networks that are nearing full capacity.

For a list of other dashboards and reports, see the [Infoblox Reporting and Analytics Sample Report Guide](#). And for more information on Infoblox Reporting and Analytics, visit the [Reporting](#) microsite.

Beyond these resources, another unique Infoblox advantage is the [Infoblox Community](#) and [Reporting Forum](#). Join for free and connect with SMEs, engineers, product managers and other Infoblox customers for networking, best practices, problem resolution, customer-developed reports, tricks-of-the-trade, learning and other resources to help you get the most visibility into your data and value out of your network.

If any of this has captured your interest, let's have a conversation. Visit us at [Infoblox.com](http://Infoblox.com), email us at [info@infoblox.com](mailto:info@infoblox.com) or call us toll-free at 1.866.463.6256.

## CASE STUDIES

**Case Study – Large US Federal Government Agency**

**Problem:**

- No centralized visibility, IPAM repository or management
- Scalability to handle extensive data from nationwide locations & devices (153 hospitals, 1,700 clinics)
- Inefficient spreadsheets, manual processes, conflicts & errors
- Lack of visibility, manageability, automation & control

**Results:**

- Central management of IP infrastructure for all environments with physical & virtual appliances
- Automated workflows to manage resources & change config
- Improved agility and customer experience with automation
- Superior visibility, discovery, data sharing, reporting & control

**Solutions:**

- IPAM, Microsoft Management, Network Insight, Cloud Network Automation with Plugins, Ecosystem, Reporting and Analytics and Professional Services

"After extensive research, Infoblox's discovery, real-time data, Active Directory and ForeScout ecosystem integrations made it the clear choice for authoritative IPAM, reporting and control..."

Sr. Director  
IT & Network Services

**Case Study – HR Enterprise Resource Planning Provider**

**Problem:**

- Siloed worksheets, manual processes, spreadsheets, IP conflicts, data errors, need for cloud deployment & reporting visibility

**Results:**

- Centrally manage IP infrastructure for all environments with physical & virtual appliances
- Automate workflows for discovery & change config
- Improve agility and customer experience with automation
- Bonus: Out-of-the-box intelligent reporting

**Solutions:**

- IPAM, Microsoft Management, Network Insight, Cloud Network Automation and Reporting and Analytics
- 4-Phase DHCP progressive deployment (12 months start to finish)
- Engaging now for cloud, DNS & security

"Infoblox really helped us unify, centralize and automate our IP address management."

SVP  
Network Services

**Case Study – Council Rock School District**

**Problem:**

- Inefficient, hard-to-manage Microsoft DHCP system
- Scaling for 16 campus locations, siloed locations, 257 switches
- Unauthorized changes, manual processes & spreadsheets
- Malware infected clients
- Lack of centralized visibility, alerting & reporting

**Results:**

- Significant reduction of issues caused by unauthorized changes
- Central management of IP infrastructure for all environments with physical & virtual appliances
- Automated workflows to manage resources & change config
- Rapid identification & remediation of malware infected machines
- Superior visibility, discovery, data sharing, reporting & control


**Solutions:**

- IPAM, DHCP, DNS, DNS Firewall, NetMRI, Reporting and Analytics, Professional Services

- 12<sup>th</sup> largest PA school district
- 11,200 students
- 16 campus locations

"If you're responsible for safeguarding your network and you're not using Infoblox DNS Firewall, you're not doing your job."

Matthew Frederickson  
Director of IT



## CONCLUSION

Network Operations, Microsoft/Server and Security Operations teams face numerous challenges including limited network discovery and visibility, IP conflicts, DHCP issues, network outages, inefficient, error-prone tools and processes, disparate platforms and silos, lack of near-real-time data, external threats, malware and DDoS attacks and much more. Your employees and customers are depending on you, so you've got to get it right the first time.

Fortunately, Infoblox can help. It all begins with authoritative IPAM to ensure that the state of network data matches the IP database to confirm a single source of truth for all end-points on the network. When data is accurate and reliable it can then be automated.

Discovery and visibility come next, along with the capacity to sync IPAM data in near-real-time regardless of the environment, on-premises or in the private, public or hybrid cloud. Next, the job is to keep the bad actors out, and for that, the leading global security ecosystem is engaged with integrations with top security vendors, cutting-edge security tools, leading platforms, automated threat detection, massive data sharing, remediation and more.

And finally, you need to be able to access and manage your data, whether looking back to complete an audit or forensic investigation, watching now to ensure app performance, data and infrastructure security or planning ahead to certify that you'll have the resources to sustain business continuity.

While it all seems daunting, it can't cost an arm and a leg. And it needs to be quick and easy to deploy, easy to use, flexible, secure, scalable and deliver five-nines reliability, mission critical expertise, global reach and world-class support.



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)