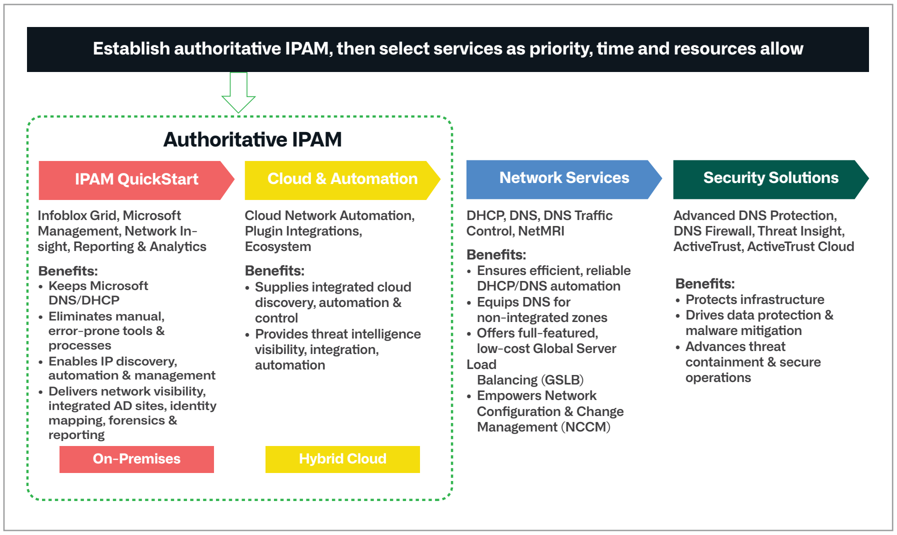
DATASHEET

IPAM QuickStart

AUTHORITATIVE IP ADDRESS MANAGEMENT (IPAM) FOR VISIBILITY, AUTOMATION AND CONTROL

Today's network complexities require accurate, near-real-time infrastructure, DNS- and DHCP-based discovery, centralized visibility on-premises or in the hybrid cloud, efficiencies and cost savings from integrated process automation, deep threat-intel from ecosystem integrations, defense against DNS-based attacks, automated reporting and predictive analytics for greater insight and control. Here's where Infoblox can help.



Establish authoritative IPAM, then select services as priority, time and resources allow

Authoritative IPAM

IPAM QuickStart

Infoblox Grid, Microsoft Management, Network Insight, Reporting & Analytics

Benefits:
- Keeps Microsoft DNS/DHCP
- Eliminates manual, error-prone tools & processes
- Enables IP discovery, automation & management
- Delivers network visibility, integrated AD sites, identity mapping, forensics & reporting

On-Premises

Cloud & Automation

Cloud Network Automation, Plugin Integrations, Ecosystem

Benefits:
- Supplies integrated cloud discovery, automation & control
- Provides threat intelligence visibility, integration, automation

Hybrid Cloud

Network Services

DHCP, DNS, DNS Traffic Control, NetMRI

Benefits:
- Ensures efficient, reliable DHCP/DNS automation
- Equips DNS for non-integrated zones
- Offers full-featured, low-cost Global Server Load Balancing (GSLB)
- Empowers Network Configuration & Change Management (NCCM)

Security Solutions

Advanced DNS Protection, DNS Firewall, Threat Insight, ActiveTrust, ActiveTrust Cloud

Benefits:
- Protects infrastructure
- Drives data protection & malware mitigation
- Advances threat containment & secure operations

AUTOMATED VISIBILITY AND ACCURACY

Network availability begins with Authoritative IPAM to identify the accuracy and status of network assets (e.g., IP addresses, subnets, and VLANs). Unlike manual spreadsheets, it automatically detects discrepancies between an IPAM database and the true network asset state to enable visibility, alerting, reporting and automated remediation for each endpoint— regardless of environment. With Authoritative IPAM, NetOps, Microsoft/Server and SecOps teams can share and be confident in accurate, reliable, near-real-time intel, automated discovery, clear visibility and control over the entire network, all from a single pane of glass.

KEY FEATURES

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, securityhardened, high availability and easy-tomanage 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.

CENTRALLY-MANAGED, RELIABLE AND SECURE DDI

The Infoblox Grid, using sophisticated technology embedded-in and linked-across distributed physical or virtual appliances, delivers discovery and automation for a reliable, secure, easy-to-deploy and manage platform. The Grid enables a central repository of network data, hosts, servers, dynamic clients and virtual environments for tracking and synchronization. It delivers High Availability, hardened system security and an integrated DDI database to ensure resilience, IPAM automation and guaranteed performance with significant labor and cost savings.

RELIABLE DISCOVERY AND CONTROL

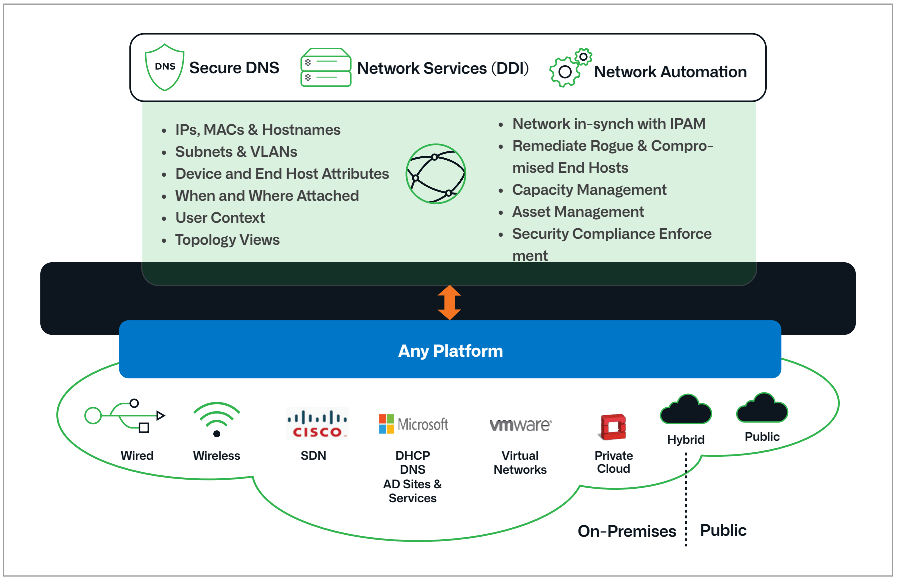
Whether on-premises or in the private, public or hybrid cloud, Infoblox Network Insight and Cloud Network Automation helps you discover all layer-2 and layer-3 devices, end-hosts, switch ports and VLANs, see into VRF space, integrate with multi-cloud platforms (e.g., VMware, OpenStack, Azure, AWS), sync with IPAM, manage ports, provision assets, detect and resolve IP conflicts, automate policies, support audits and distribute reports—all from a central unified platform.

ENHANCED MICROSOFT INFRASTRUCTURE VALUE

Devices. Apps. IoT. IPv6. Virtualization. The IPAM demand on networks is exploding. Teams preferring to keep Microsoft DNS/DHCP protocols can apply the agentless Infoblox Microsoft Management overlay to automate, scale and deliver efficient, highly available, secure and resilient environments.

INFOBLOX DISCOVERY-AUTHORITATIVE IPAM FOR ANY PLATFORM

The Foundation of a secured, Controlled Network



Infoblox Microsoft Management delivers central DNS/DHCP integration, DDI component syncing, AD Sites and Services and user/IP visibility, reporting and predictive analytics for resource planning. Adding it solves IP conflicts, DHCP availability issues, network outages and extends existing Microsoft infrastructure value.

KEY FEATURES CONT.

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 geodiverse on-premises, wireless and SDN environments for efficient, automated workflow management.

Cloud Network Automation and Plugins: Provides multi-cloud interfaces, (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.

ECOSYSTEM INTEL AND THREAT DATA SHARING

Control of accurate network database records, APIs and extensive security vendor integrations enable automation, contextual data sharing and customization with security, configuration management database (CMDB) and service management tools. Integrations with 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 data is shared with NAC and SIEM tools including Cisco ISE/pxGrid. With Ecosystem, automation discovers, scans, remediates and shares data for greater protection and manageability.

ACTIONABLE DATA AND INSIGHTS

Your network contains a wealth of business-impacting data about your network, clients and apps. Can you see it? Are you leveraging it to make your network better? Built on Infoblox DDI and the Splunk reporting and visualization engine, Reporting and Analytics provides role-based, plug and play search, 100+ pre-built, customizable dashboards and reports, summary, near-real-time alerting, historical and predictive views, granular query logging, security forensics and actionable data for on-demand tracking, audit, forecasting and control.

infoblox.

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