SOLUTION NOTE

THE KEY TO DELIVERING AN ALWAYS-ON WORLD: CARRIER-GRADE PERFORMANCE, RELIABILITY, SECURITY AND SCALE FOR TELECOMMUNICATIONS SERVICE PROVIDERS

Service provider portfolio overview

Infoblox solutions for service providers enable a safe, reliable, and fast first-connection impression to residential subscribers and enterprise customers.

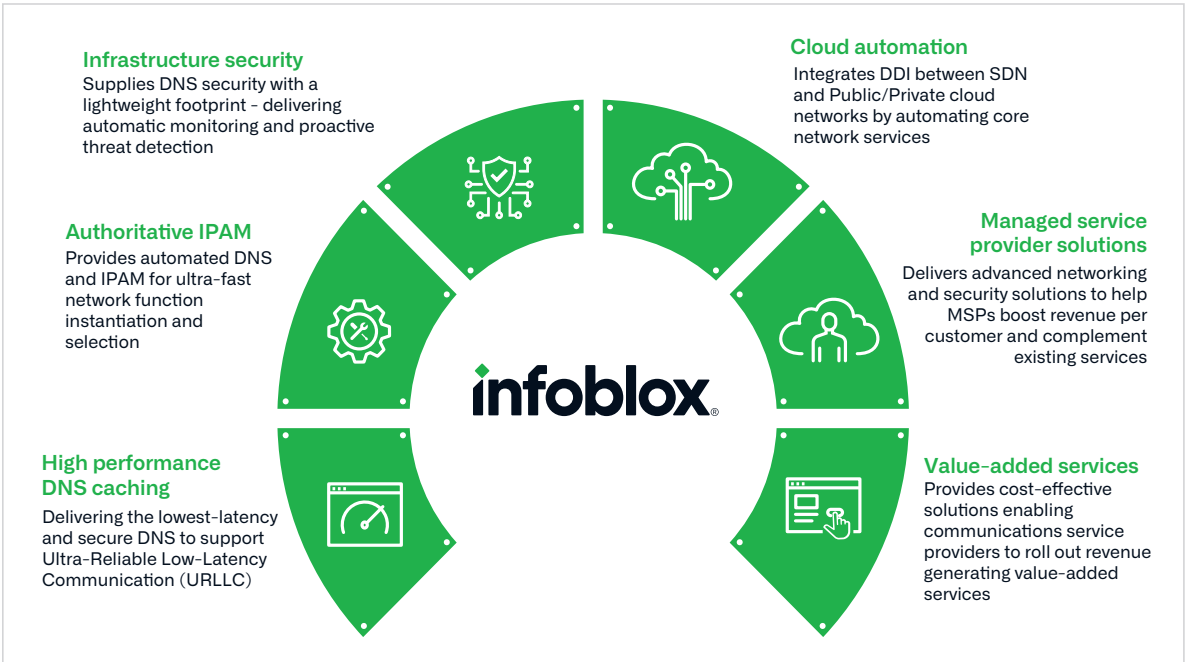
Security is one of the top criteria when selecting a service provider. Unsecured devices put network assets at risk, and dissatisfied subscribers can damage a trusted, valuable brand and reputation. Infoblox solutions provide highly cost-efficient control, improved subscriber experience, and protection from a wide range of DNS attacks and malicious website access.

THE INFOBLOX SERVICE PROVIDER SOLUTION PORTFOLIO

Infoblox delivers the intelligence, performance, and proactive protection service providers need to safeguard their networks, subscribers, and brand. All Infoblox solutions include patented Infoblox Grid™ technology, which provides optimal operator visibility and control across the entire Infoblox DNS infrastructure, enabling quick detection of service-threatening attacks while easing operational costs and increasing manageability.

INFOBLOX SERVICE PROVIDER INFRASTRUCTURE SERVICES

Deliver 5G speed and performance | Reduce operational costs | Increase top line revenue



HIGH PERFORMANCE AND SECURE DNS CACHING

Secure DNS caching protects subscribers from growing malware threats, service disruption, and slow response through the use of global threat intelligence and automated protection packages. The solution maintains critical DNS service availability in rapidly evolving networks, growing traffic, and even during a malicious DDoS attack. Advanced caching functions ensure that the best and most-used responses are always available for subscribers.

- **Infoblox secure DNS cache acceleration.**
  Offers the most robust and cost-effective DNS caching infrastructure solution, combining submillisecond response and advanced threat protection, maintaining low latency and a secure subscriber experience.
- **Infoblox encrypted DNS for service providers.**
  Provides efficient encryption for DNS over TLS (DoT) and DNS over HTTPS (DoH) while delivering Infoblox best-in-class DNS and value-added subscriber services.
- **Authoritative and recursive DNS.**
  With Infoblox DNS, you can enable and centrally manage and automate all aspects of authoritative and recursive DNS to achieve the high availability, efficiency, security, and application response times subscribers need to thrive in a digitally connected world.
- **DNS traffic control.**
  Instead of deploying costly global server load balancers (GSLB) to ensure availability, DNS Traffic Control eliminates costly delays in application response times. It uniquely combines advanced load balancing functionality with DNS management within a single, unified platform.

AUTHORITATIVE IPAM

The transition from 4G to the advanced realms of 5G, including non-stand-alone (4G/5G) and pure stand-alone 5G, rapidly reshapes the landscape of mobile service providers, be they industry giants or nimble challengers. This seismic shift, spanning the entire spectrum of telecommunications, necessitates a relentless pursuit of automation–and the bedrock of success lies in automating DNS, DHCP, and IP Address Management (DDI). These pillars are instrumental and imperative for the seamless deployment of 5G radios, the evolution of the next-generation 5G core, and the function of the 5G Session Management Function.

- **Automated IPAM and DHCP for 5G new radio.**
  Significantly makes the 5G radio deployment process more efficient and cost-effective by integrating operations support system/business support system (OSS/BSS) device data. For example, a radio serial number and MAC/DHCP Unique Identifier (DUID) can be scanned in the field to automatically create appropriate DNS and DHCP records for bare-metal provisioning services.
- **IPAM network assignment for the Session Management Function (SMF).**
  Unlike manual methods employed in 4G networks for user equipment IP address assignment, Infoblox automates the IPAM network assignment lifecycle for the SMF. Infoblox's automated IPAM assignment is invoked for initial network assignment and reclamation when the SMF is terminated.

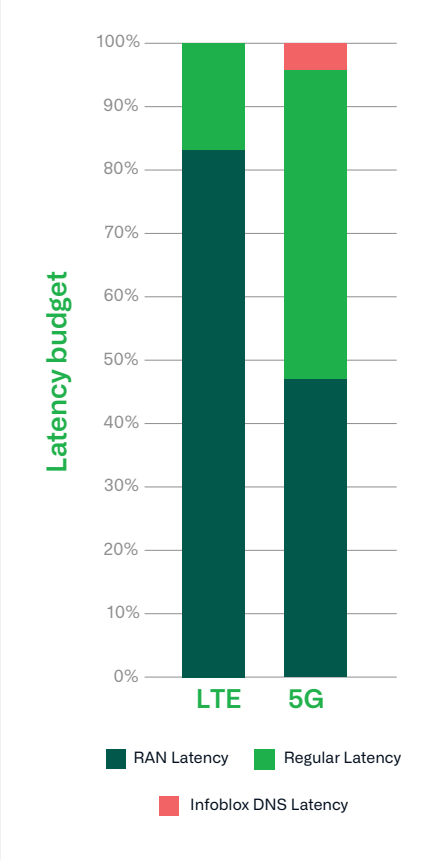


Figure 1: The Infoblox Advantage—Ultra Low Latency for 5G

- **Automated DNS for 5G core.**
  Founded on the principles of cloud-native computing with a fully automated lifecycle, the new 5G core not only replaces dedicated protocols with a modern service-based architecture (SBA), it also replaces the legacy gateway selection process with a new network repository function (NRF). Infoblox provides automated DNS registration for the 5G core to authenticate encrypted communications and provide a fully qualified domain name (FQDN) to IP resolution.
- **Secure and centralized DNS and IPAM for OpenRAN.**
  Infoblox can interface with the different OpenRAN platform management systems, providing critical and centralized DNS and IPAM. The Infoblox RESTful WAPI helps ensure the IP space perspective's overall integrity by interfacing across the different RAN management platforms, providing automated discovery and management across multiple data centers, cloud management platforms, and networks.
- **Mobile service selection.**
  The Infoblox mobile service selection solution provides the crucial service-selection information for elements within the mobile network Evolved Packet Core (EPC), supporting 3GPP-defined use cases and delivers carrier-grade performance and availability to provide a superior subscriber experience. Additionally, the solution dynamically monitors element status, supporting efficient assignments only to truly available nodes and reducing administrative operating costs.

INFRASTRUCTURE SECURITY

Constantly evolving threats and increased attack surface demand a foundational approach to security that is ubiquitous, scalable and automated. Leveraging threat intelligence and AI/ML-based analytics on DNS provides scalable protection against modern malware, command and control (C&C), data exfiltration, domain generation algorithms (DGAs) and more. In addition, traditional DNS open-source software and Internet-facing firewall appliances were not designed to address DNS-based attacks that could slow or crash a DNS server. Stopping these DNS attacks requires deep inspection with high compute performance to maintain network uptime during an attack.

- **BloxOne® Threat Defense.**
  Strengthens and optimizes a solution provider's security posture from the foundation, maximizing brand protection by securing existing networks and subscriber imperatives like 5G, IoT, the network edge and the cloud. It works with a service provider's existing defenses to automatically stop malware from spreading inside a network–automatically detecting malware at the DNS layer, preventing devices from connecting with malicious destinations, isolating compromised devices and then triggering their remediation.
- **Advanced DNS protection for service providers.**
  Maintains service availability during malicious attacks. It is available as a virtual add-on with software subscription pricing. It supports service availability, critical DNS functionality and performance during a volumetric DDoS attack or unexpected traffic spikes generated by misconfigured devices, emergency situations, or network outages.
- **Infoblox threat intelligence.**
  Rapid detection reduces subscriber complaints, providing up-to-date, coordinated threat intelligence from multiple sources. It greatly simplifies what it takes for service providers to shut down attacks early before they spread and cause harm. Infoblox Threat Intelligence integrates with security solutions such as BloxOne Threat Defense and updates the service provider's cybersecurity ecosystem in real-time on new and evolving malicious Internet destinations.
- **Infoblox ecosystem exchange.**
  Enables protection to keep pace against new threats, providing security professionals with a highly interconnected set of integrations that allow them to eliminate silos, optimize their security orchestration, automation and response (SOAR) solutions and improve the ROI of their entire cybersecurity ecosystem, including third-party, multi-vendor assets.

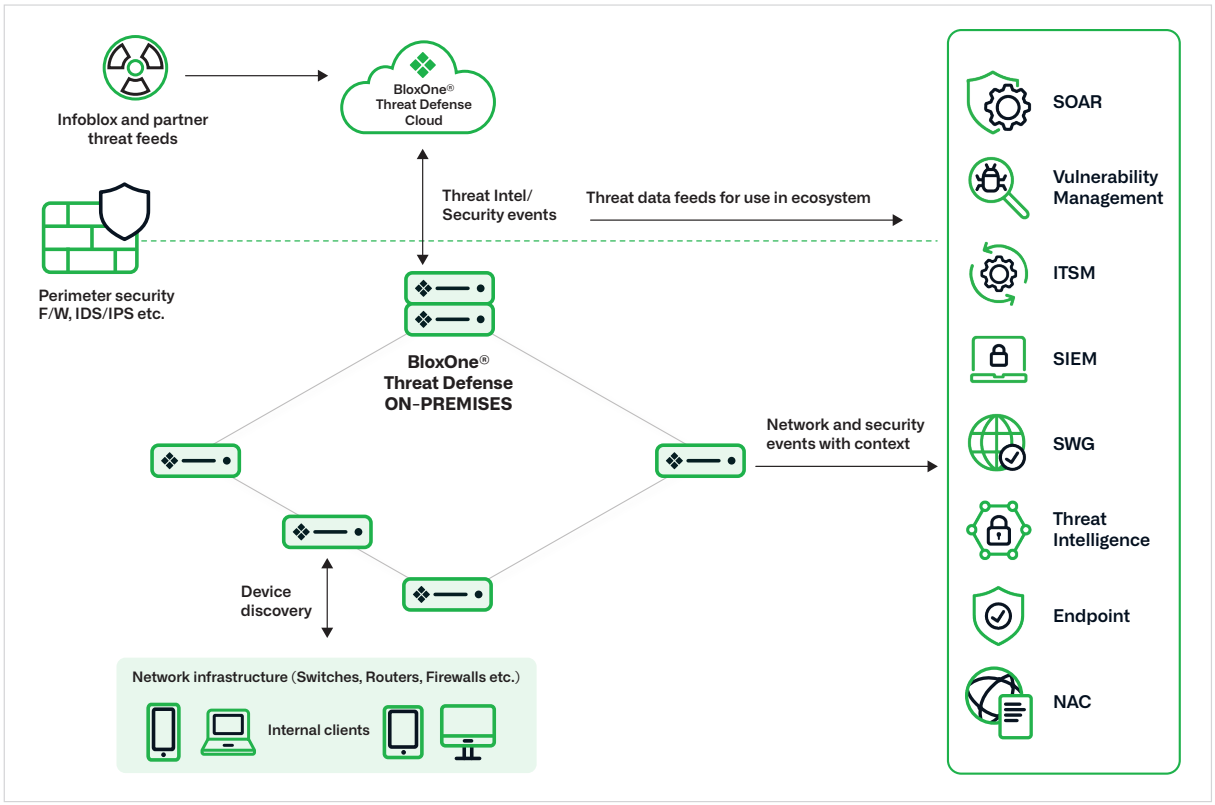


Figure 2: Infoblox hybrid architecture enables protection everywhere and deployment anywhere

CLOUD NETWORK AUTOMATION

Legacy DDI management approaches will not work in 5G environments environments and may delay critical deployments and dilute the automation and orchestration benefits that telco clouds promise to bring. Stale, duplicate and contradicting DNS records can cause significant problems in the network. Manual processes are error-prone, labor-intensive and non-scalable–forcing administrators to perform mundane activities instead of focusing on higher-value business initiatives.

- **Monitoring and accelerated troubleshooting:**
  vDiscovery automatically and dynamically detects detects virtual instances, tracks the resources and relationships within a single platform for complete visibility when new instances are created and cleans up records when instances are destroyed. It collects information about a specific VM, such as its virtual data center, virtual switch and virtual cluster.
- **Automated provisioning and de-provisioning.**
  Infoblox integrates with cloud orchestration technologies through a RESTful API, providing a fully-automated IPAM platform integrated into the container/VNF life cycle management. Cloud orchestration adapters including OpenStack, Ansible, VMware vRealize Orchestrator, Microsoft System Center Orchestrator, and others allow operators to simplify and streamline provisioning and de-provisioning of IP addresses to newly created VMs and containers, update DNS records and release IP addresses/DNS when the VMs are terminated.
- **Red Hat Ansible platform integration.**
  Infoblox NIOS Collection for Ansible Automation Platform saves time and money, enabling network professionals to utilize Infoblox infrastructure for DNS and IPAM automation of VMs and containerized workloads deployed across multiple platforms.

MANAGED SERVICE PROVIDER SOLUTIONS

As enterprises deploy hybrid clouds, expand security focus, implement IoT and roll out extensive digital economy solutions, many still use legacy DNS platforms and spreadsheets for managing IP addresses. These out-of-date, manual processes cannot meet the requirements of dynamically spinning up resources, handling latency-sensitive requirements and ensuring security and compliance. Also, DNS is the fastest growing threat vector for malicious activities, including malware propagation, data exfiltration and DoS attacks.

- **Cost-Effectively close the managed secure DDI gap.**
  Scalable licensing cost and billing structures that minimize up-front investments and provides flexible pricing models to fit the overall Managed Service Provider (MSP) strategy. Because DDI is businesscritical to the core infrastructure, MSPs can complement and expand existing network offers deeper into the customer networks.
- **Meet customers' needs with optimized deployment options.**
  Solve customer challenges with deployment models that include on-premises, virtual and/or cloud-based services. Managed Secure DDI services complement existing service offerings, allowing MSPs to minimize incremental service creation costs by keeping the same sales motions and using existing managed service staff, processes and tools.
- **Maximize profitability with cost-effective pricing models.**
  Through multiple pricing options that include CapEx purchase or OpEx subscription models, Infoblox pricing and deployment models allow MSPs to minimize up-front capital requirements when creating new services and easily scale as new customers are added.

REVENUE-GENERATING VALUE-ADDED SERVICES

Infoblox offers a robust, highly scalable DNS-based platform for delivering a comprehensive portfolio of value-added security services for fixed and mobile access. By consuming subscriber management information, Infoblox correlates identity to traffic, enabling policy enforcement and the identification of security incidents at the individual subscriber level for granular visibility. Moreover, the platform enables you to minimize up-front investments and generate a predictable ROI by leveraging a flexible, pay-as-you-grow model.

- **Monetize core network assets.**
  Generate new revenue streams with intelligent, value-added security services that can be upsold as data and mobile device security or consumer-controlled parental control solutions for their high-value installed base and new customers. Infoblox helps minimize the initial investment to launch value-added offers for both fixed and mobile subscribers through a cost-effective, scalable approach covering various market segments.
- **Easier subscriber attach.**
  With no software to download and install, subscribers are in complete control to configure and manage the solution across all of their devices with little operator intervention. Through the enablement of opt-out controls, service providers can provide free or bundled services by default to large groups of subscribers, offering them the choice and the means to discontinue the service if desired.
- **Predictable ROI.**
  Service providers can leverage their existing DNS infrastructure and investments, transforming it into a revenue-generating service. Our DNS-based approach reduces network impact because only the traffic from specific customers is analyzed. Infoblox also minimizes the up-front investment with a scalable solution and a pay-as-you-grow licensing model, so providers only pay for the number of subscribers using the service.

ADDITIONAL INFOBLOX ADVANTAGES

Infoblox solutions for service providers deliver the reliability, manageability, performance, and proactive protection service providers need to safeguard their networks, subscribers, and brand—enabling them to create the best first-connection impression for their subscribers. Additional benefits include:

- **Infoblox Grid.**
  Patented Infoblox Grid technology provides highly efficient management and control, freeing key technical and network operations staff from labor-intensive, costly, and error-prone administrative tasks; automates routine tasks such as updates, patches, and configuration changes; and provides a single centralized view of the entire network, with advanced reporting visibility for planners and operations teams.
- **Physical and virtual appliances.**
  Designed for service provider environments requiring scalable edge deployments, Infoblox solutions are available in multiple form factors, including network functions virtualization (NFV) options and carrier-grade appliances.
- **Infoblox Trinzic Flex.**
  Provides an NFV virtualized DDI solution that offers elastic scaling capabilities. Service providers can pay based on their needs through flexible capacity-based pricing and then scale the solution as requirements grow. Trinzic Flex appliances are covered under the Service Provider License Agreement Program (SPLA).
- **Advanced reporting.**
  Infoblox Trinzic Flex is a software appliance that provides service providers with scalable and flexible DNS, DHCP, and IP address management (DDI) solutions. It is designed to support network functions virtualization (NFV), cloud-based deployments, and hybrid and multi-cloud environments. Infoblox Trinzic Flex appliances can automatically detect the capacity of the virtual machine and scale to the appropriate platform without requiring additional hardware or licenses. Trinzic Flex appliances are covered under the Service Provider License Agreement Program (SPLA), allowing providers to pay based on usage and demand rather than fixed resources or models.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

DEPLOY INTELLIGENT NETWORKS FOR FUTURE 5G, EDGE AND ADVANCED BROADBAND

Infoblox solutions unite DNS, DHCP and IP address management (DDI) to automate network visibility, scalability and management. Infoblox gives networking teams solutions that provide a modern and agile DDI foundation for the telco cloud. With Infoblox, CSPs gain new levels of speed, automation and security they need to evolve their networks. Infoblox solutions deliver these results through centralized management that automates and simplifies networking and security from the data center to the edge. In addition, Infoblox enables massive scale with the highest levels of availability and resiliency that telecommunications networks demand while delivering total network visibility and automation to streamline, orchestrate and secure distributed network services from a single pane of glass.

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

Version: 20230915v1