

Infoblox NIOS DDI

Ensure Five-Nines Uptime and Operational Resilience with the Industry-Leading Software for Managing and Securing Critical Network Services

OVERVIEW & CHALLENGES

The enterprise IT stack keeps evolving, with new cloud, security and operational resilience requirements emerging seemingly every week. Yet in many organizations, the critical network services that underpin every user, device and application—that is, DNS, DHCP and IP address management (IPAM), or DDI—remain stuck in an earlier age.

These foundational network connectivity services are the definition of mission-critical: If DNS or DHCP fails, nothing can connect to the network and business operations grind to a halt, causing outages that can last hours and cost \$1.4 million per hour of downtime.² Bottom line, these critical network services absolutely must stay online and available, at all times and locations, no matter what. Because the moment these services fail—not days or even hours later—the entire digital business becomes unreachable and stays that way until they are restored. Nevertheless, many organizations continue to rely on fragmented DDI workflows that add blind spots, manual work and complexity, all of which slow down application rollouts, make integrations brittle and make outages far more likely.

Legacy approaches typically rely on a patchwork of spreadsheets, homegrown tools and, often, “freeware” DNS/DHCP services bundled with Microsoft Active Directory or open-source servers like BIND. These approaches were never designed to accommodate the scale, security expectations or cloud velocity requirements of modern networks, resulting in:

- **Limited visibility** across overlapping address spaces, clouds, tenants and sites
- **Manual, error-prone processes** for IP assignment, DNS updates and subnet planning
- **Inconsistent policies and controls** across on-prem, private cloud and public cloud
- **Complex, risky network changes** that make errors and outages more likely and complicate audits and compliance
- **Slow, cross-team communications** every time teams need to request IP address and DNS changes, delaying deployments and impeding business agility
- **Growing threat exposure** as DNS becomes a key vector for malware, ransomware and data exfiltration

KEY CAPABILITIES

- **Simplified Critical Network Services Management:** Gain scalable, consistent control over mission-critical DNS, DHCP and IPAM services from a single, unified interface. Standardize operations and reduce risk of configuration errors across on-premises, hybrid and multi-cloud environments with centralized policy, RBAC and integrated workflows.
- **Highly Available Architecture:** Maintain non-stop resilience for critical network services with built-in redundancy features such as HA pairs, DNS anycast and DHCP failover, eliminating single points of failure and ensuring continuous uptime for users and applications wherever they connect.
- **Identity Mapping with Rich Context:** Use NIOS to correlate DNS records, IP addresses and MAC addresses with usernames, device attributes and extensible metadata in an authoritative IPAM database. NetOps and SecOps teams gain the context they need to troubleshoot quickly, resolve conflicts and accelerate investigations.

Meanwhile, expectations for IT services keep rising. Users demand always-on, performant applications from anywhere. Business leaders expect the network to be reliable, agile and secure, enabling rapid adoption of cloud-based applications, AI initiatives and M&A integration—without ballooning costs or headcount.

Without a purpose-built, enterprise-grade approach that delivers visibility, automation and control over critical network services across all environments, IT teams will continue struggling to meet these needs.

THE SOLUTION: INFOBLOX NIOS DDI

Infoblox is the longtime market leader in critical network services and has been driving DDI innovation for more than two decades. Our flagship Network Identity Operating System (NIOS) was the original, category-defining DDI platform and continues to power many of the world's most demanding networks. Today, thousands of customers, including most of the Fortune 500, rely on NIOS DDI to keep their critical services online and secure.

Unlike freeware and DIY approaches to mission-critical DNS, DHCP and IPAM services, NIOS is purpose-built to:

- **Ensure network availability** for critical network services across on-premises, hybrid and multi-cloud environments
- **Unify management and delivery of DNS, DHCP and IPAM** on hardened infrastructure purpose-built for mission-critical services
- **Automate and accelerate NetOps and CloudOps collaboration** so cloud teams can move quickly deploying new environments and applications, while NetOps maintains pervasive visibility and control over IP addresses across the organization
- **Enable pervasive automation of critical network service operations** and seamless integrations with leading security, cloud and infrastructure-as-code (IaC) tools
- **Scale elastically** from small sites to large global enterprises and service providers, while ensuring the same non-stop availability and performance
- **Support modern hybrid and multi-cloud architectures**, including virtualization, containers and public cloud workloads

Additionally, unlike other DDI solutions, Infoblox augments NIOS with a rich, continually expanding ecosystem of value-added solutions and integrations. Expanded cloud capabilities, robust APIs and support for standards-based automation frameworks and toolsets help organizations reduce complexity, improve ROI and accelerate time-to-value.

Proven Business Impact

Independent research, as well as real-world results from thousands of customers, show that NIOS DDI can deliver significant operational and financial benefits, including:

- **\$7.1M DDI cost reductions** versus legacy, fragmented infrastructure
- **\$3.6M in savings** through DNS, DHCP and IPAM automation
- **346% return on investment (ROI)** with payback in less than six months
- **70% less time required to manage DDI**, thanks to integrated IPAM, automation and reporting
- **\$500K in productivity gains** from improved business continuity and fewer outages

- **Integrated On-Premises Threat Protection:** Protect users and devices against malware, data exfiltration and other threats by enforcing policy at the protocol layer, using Infoblox Threat Defense™ on-premises with NIOS. Administrators can easily define rules to redirect DNS queries to trusted destinations, quickly contain compromised endpoints and block malicious domains using curated threat intelligence directly on existing infrastructure.
- **Encrypted DNS:** Strengthen security posture and meet stringent regulatory mandates such as Zero Trust with built-in DNS encryption. NIOS now includes DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) encryption as a standard feature in Trinzic X6 deployments—so organizations can protect DNS traffic and meet evolving compliance requirements without needing separate licensing.¹
- **Broad Ecosystem of Value-Added Solutions:** Extend NIOS visibility, automation and control by adding capabilities like hybrid/multi-cloud discovery and synchronization, centralized management of Microsoft DNS/DHCP environments, advanced reporting and analytics, and more.

Additionally, organizations adopting NIOS DDI typically realize:

- **Significantly fewer outages and incidents** related to IP conflicts and misconfigurations, by replacing spreadsheets and manual updates with authoritative IPAM and automated workflows
- **Faster service delivery**, with up to 90 percent reduction in time needed to spin up new servers and network services in cloud and virtualized environments when using NIOS with modern automation toolsets
- **Simpler audits and compliance**, with up to 70 percent reduction in time spent on reporting and audit preparation using integrated DDI visibility and reporting

KEY FEATURES

Enterprise-Grade DDI for On-Premises, Hybrid and Multi-Cloud Environments

NIOS DDI delivers secure, resilient DNS, DHCP and IPAM for any architecture, whether organizations prefer to tightly control critical network services on-premises or are expanding into hybrid and multi-cloud environments. It provides a consistent foundation for critical network services across on-premises data centers and remote sites, virtualized environments and private and public clouds including AWS, Microsoft Azure, Google Cloud and Oracle Cloud Infrastructure (OCI).

With NIOS, organizations can:

- **Reduce operational complexity and errors** by standardizing DNS, DHCP and IP address policies and configurations across all locations and platforms
- **Minimize outages** by maintaining authoritative IP address information across on-premises networks and hybrid, multi-cloud and multi-tenant environments, and surfacing IP address overlaps and other risks
- **Maintain enterprise-wide consistency** by extending the same critical network service workflows and naming conventions to cloud-native workloads via vNIOS software and automation plug-ins
- **Ensure non-stop business resilience** with proven high availability (HA) and disaster recovery capabilities based on Infoblox Grid technology

Holistic Management and Visibility

NIOS centralizes control of DNS, DHCP and IPAM through the Grid Management Console, providing a single source of truth for the IP address space, DNS zones and DHCP scopes. (Figure 1.) Key capabilities include:

- **Authoritative IPAM database** with visualization of subnets, VLANs, address utilization and history
- **Integrated DNS and DHCP management**, with support for IPv4 and IPv6, DHCP failover, DNS anycast and DNSSEC
- **Role-based access control (RBAC)** and approval workflows to safely delegate tasks across teams
- **Smart folders and extensible attributes** to organize objects by business, security or operational context

- **Infoblox DNS Traffic Control:** Maintain non-stop application uptime and performance with DNS Traffic Control (DTC) load balancing. Also now included in standard NIOS, DTC uses protocol-layer intelligence to efficiently distribute load, detect critical network service failures and automatically fail over to preserve uptime. It can replace standalone load balancing solutions and deliver up to 100 percent annual savings on load balancing costs.
- **Infoblox DNS Infrastructure Protection:** Use this optional NIOS add-on to protect self-hosted DNS servers from DDoS, DNS hijacking, cache poisoning and other attacks on the integrity and availability of mission-critical DNS infrastructure. Keep websites and applications up and running by continuing to process legitimate queries even while under heavy attack.

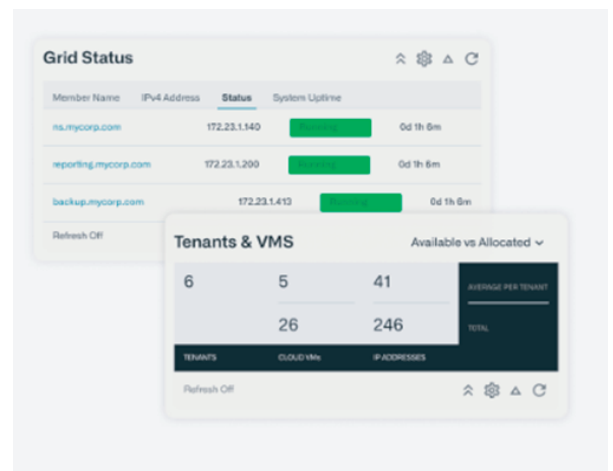


Figure 1. Grid Management Console

- **Real-time visibility** into device identities and ownership via IP-to-user and IP-to-device mappings, as well as visibility into cloud DNS services such as Amazon Route 53, Azure DNS and Google Cloud DNS

Organizations standardizing on the Infoblox Portal can also monitor and manage NIOS deployments alongside software as a service (SaaS)-based NIOS-X/Infoblox Universal DDI™ deployments, cloud-native DNS services (such as Amazon Route 53 and Azure DNS) and even third-party external DNS services hosted by providers such as Cloudflare and Akamai—extending pervasive DNS visibility and control across the entire digital estate. (Figure 2.)

Expansive Automation

As modern networks grow larger and more complex, the need to minimize manual effort and errors in day-to-day network operations becomes an essential requirement. NIOS DDI is designed to plug into existing automation pipelines and take advantage of standardized automation frameworks and IaC tools, so NetOps can move at cloud speed without sacrificing governance. (Figure 3.)

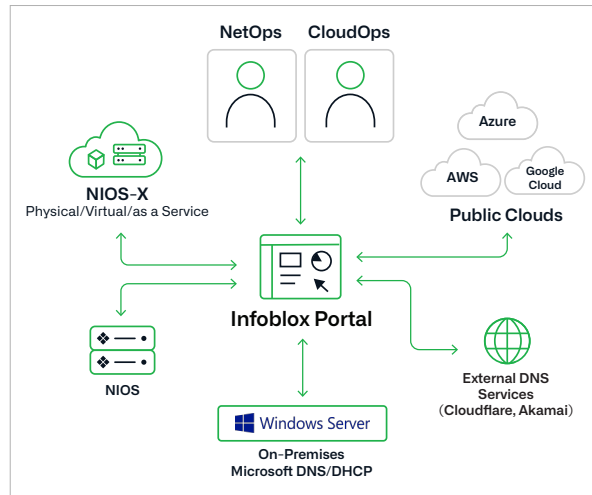


Figure 2. Manage NIOS instances alongside on-premises Windows Server environments, NIOS-X, public cloud DNS and third-party-hosted external DNS services from the Infoblox Portal

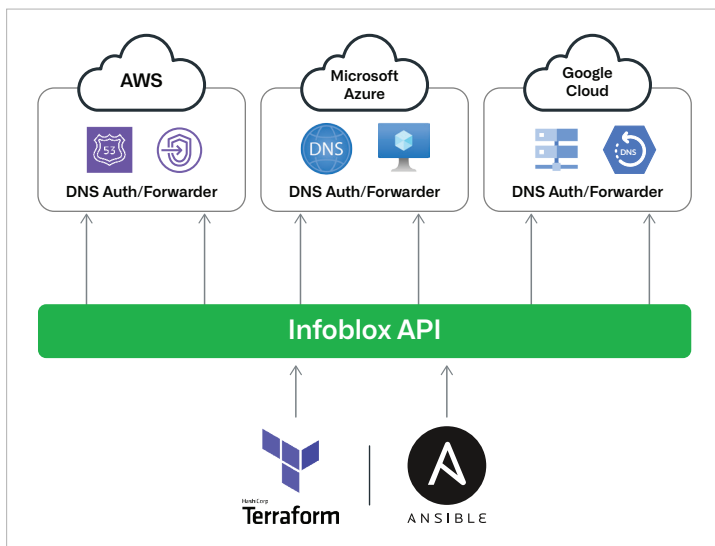


Figure 3. NIOS provides built-in IPAM and DNS integrations, along with the Infoblox API for faster configuration and deployment across on-premises and cloud environments

Key automation capabilities include:

- **Comprehensive REST-based Web API (WAPI)** with full object coverage for DNS, DHCP and IPAM
- **OpenAPI/Swagger specifications and universally unique object identifiers** to make automation code more robust and easier to maintain
- **Native integrations** with leading orchestration and IaC tools, including Terraform, Ansible, VMware, OpenStack, Kubernetes, Docker and more

These integrations reduce manual effort and errors, streamline provisioning of IP addresses and DNS records, and tie network changes directly into continuous integration (CI)/continuous delivery (CD) pipelines, lowering operational costs and improving consistency.

Flexible Deployment Options

Customers have multiple platform choices to run NIOS DDI, including physical, virtual and cloud-based appliances (Figure 4):

- **Infoblox Trinzic X6 Appliance:** This purpose-built hardware platform for NIOS delivers up to 50 percent better DNS and DHCP performance versus prior generations, with a hardened OS, redundant components and options for HA pair deployments. For detailed appliance specifications and performance metrics, see the [Trinzic X6 Enterprise DNS, DHCP and IPAM \(DDI\) Appliances datasheet](#).

- Infoblox vNIOS for Public Cloud (AWS, Azure, Google Cloud, OCI):** Virtual NIOS instances provide the same DDI functionality as on-premises appliances but can be purchased through hyperscaler marketplaces and deployed in public cloud environments. Customers can standardize DNS, DHCP and IPAM policies across data centers and clouds, and take advantage of NIOS PayGo pay-as-you-go, consumption-based licensing in AWS and Azure for self-service deployment of DDI services.
- Infoblox vNIOS for Private Cloud:** NIOS virtual appliances can also run on leading hypervisors and private cloud platforms, including VMware ESXi, Proxmox, Microsoft Hyper-V, Nutanix AHV, KVM, OpenStack and Red Hat OpenShift, enabling organizations to use their existing server infrastructure while maintaining enterprise-grade critical network services.

For detailed sizing guidance and platform specifications, please visit the [Infoblox Documentation Portal](#) for both NIOS [Physical Appliances](#) and [Virtual Appliances](#) (including vNIOS in public cloud).

Hybrid and Multi-Cloud Extensibility

NIOS supports HA deployment options across on-premises and cloud footprints, including HA pairs and Grid redundancy for on-premises and virtual deployments, and DNS anycast and DHCP failover for service continuity. vNIOS instances in AWS, Azure, Google Cloud and OCI bring the same enterprise-grade DDI capabilities to cloud workloads. (Figure 5.)

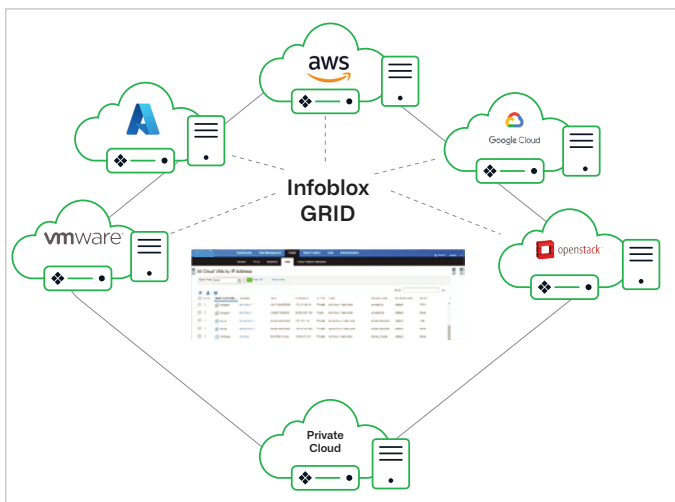


Figure 5. Only Infoblox can support traditional on-premises networks alongside private, hybrid and multi-cloud environments with authoritative single-control-plane visibility

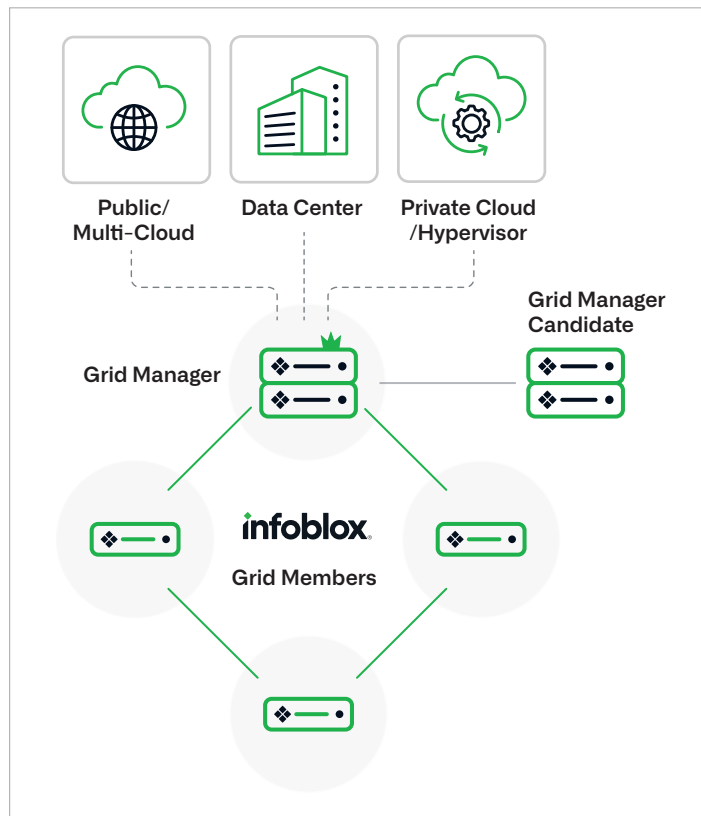


Figure 4. Deploy NIOS in on-premises data centers, hybrid environments and public and private clouds

For organizations that prefer a consumption-based model, NIOS PayGo offers pay-as-you-go licensing through AWS and Azure marketplaces. By taking advantage of PayGo options, organizations can quickly stand up NIOS DDI in cloud environments without traditional procurement, align DDI spend with cloud consumption, experiment with new use cases and scale up or down as business needs change.

Ongoing Customer-Driven Innovation

Recognizing that modern IT organizations are working under tight budgets, Infoblox continues to invest heavily in expanding NIOS capabilities to help customers realize more value from their critical network services investments over time. In fact, recent NIOS releases have added more than 110 major features and enhancements directly driven by customer feedback.

As part of these enhancements, several capabilities that previously required separate licensing are now included in the core NIOS product, including DNS Firewall and RPZ capabilities, DoT/DoH DNS encryption, [DTC load balancing](#), CP API automation, dnstap high-speed DNS logging and the NIOS outbound event API for real-time ecosystem integrations. Infoblox is committed to helping customers protect their investment and continually add new capabilities, without proliferating add-on SKUs.

NIOS Value-Added Solutions

On top of foundational DDI capabilities, NIOS offers a wide range of Value-Added Solutions (VAS) that extend visibility, automation and control, including:

- **Cloud Network Automation (CNA):** Multi-cloud discovery and control that automates DDI for private, hybrid and public cloud environments, with deep integration into cloud and virtualization platforms.
- **Network Insight (NI):** On-premises network discovery and control, correlating IPAM data with switches, routers, firewalls and endpoints to resolve conflicts, find rogue devices and improve operational efficiency.
- **Reporting & Analytics (R&A):** Integrated, Splunk-based DDI reporting and dashboards, with 100+ pre-built reports to accelerate troubleshooting, capacity planning, audits and policy validation.
- **IPAM for Microsoft Environments (Microsoft Management / MSM):** Centralized, bidirectional management of Microsoft DNS/DHCP and Infoblox DDI from a single pane of glass, so organizations can modernize how they manage critical network services right away—eliminating IP conflicts and operational silos—without having to rip and replace their Windows Server infrastructure.

These solutions are tightly integrated with the Infoblox Grid and Infoblox Ecosystem, so organizations can adopt advanced capabilities incrementally as their requirements grow.

INSIDE THE ARCHITECTURE: INFOBLOX GRID

Infoblox Grid is the architectural foundation of NIOS DDI. It links multiple NIOS instances—physical, virtual and cloud—into a single, integrated system with centralized management and distributed service delivery. Key characteristics include:

- **Real-Time, Authoritative Data:** Grid technology automatically consolidates, synchronizes and distributes DDI data across all members, ensuring that DNS records, DHCP leases and IPAM data remain accurate and consistent across sites and clouds.
- **Built-In Security:** The Grid uses encrypted communication between members, certificate-based authentication and SSL/TLS for management access. It is designed to minimize attack surfaces, support distributed denial-of-service (DDoS) resilience (when paired with [Infoblox DNS Infrastructure Protection](#)) and protect sensitive DDI data.
- **Consistent, Centralized Visibility:** A single control plane, accessible via both the Grid Management Console and the Infoblox Portal, provides unified visibility into all DDI objects and services, whether running on physical appliances, COTS servers, virtual machines or cloud instances.
- **Flexible Deployment Options:** Organizations can deploy Grid members as Trinziq appliances, virtual appliances or cloud instances, mixing and matching form factors as needed. The Grid architecture supports on-premises-only, cloud-only or hybrid designs with the same operational model.
- **Elastic Scalability:** The Grid scales from small environments to large global enterprises and service providers. Additional Grid members and services can be added as demand grows without rearchitecting the entire system.
- **Business Continuity and Disaster Recovery:** Grid Manager and Grid Manager Candidate (GMC) roles provide high availability for management, while support for HA pairs, DNS anycast, DHCP failover and distributed DNS services ensure resilience for protocol services.

KEY USE CASES

Organizations around the globe use NIOS DDI to solve some of their biggest, most urgent business and technical challenges, including:

- **Building an Enterprise-Grade Architecture for Critical Network Services:** Organizations struggling with the security, manageability and reliability of their current critical network services—often based on open-source software or Microsoft DNS/DHCP bundled with Active Directory in Windows Servers—are moving DNS/DHCP to infrastructure purpose-built to support them. By decoupling these mission-critical services from Active Directory and moving them to NIOS DDI, they eliminate single points of failure, ensure consistent policy and align with National Institute of Standards and Technology (NIST) recommendations for best-practice security and operational resilience.³
- **Ensuring Uptime and Business Continuity Critical Business Applications:** Organizations are using NIOS DDI's high-availability architecture and capabilities—HA pairs, DNS anycast, DHCP failover, DTC load balancing and Grid-based redundancy—to keep critical network services online at all sites, all the time. Using proven HA and resilience mechanisms, the network stays reachable even during data center failures, maintenance windows or large-scale migrations. By standardizing on NIOS for resilient critical network services, customers such as [Arvato Systems](#) have migrated thousands of servers and applications under tight deadlines with zero downtime and run production labs at 100 percent uptime for years.
- **Simplifying Hybrid Cloud DNS Management:** Many organizations using NIOS DDI do not stop at the borders of their on-premises networks. By integrating with AWS, Azure and Google Cloud, NIOS functions as a unified DNS and IP address platform for the entire enterprise. Teams can monitor and manage DNS everywhere—internal networks, public clouds, self-hosted websites and even on-premises Microsoft DNS environments—from one place, instead of juggling multiple disconnected toolsets.
- **Automating Critical Network Service Operations to Reduce Manual Effort and Accelerate Deployments:** Organizations are using expansive NIOS automation capabilities, automating via an interactive, standards-based Swagger/OpenAPI interface, using full API coverage in the NIOS Terraform provider to integrate directly with CI/CD pipelines, using Ansible playbooks to accelerate provisioning and changes, and more. Using modern API-driven automation frameworks and IaC tools, they are minimizing manual ticket-driven changes and pushing consistent policies across environments in minutes instead of days.
- **Building Highly Reliable, Redundant External DNS:** Many organizations run external authoritative DNS, the service that keeps websites, email and other internet-connected applications online, on the same enterprise-grade NIOS platform they use for internal networks. For those outsourcing external DNS services to a third-party SaaS or cloud host, NIOS can also provide a small, self-hosted redundant external DNS infrastructure to ensure critical sites and services are always reachable, even in the event of an outage in the SaaS/cloud service.

NIOS DEPLOYMENT OPTIONS

Infoblox offers a wide range of purpose-built TrinziC physical and virtual appliance options for NIOS DDI software, as well as virtual NIOS (vNIOS) images that run on those software appliances and on a broad range of hypervisors and clouds. No matter how organizations deploy NIOS, these purpose-built appliances deliver secure, resilient, high-performance critical network services.

For an overview of NIOS appliance options, visit the [Infoblox Platform Appliances](#) page at Infoblox.com or download the [TrinziC X6 Enterprise DNS, DHCP and IPAM \(DDI\) Appliances datasheet](#). For detailed, up-to-date vNIOS specifications for all supported hypervisors and clouds, see the [vNIOS X6](#) and [vNIOS X5](#) specifications pages on the [Infoblox Documentation Portal](#).

LICENSING

Infoblox offers flexible licensing options to align NIOS DDI with customer procurement and deployment models:

- **Subscription licenses** for on-premises hardware and virtual deployments, typically based on DDI object counts and feature bundles.
- **Usage-based NIOS PayGo** licensing for AWS and Azure marketplaces, providing self-service, consumption-based access to NIOS DDI without traditional sales cycles.

This flexibility lets organizations choose the model that best fits their financial, operational and cloud strategies while maintaining a consistent, enterprise-grade DDI platform.

CONCLUSION

Infoblox NIOS DDI turns fragmented, error-prone DDI infrastructure into a resilient, automated foundation for digital business. From on-premises data centers to multi-cloud environments, it delivers the visibility, security and agility required to keep every user, device and application securely connected.

By unifying core DDI services on a purpose-built, enterprise-grade platform, NIOS helps organizations modernize their networks without sacrificing reliability or control. IT teams gain the visibility, automation and extensibility they need to support hybrid and multi-cloud growth—while reducing risk, improving uptime and accelerating time-to-value.

-
1. DoT/DoH encryption and DTC features are available at no additional licensing charge for customers using NIOS on TrinziC X6 appliances. Customers using X5 deployments will still need to purchase additional licensing for DNS encryption and DTC. Support for dnstap logging and the NIOS outbound event API are now included in core NIOS whether deployed on X5 or X6 appliances.
 2. *The Rising Costs of Downtime*. Blau, Adam. BigPanda. April 25, 2024. <https://www.bigpanda.io/blog/it-outage-costs-2024/>
 3. *NIST Special Publication 800-81r3: Secure Domain Name System (DNS) Deployment Guide*. Rose, Scott. Liu, Cricket. Gibson, Ross. National Institute of Standards and Technology (NIST). March 2026. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.pdf>



Infoblox unites networking, security and cloud with a protective DDI platform that delivers enterprise resilience and agility. We integrate across hybrid and multi-cloud environments, automate critical network services and preemptively secure the business—providing the visibility and context needed to move fast without compromise.

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

+1.408.986.4000
www.infoblox.com