INFOBLOX DDI AND PROTECTIVE DNS SECURITY: MODERNIZE MICROSOFT DNS AND DHCP WITHOUT CHANGING YOUR EXISTING INFRASTRUCTURE

Centralize control with a native agent, bidirectional sync and a single cloud-native interface.

Infoblox equips Microsoft-enabled organizations with the tools to meet today's network and security challenges while preparing for tomorrow's demands. Bring existing Microsoft DNS and DHCP into a single, cloud-native control plane, without replacing current infrastructure.

Modernizing Microsoft networks is easier and more secure with Infoblox Universal DDI™ for Microsoft Management and Infoblox Threat Defense™. These solutions streamline critical network services while enhancing security—all in a unified platform. This united approach helps organizations increase agility, lower risks and evolve Microsoft infrastructure without a painful rip-and-replace scenario.

THE COST OF FREE: SIMPLIFY DNS AND DHCP MANAGEMENT WITH INFOBLOX UNIVERSAL DDI

Many IT organizations aim to cut costs using "free" Microsoft DNS and DHCP Server features for DNS, DHCP and IP address management (DDI). However, managing these "free" critical network services is time-consuming and operationally complex. Each server must be configured and managed separately, requiring every patch, update or configuration change to be performed independently. This increases risk, elevates costs and introduces more opportunities for human error.

Infoblox Universal DDI for Microsoft Management extends the value of your Microsoft infrastructure with secure, admin-controlled integration installed by Microsoft administrators offering bidirectional synchronization for consistent DNS and DHCP management, without elevated domain access. It coexists with Microsoft DNS and DHCP, allowing organizations to centralize management in a single portal alongside Infoblox NIOS and NIOS-X, reduce operational risk and maintain familiar workflows. Considering a move to the cloud? No problem. Infoblox offers the flexibility to modernize at your own pace across data centers, branches and cloud environments with our enterprise-grade full DDI platform. In the world of technology, a small upfront investment in a robust infrastructure solution can result in significant long-term savings.

FOUR BIG BENEFITS

1. **Unified management** for centralized discovery and control of critical network services across all Microsoft DNS and DHCP server deployments through a single cloud-native interface, including support for Infoblox NIOS and NIOS-X. Bidirectional synchronization keeps zones, records, scopes and leases aligned.
2. **In-depth visibility** for real-time monitoring and classification of network assets across the hybrid, multi-cloud environment, enabling organizations to validate usage against declared configurations.
3. **Role-based administration** for consistent permission-based access and control of all DNS and DHCP servers throughout the network, supporting least-privilege access and secure operational boundaries while reducing administrative overhead.
4. **Seamless integration** with the Infoblox Universal DDI Product Suite, Microsoft, NIOS, NIOS-X or other supported DNS platforms within a single portal, ensuring platform-agnostic management through a consistent workflow and API.

STOP CYBERATTACKS PREEMPTIVELY WITH INFOBLOX THREAT DEFENSE

Infoblox Addresses Critical Security Gaps in Microsoft DNS

80 percent of organizations recognize DNS security (Protective DNS) as vital for their overall security posture.[1] While Microsoft does not offer robust Protective DNS capabilities, Infoblox can close this gap with preemptive, DNS-layer security that blocks threats before they impact your Microsoft DNS Server environment.

By stopping threats before they enter the attack chain, Infoblox reduces the likelihood of an organization becoming "patient zero," minimizes security alerts, eases the burden on downstream defenses and saves significant SecOps time and resources. With centralized security across on-premises, cloud workloads, remote users and IoT/OT devices, organizations gain consistent protection and simplified policy enforcement—without the need to rip and replace existing infrastructure.

FOUR REASONS WHY

Adding Threat Defense to the Microsoft DNS Server environment offers:

1. **Preemptive Threat Detection:** DNS-focused threat intelligence and AI/ML technology preemptively block cyberthreats on average **68.4 days earlier**[2] than other security tools.
2. **Instant Protection:** Secure your Microsoft DNS environment with minimal configuration (see Figure 1).
3. **Real-Time Threat Intelligence:** Threat Defense continuously updates and adapts to emerging threats.
4. **Tangible ROI:** Organizations typically see a **315% ROI** and a **55% reduction in expected operational costs.**[3]

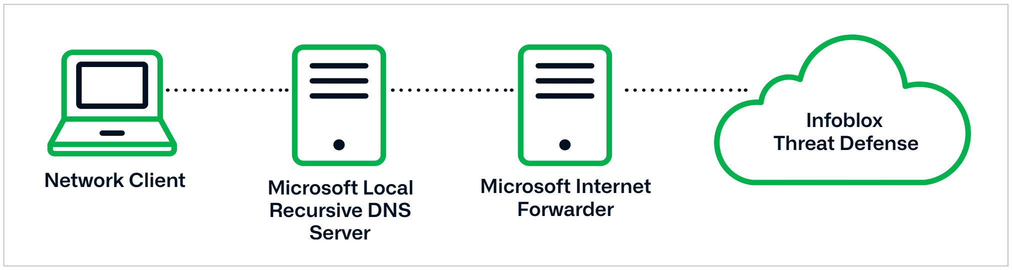
Network Client
Microsoft Local Recursive DNS Server
Microsoft Internet Forwarder
Infoblox Threat Defense

Figure 1. Connect the Microsoft DNS Server to Infoblox Threat Defense in just a few steps

ADD INFOBLOX CRITICAL NETWORK SERVICES AND SECURITY FOR UNMATCHED PERFORMANCE AND PROTECTION OF YOUR MICROSOFT NETWORK

By adding Infoblox Universal DDI and Threat Defense to the Microsoft environment, IT and security departments gain a unified platform that modernizes the network while boosting security and efficiency. And because Infoblox delivers Protective DNS on the same platform as Universal DDI, organizations can turn on security with minimal configuration, keep Microsoft admins in control and operate from one cloud-native portal.

Infoblox provides the performance and protection a Microsoft-run business requires to keep pace with the speed, change and overwhelming demands of today's most critical network and security needs. Do not wait for a costly outage or security breach. Proactively secure and streamline your Microsoft DNS and DHCP environment with Infoblox today.

[1] *2023 Global DNS Threat Report*, Fouchereau, Romain, International Data Corporation (IDC), August 2023. https://efficientip.com/wp-content/uploads/2023/09/IDC-2023-DNS-Threat-Report.pdf

[2] Infoblox Threat Intel customer research.

[3] *Analyzing the Economic Benefits of Infoblox Threat Defense™ Through DNS Threat Detection and Integrations*, Enterprise Strategy Group (ESG) Economic Validation Report, September 2025.

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