USE CASE BRIEF | CLOUD

infoblox

Identity Modernization

Decouple Critical Network Services from Identity Solutions to Accelerate Cloud Transformation

IMPACT SUMMARY

Minimizes Downtime: Drives down risk of cyberattacks or network outages that can grind a business to a halt.

Reduces Costs: Saves up to millions in operating costs annually that were previously devoted to managing identity and other critical network services.

Unleashes Agility: Empowers businesses to move more quickly and confidently, adding new applications, sites and clouds.

Strengthens Security: Dramatically reduces the risk and impact of a successful breach while accelerating security investigations and recovery.

69% faster network changes

70% fewer remote site outages

50%+ total cost of ownership (TCO) savings from modernizing legacy onsite network services

INTRODUCTION

As organizations look to accelerate cloud transformation, many choose identity—the systems that control access and authentication for every user and device—as a top priority for modernization. By migrating from traditional on-premises Active Directory to cloud services like Microsoft EntraID, Ping or other cloud identity solutions, they gain a more agile, flexible foundation for enterprise-wide identity, without the costs and complexity of managing access locally at each site.

However, identity modernization is only the first milestone in the journey to become a cloud-first business. If businesses do not take the opportunity to modernize all foundational network services at distributed sites—if they continue providing DNS/DHCP with the same legacy servers—they will continue to suffer from outages, inefficiencies and security gaps. Yet if they rearchitect these mission-critical services with anything less than an enterprise-grade, standalone platform, they will face ongoing performance, reliability and manageability issues that erode the value of cloud transformation investments.

CHALLENGE

Every application business users interact with, every minute of the day, depends on critical network services like DNS, DHCP and IP address management (IPAM), collectively known as DDI. If these foundational services fail, the company's networks and everything connected to them can go dark. Yet even after reimagining how the business handles identity services, too many organizations re-deploy DNS and DHCP as effectively "best effort" services—not treating them as the mission-critical, business-enabling services they are.

Orphaned Services Require Action

In theory, organizations could continue using the same DNS and DHCP services, running from the same legacy on-premises servers, even after migrating identity to cloud. Since many organizations modernize identity due to the costs and inefficiencies of maintaining legacy Windows Servers, however, most prefer to retire that onsite server infrastructure. Yet DNS and DHCP have to go somewhere.

If the organization opts to backhaul DNS to a data center, they will likely add significant latency, eroding the performance of every cloud and business app at those sites. If they move DHCP services to the wide-area network (WAN) router, they risk increasing the attack surface and diverging from the latest cyber resiliency recommendations, like those from the National Institute of Standards and Technology (NIST), that strongly recommend separation of duties for mission-critical services.[1]

Outages and Revenue Loss

Even when businesses migrate identity off on-premises servers, continuing to manage DNS and DHCP with legacy hardware and architectures impedes IT visibility, leading to wasted IP address resources, frequent IP conflicts and network errors—the number one cause of outages.[2] NetOps teams must constantly swivel between dedicated DNS services for each on-prem and cloud environment, none of which talk to each other. CloudOps teams struggle to quickly deploy applications, let alone automate tasks like provisioning new cloud environments. Additionally, when outages or security incidents occur, identifying affected devices can take hours, delaying remediation and extending their impact.

Inevitably, these challenges lead to business disruptions, failed compliance audits and potentially millions in lost revenues. One recent study found businesses without enterprise-grade DDI have cloud outages 44 percent more often and need 38 percent more time to fix them.[3]

Slow, Inefficient Operations

When IT teams try to manage critical network services across hybrid, multi-cloud environments using antiquated tools, even basic operations get complicated and expensive. Because each cloud provider handles provisioning of critical network services differently, teams must duplicate tasks manually across each cloud environment and their on-prem networks, a recipe for errors and delays. In fact, organizations relying on legacy DNS approaches spend 798 hours annually on network changes and 612 hours troubleshooting outages.[4]

Impediments to Cloud Transformation

Every modern business initiative, from cloud transformation to AI, assumes a highly reliable network. If the organization cannot trust that the network will always be available, they cannot move quickly to seize new opportunities, and every digital initiative carries extra risk. Yet outdated approaches to the foundational services that every application depends on increase complexity as the network expands, creating constant drag on the organization. Transformation initiatives become more expensive and take far longer than they should. One study found that IT teams relying on legacy DDI approaches are 34 percent less confident in their ability to deliver on cloud adoption goals than those using purpose-built, enterprise-grade tools.[3]

SOLUTION

Infoblox helps organizations modernize critical network services deployed alongside identity, so their digital foundation stays secure, reliable and agile as the business evolves. With enterprise-grade DDI capabilities designed from the ground up for hybrid, multi-cloud networks, organizations gain pervasive visibility and control. They can drive down errors and outages, improve operational effectiveness and ensure the non-stop resiliency that underpins successful cloud transformation.

Non-Stop Resiliency for Critical Network Services

Infoblox provides industry-leading capabilities to ensure resiliency of critical network services across hybrid, multi-cloud environments. Businesses can apply enterprise-grade high-availability capabilities like DNS anycast and automated failover to keep critical network services online and performant everywhere the business operates. That holds true whether businesses modernize with cloud-based, infrastructure-free DDI as a service or use onsite backup appliances that keep locations online even if the WAN goes down.

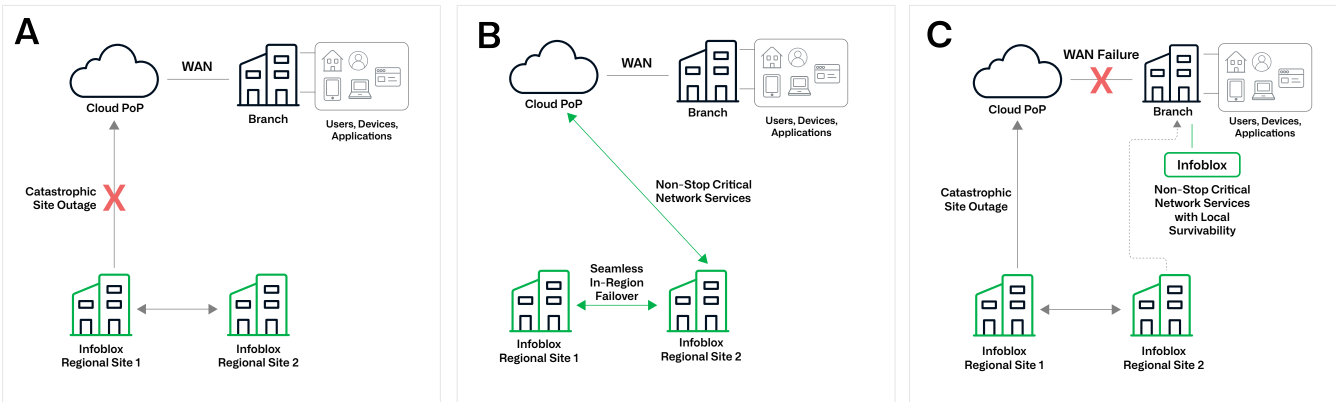

Figure 1. Non-stop resiliency during outage (A), with infrastructure-free (B) and local survivability (C) options

Comprehensive Visibility and Management for Hybrid, Multi-Cloud Networks

Infoblox gives IT teams a single, unified view of DNS, DHCP and IP addresses across hybrid, multi-cloud environments, helping them spot problems before they trigger outages. Infoblox provides:

- Unmatched visibility into critical network services across the hybrid, multi-cloud asset inventory from a single pane of glass
- The ability to surface forgotten DNS records, overlapping IP ranges and other common problems in hybrid, multi-cloud networks before they degrade performance or knock critical applications offline
- Universal IP address mapping and DHCP fingerprinting, so that teams investigating security issues and network problems can zero in on affected devices in seconds

Faster, More Efficient Operations

Infoblox provides the industry's only solution that automates and unifies management of critical network services, so teams can work faster, reduce errors and cut costs. Teams can monitor and control critical network services across the entire digital estate: on-premises networks, public and private clouds, and even website DNS services hosted by third-party providers like Cloudflare and Akamai. IT teams gain:

- Automated, policy-driven IP address allocation for all locations and clouds
- Real-time network data synchronization across the enterprise
- Ability to make changes once and automatically propagate them throughout their hybrid, multi-cloud environment

With these capabilities, NetOps, CloudOps and SecOps teams can use the same consistent tools and network data for all operations. They can drive down errors and outages, lower costs and accelerate timelines for application deployments and new cloud initiatives.

STAY AGILE AND RESILIENT AS THE BUSINESS EVOLVES

Moving identity services out of legacy on-premises servers is an essential step toward building a more secure, resilient cloud-first business. However, it is just one step. If organizations stop there—if they fail to modernize the other critical network services running at each local site—they will find themselves with an inefficient, unreliable IT foundation that cannot keep up with business growth.

By contrast, when organizations modernize DDI services, critical network operations become more automated and resilient. Businesses gain holistic visibility across the hybrid, multi-cloud environment. They benefit from lower costs, simplified compliance and an agile, highly reliable digital foundation for whatever comes next.

Success Across Real Customer Implementations

- One major oil and gas supplier went from 48 outages annually to zero after deploying Infoblox's enterprise-grade DDI solution, saving millions from avoiding downtime. Additionally, the company no longer needed to spend $1.3 million annually for a large team dedicated exclusively to managing on-prem DNS/DHCP infrastructure—and could instead redirect those investments to more strategic projects.
- A state K-12 education agency was spending $8 million annually to maintain its legacy identity deployment across 180 sites and wanted to retire Active Directory within two years. However, they wanted to continue delivering DNS and DHCP locally to ensure good performance and resiliency. With Infoblox, the agency deployed a centrally managed, enterprise-grade solution for DNS and DHCP at all sites, while moving to a modern cloud-based identity system. They improved resiliency and saved millions while implementing a more agile, reliable foundation for growth.

KEY CAPABILITIES

Enterprise-grade DDI tools automate IP allocation and DNS management, simplifying multi-cloud operations while reducing costs and errors.

Holistic visibility and centralized management help NetOps teams discover assets, monitor IP usage and centrally control network services across all locations and clouds.

Faster troubleshooting and improved security help SecOps and NetOps identify affected endpoints during outages or breaches with IP mapping and DHCP fingerprinting.

High availability ensures non-stop network services to keep the business running, using enterprise-grade resiliency strategies like DNS anycast, DHCP failover and Infoblox DNS Traffic Control.

Proactive security uses the protective DNS capabilities in the same DDI platform managing critical network services to preemptively block threats, lower costs and improve SecOps effectiveness.

1. NIST Special Publication 800-81r3. Secure Domain Name System (DNS) Deployment Guide, Rose, Scott, Liu, Cricket, Gibson, Ross, National Institute of Standards and Technology, April 2025.
2. Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short, South, Uptime Institute, June 8, 2022.
3. 9 Pitfalls of Not Using Enterprise-Grade DDI, Enterprise Strategy Group, February 2025.
4. Infoblox Authoritative IPAM for DNS and DHCP, Tolly Test Report, June 2022.

infoblox

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

Version: 20250918v1