infoblox

SOLUTION NOTE

BUILDING AN AGILE AND RESILIENT INFRASTRUCTURE

In today's fast-paced and competitive business landscape, agility and innovation drive a company's success. As technology continues to evolve, the modern network must be adaptable, keeping pace with innovation by leveraging the latest advancements, enabling the efficient deployment of new applications and services, and providing the flexibility needed to respond to changing market demands.

PACE OF MODERNIZATION IS RELENTLESS

By 2026, at least 50% of on-premises applications will modernize to integrate with SaaS management platform (SMP) tools, up from 20% in 2021, according to a Gartner report. With digitalization, networks are becoming more dynamic and changing all the time. Various factors, including remote work, multi-cloud expansion, new cybersecurity demands, and the need for new skill sets, contribute to the increasing speed of modernization.

SHORTCOMINGS OF LEGACY CRITICAL NETWORK SERVICES

Network infrastructure comprises many components – firewalls, routers, switches, Wifi devices, domain name servers, DHCP servers, etc. Most critical infrastructure elements are already upgraded to modern hardware or software versions. What about domain name servers and DHCP servers? Are your core network services still legacy? Relying on legacy network services – freeware, do-it-yourself or disparate systems is a huge roadblock for your digital journey.

- **Legacy systems are disjointed**: Manual management is costly and has a high risk of downtime and outages.
- **Legacy systems are slow**: Networks must be agile to adopt new ideas and technologies as a part of strategic initiatives for digitalization or M&A.
- **Legacy systems are exposed**: Security gaps and lack of contextual awareness result in inefficient and delayed remediation of threats.

DNS and DHCP are critical to all networks, and if you are still leveraging native services, your network is subject to massive outages.

KEY DRIVERS OF MODERNIZATION: WAY FORWARD

Organizations are modernizing their network to address the challenges of the ever-growing regulatory landscape, resource constraints, constantly evolving threats and skills gaps in the security sphere. They must constantly reduce downtime, manage overhead, and minimize security breaches to deliver 100% uptime, embrace new ideas, and enhance the existing security stack. This calls for rethinking approaches to critical network operations including DNS, DHCP and IP address management (collectively "DDI"). Here are the key drivers to modernize your network.

STREAMLINE OPERATIONS: REPLACE FREEWARE WITH PURPOSE-BUILT TOOLS

Free is not free. Though initial capital expenses may seem lower, the operational expenses you would incur using free or low-cost DDI tools will outweigh the advantages. Freeware solutions like Microsoft or open-source tools cannot scale for growth because of system limitations and lack of advanced features to support high availability, the discovery of unused virtual machines, policy-based validations, etc. Microsoft infrastructures are prone to outages and downtime either due to constant patch updates or they need to move to Azure AD. Manual management of distributed sites adds to inefficiency and increases overhead costs.

The best approach is to leverage **purpose-built tools** to simplify and streamline mission-critical operations. These tools are built for globalization and allow you to reduce operational tasks by seamlessly expanding to diverse infrastructure and remote locations. They simplify management, optimize maintenance, and reduce time by providing automation, discovery and centralized network visibility. They provide zero downtime upgrades and reduce downtime by providing high availability at scale.

ACCELERATE INNOVATIONS: USE A SINGLE CENTRALIZED TOOL INSTEAD OF DISPARATE SYSTEMS

Most enterprises use two to four DNS solutions, making it harder to manage critical services and respond to issues faster. Organization and informational silos often cause delays and errors. Different naming conventions and operational models across multiple cloud providers lead to misconfigurations and downtime. Fragmented visibility across the networks increases the time taken for troubleshooting and auditing.

Organizations must find an efficient and effective solution to accelerate innovations and enable business initiatives such as multi-cloud expansion, mergers and acquisitions, etc. Investing in a **centralized tool** will enable you to achieve these objectives through automation, a single DNS naming convention, and visibility across on-prem and cloud networks. Instead of using a mix of disparate systems, you can adapt faster to business needs and reduce inefficiencies with a centralized tool. It provides policy control and consistency, faster troubleshooting, and better collaboration, eliminates misconfigurations and errors and lowers audit and compliance risks and operational costs.

PROTECT BRAND INTEGRITY: LEVERAGE DNS TO DETECT THREATS EARLY

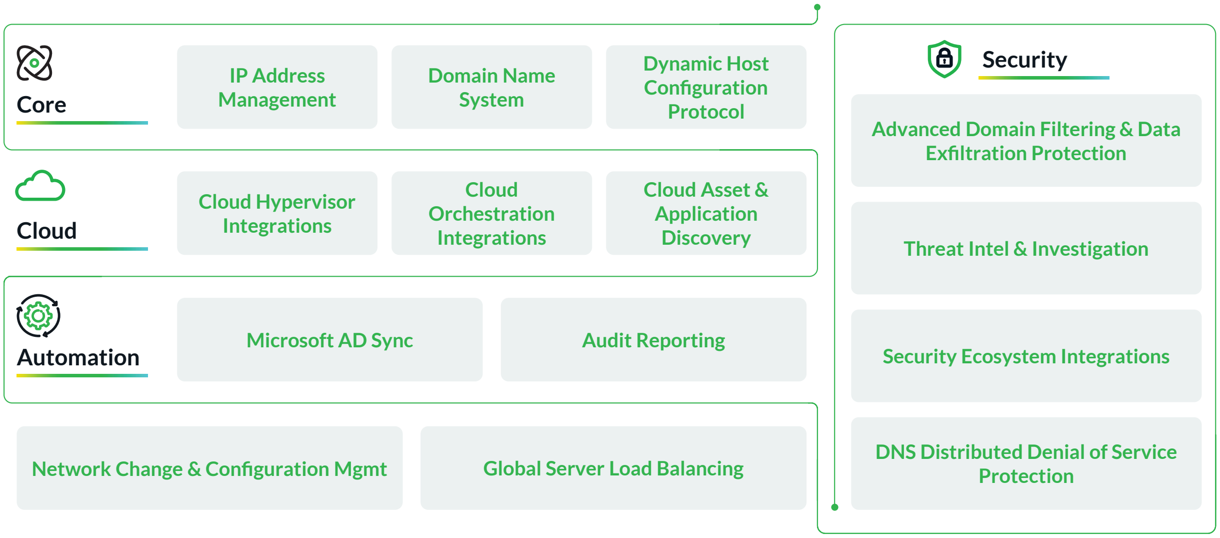
The constantly evolving realms of the threat landscape, such as malware, ransomware, lookalike domains, data exfiltration, and phishing, are huge risks for brand identity and data protection. A significant security gap exists as existing market solutions overlook DNS and fail to preempt attacks. In the past year only, hackers used nearly 42,000 imposter domains in a massive phishing attack. In addition, siloed and disparate systems, skills shortage, manual management, and lack of contextual awareness result in SecOps inefficiencies and delayed response times.

Detection of threats early reduces risk and closes the security gap. Leveraging **DNS-based threat hunting** detects and blocks threats earlier, as most cyber-attacks rely on DNS. Using DNS as a first line of defense protects against data exfiltration, domain generation algorithms, and imposters and secures all IoT/OT devices. It improves SecOps efficiency by reducing investigation time, automating remediation, and proactively assessing vulnerability risks.

INFOBLOX SOLUTIONS FOR AGILE AND RESILIENT INFRASTRUCTURE

Visibility, Automation and Control

Infoblox gives organizations unparalleled visibility, automation and control over who and what connects to their network. Infoblox significantly reduces costly downtime by eliminating cumbersome and mandatory maintenance, automates labor-intensive operational tasks, and reduces the burden associated with network asset inventory management. Infoblox solutions are built with security in mind reducing false alerts with increased contextual awareness and improving efficiency. Infoblox provides:



Core

IP Address Management

Domain Name System

Dynamic Host Configuration Protocol

Cloud

Cloud Hypervisor Integrations

Cloud Orchestration Integrations

Cloud Asset & Application Discovery

Automation

Microsoft AD Sync

Audit Reporting

Network Change & Configuration Mgmt

Global Server Load Balancing

Security

Advanced Domain Filtering & Data Exfiltration Protection

Threat Intel & Investigation

Security Ecosystem Integrations

DNS Distributed Denial of Service Protection

Figure 1: Infoblox solutions

CONCLUSION

Modernization drives digital transformation. Choosing the right solution for your network drives continuous modernization. Legacy approaches to managing critical network service will hinder your ability to innovate swiftly, adapt to changing business demands, and remain competitive. Leverage the visibility, automation and control that Infoblox provides to modernize your network at the speed that is needed and suitable for your business growth.

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: 20230803v1