

SOLUTION NOTE

TRANSFORM HEALTHCARE: OPTIMIZE IT OPERATIONS, SECURE DATA AND IMPROVE PATIENT OUTCOMES

SUMMARY

With Infoblox solutions, your healthcare organization can simplify and modernize critical network services while improving security, leading to higher efficiency and better patient outcomes.



Infoblox solutions streamline and automate the foundational services that make modern networking possible—DNS, DHCP and IP address management (DDI). Together, our enterprise-grade DDI and comprehensive security capabilities empower you to increase operational efficiency, reduce cyber risks that target the healthcare industry, safeguard patient data and improve care. These capabilities empower your healthcare organization to adapt quickly, scale securely and deliver reliable service in an evolving regulatory and threat landscape.

OVERVIEW & CHALLENGES

Thriving healthcare organizations like yours have embarked on an IT modernization journey. Cloud-first strategies, increasing cyberthreats and rising patient expectations are accelerating this shift and exposing critical gaps in visibility, security and operational control. Hybrid and multi-cloud environments are becoming standard, yet many healthcare organizations still rely on legacy, fragmented systems and siloed teams. Cyberattacks, such as ransomware, are increasingly—and often successfully—targeting healthcare companies, impacting operational efficiency and causing delays in patient care. Disjointed critical network services lead to network misconfigurations and poor asset visibility, exposing operations to pervasive threats that traditional security tools cannot detect. Lastly, aging infrastructure, rising scalability and evolving regulatory compliance requirements only add complexity.

Infoblox can help you bridge these challenging gaps. By providing unified and automated critical network services and strengthening your cybersecurity posture, Infoblox enables your organization to operate with greater speed, resilience and confidence while enabling better patient outcomes.

KEY BENEFITS FOR HEALTHCARE ORGANIZATIONS

- **Accelerate Cloud Transformation:** Centralize and automate critical network services and bolster security across hybrid and multi-cloud infrastructure.
- **Maximize Uptime and Reduce Outages:** Ensure network services that connect patients, medical staff and devices are always available.
- **Secure Your Network and Prevent Breaches:** Protect all devices (traditional, IoT, IoMT) to maintain uninterrupted patient care and safeguard sensitive data.
- **Simplify Regulatory Compliance:** Automatically assess and ensure compliance with evolving regulations, avoid legal penalties and sustain customer trust.

Challenges Healthcare Organizations Face and the Consequences of Maintaining the Status Quo

Challenge	Description	Consequence	Description
Operational Complexity	By 2027, hybrid, multi-cloud will dominate IT in healthcare. ¹ Managing these systems and integrating data can create silos and delays, increasing operational complexity and reducing agility.	Rising Operational Costs	Maintaining legacy infrastructure requires more effort and manual oversight. The cost of downtime and troubleshooting can exceed the cost of investing in automation and centralized control. IT budgets may shift from strategic projects to firefighting and patching.
Cybersecurity Pressure	Healthcare organizations often face cyberattacks due to the sensitive data they handle. In 2024, 734 significant data breaches occurred in the United States, compromising 261 million patient records. ²	Increased Exposure to Threats	Without proactive measures, healthcare organizations remain vulnerable to cyberattacks. Recovery can be costly and disruptive and damage the organization's reputation and regulatory standing.
Regulatory Compliance Burden	Healthcare must adhere to regulations like HIPAA, HITECH, GDPR and NIS2. Ensuring compliance requires detailed logging, reporting and staying updated on evolving requirements.	Compliance Gaps	Non-compliance can lead to fines, legal penalties and loss of trust, attracting regulatory scrutiny and damaging the organization's reputation.
Scalability and Resilience	Healthcare organizations need scalable and resilient network services to avoid downtime and maintain operations. This ensures patient services remain uninterrupted.	Inability to Scale and Adapt	Without scalable services, handling increased traffic and ensuring high availability becomes challenging, leading to service disruptions and patient dissatisfaction.

THE INFOBLOX SOLUTIONS

Infoblox solutions enable your healthcare IT organization to meet the complexity, scale and security demands of on-premises, hybrid and multi-cloud environments. The Infoblox Universal DDI™ Product Suite combines DNS, DHCP and IP address management (IPAM) to simplify and automate network operations across your existing legacy and cloud-based infrastructure. By unifying these critical network services in a centralized platform, the solution eliminates manual errors, reduces provisioning delays and ensures consistent policy enforcement across distributed environments. In addition, it provides comprehensive visibility and analysis of all assets across public clouds, on-premises networks, IoT/IoMT devices and third-party applications, enabling teams to troubleshoot faster while avoiding resource conflicts.

Traditional security measures are insufficient against evolving malware and AI-driven threats. Most tools detect and respond reactively, only after a breach occurs. Infoblox Threat Defense™ uses industry-leading DNS threat intelligence and algorithmic detection to preemptively block devices from accessing malicious domains, proactively safeguarding healthcare operations against cyberattacks. These capabilities integrate into broader security ecosystem tools, such as security information event management (SIEM) platforms, improving visibility and accelerating response times.

Infoblox Universal DDI and Threat Defense can help your networking and security teams streamline operations, strengthen cyber resilience and meet compliance requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, General Data Protection Regulation (GDPR) and Network and Information Security Directive (NIS2), while supporting flexible deployment models and centralized cost control. With built-in automation and API support, Infoblox enables your organization to move faster, scale efficiently and stay ahead of operational and regulatory risks to offer patients better care.

KEY USE CASES

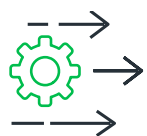
Infoblox solutions support several high-impact use cases that help healthcare organizations modernize infrastructure, improve operational resilience and strengthen their security posture. These scenarios reflect the specific demands healthcare organizations face in scaling operations, protecting sensitive patient data and enabling modern networking environments.



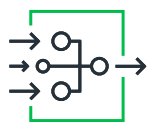
Supporting Network Services Transformation: Infoblox enables healthcare organizations to modernize aging and siloed infrastructure by centralizing DNS, DHCP and IPAM through its enterprise-grade DDI platform. These services are delivered consistently across on-premises, hybrid and multi-cloud environments, allowing teams to replace manual, error-prone processes with automated workflows. Infoblox supports extensive API integration, helping to unify systems and tools while accelerating network provisioning. The result is a more agile, secure and scalable network foundation that reduces operational costs and enables faster service deployment.



Minimizing IP Address Conflicts: In response to the explosion of connected devices—traditional, IoT, IoMT—Infoblox automatically detects and resolves IP address conflicts before they disrupt services. Real-time alerts, centralized IP address tracking and historical data analysis give teams the visibility needed to manage network changes and prevent conflicts and misconfigurations proactively. Automating IPAM helps healthcare organizations avoid costly outages, reduce troubleshooting time and free up resources for higher-value initiatives, especially in dynamic, multi-cloud environments.



Facilitating Business Continuity and Disaster Recovery: Infoblox ensures local survivability and continuous network operations during outages through local DNS caching, resilient architecture and automated failover processes. This helps healthcare organizations maintain critical network services, protect against security vulnerabilities and reduce dependency on central infrastructure, ensuring operational efficiency and the continued availability of crucial patient services and care.



Simplifying Network Consolidation Due to Mergers and Acquisitions: Infoblox's centralized DDI solutions facilitate the seamless integration of disparate networks during mergers and acquisitions. Enhanced visibility, automated processes and robust security features help healthcare organizations manage expanded network infrastructures, reduce operational complexity and protect against potential threats and vulnerabilities.

WHY HEALTHCARE ORGANIZATIONS CHOOSE INFOBLOX

- **Hybrid and Multi-Cloud Ready:** Ensure consistent critical network services across on-premises and multi-cloud environments.
- **Protective DNS:** Identify and block threats like ransomware preemptively with algorithmic detection and DNS-centric threat intelligence.
- **Complete Infrastructure Visibility:** Monitor IP activity, DNS traffic and connected devices from a single console.
- **Built-In Resilience:** Enable business continuity during outages with local caching and automated failover.
- **Streamlined Automation:** Reduce manual work and accelerate provisioning with API-driven orchestration.
- **Compliance Confidence:** Support evolving regulations through granular logging, policy enforcement and reporting.



Preemptive Protection from Ransomware and Data Breaches: Infoblox Threat Defense leverages DNS threat intelligence to detect and block malicious domains early in the attack cycle, disrupting ransomware and preventing data breaches. Proactive detection, automated response and comprehensive visibility into DNS traffic help healthcare organizations maintain regulatory compliance, protect sensitive financial data and continuously protect patient services.

CONCLUSION

As a thriving healthcare institution, your organization understands the need to modernize infrastructure while managing rising operational demands, sophisticated cyberthreats and evolving compliance obligations. Achieving these goals requires a network foundation that can scale efficiently, reduce complexity and build trust in every digital interaction. Infoblox solutions provide that foundation through a unified approach to critical network services and Protective DNS security. They empower your teams to centralize and automate DDI across all environments, reduce complexity and proactively safeguard healthcare systems, infrastructure and data.

With Infoblox, your healthcare organization can scale faster, detect threats earlier and ensure continuous network service delivery. Whether enabling cloud innovation or maintaining regulatory readiness, Infoblox helps you operate securely, efficiently and without compromise.

1 [2024 Nutanix Enterprise Cloud Index Report: Healthcare Industry Findings](#), Nutanix, April 2024.

2 [Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information](#), U.S. Department of Health and Human Services Office for Civil Rights, January 1, 2024–December 31, 2024.



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