infoblox

CASE STUDY

Global transport and logistics company

Industry: Shipping and logistics

GLOBAL TRANSPORT AND LOGISTICS COMPANY MODERNIZES NETWORK FOR RELIABILITY, VISIBILITY AND EXPANSION

Overview

From its modest beginning, a transportation, shipping and logistics company has brought people and packages together for over 100 years. Today, its operations are global with over 200K employees delivering nearly 25M packages daily through over 1M shipping customers to 11M recipients. It conducts business in over 200 countries and territories on 7 continents through warehousing, logistics and retail facilities, and over 100K delivery vehicles. The company also manages domestic and international air operations, with a fleet of nearly 600 aircraft and close to 2K domestic and flights each day to more than 750 domestic and international airports in the Americas, EMEA and Asia-Pacific.

With such a critical and massive global operation, reliability is more important than ever to the company's reputation and success. So in 2019, with widespread network visibility and performance challenges and the pending renewal of an outdated BlueCat network, the company turned to Infoblox for help in modernizing its core network infrastructure. The BlueCat network was unreliable, difficult to manage, could not provide discovery, audit visibility or share DNS, DHCP and IPAM (DDI) metadata across global IT deployments.

Infoblox outlined a multi-phase project to modernize the company's global network services. Its first priority was a like-for-like DDI upgrade to ensure network uptime, and centralize, simplify and automate protocol services. Phase two called for adding global network discovery and visibility. Future phases targeted redundancy, local Internet access and survivability, enhanced security and cloud expansion.

Through business consultation, architectural design and Professional Services, Infoblox was able to help the company modernize its global network for uptime and reliability, solve its discovery and visibility needs and enable future capabilities for business continuity, security and cloud services.

CUSTOMER PROFILE

A global transportation, shipping and logistics company delivering nearly 25M packages per day in over 200 countries and territories on seven continents through over 200K employees.

WHY CHANGE

The company prioritized three initiatives:

1. Establish reliable network uptime, and centralized, simplified, and automated protocol management through a like-for-like BlueCat DDI replacement;
2. Deploy global network discovery and visibility; and
3. Add global redundancy, local survivability, security and hybrid, multi-cloud expansion.

WHY NOW

The company's BlueCat platform presented an untenable operating environment:

1. Operating System and configuration upgrades were manual, complicated, inconsistent, error prone and expensive;

THE CHALLENGE

Centralize and modernize global networks

Beset with increasing global network availability, complexity, visibility and audit challenges, the firm's outdated BlueCat platform was approaching contract renewal. In September 2019, the company invited Infoblox to join a competitive technical evaluation against EfficientIP. Infoblox presented the best overall technical solution, migration plan, cloud roadmap, professional support and value. In response, the company engaged Infoblox with a multi-phase project to deliver three key priorities: 1) replace BlueCat and (eventually Microsoft components) through a like-for-like DDI upgrade to establish reliable network uptime, and centralized, simplified and automated protocol management (see Figures 2 and 3); 2) deploy global network discovery and visibility (see Figure 1); and 3) add global redundancy, local survivability, security and hybrid, multi-cloud expansion (see Figure 3).

THE SITUATION

Ensure global uptime and consistency

Network Upgrade Challenges: The company is driven by providing critical transportation services daily around the globe. However, since its BlueCat platform was not a centralized solution, operating system (OS) and configuration upgrades had to be updated manually on each appliance. This challenge was disruptive to its mission. Since there was no underlying user interface or backend synchronization, each appliance had to be rebuilt from scratch taking 4-8 hours per box. This deficiency added complexity, inconsistency, frequent management meetings and additional administration, testing and analysis. Further, the company had to harden the operating system before and after each upgrade. Because BlueCat could not implement standard DHCP High Availability (HA) best practices, the company struggled daily with DHCP configuration problems (e.g., servers not distributing addresses, clients receiving statically pre-assigned addresses, clients unable to reach off-subnet external networks, use Internet domain names or receive domain name suffixes) which increased errors, rework, inefficiency and cost.

Network Complexity: To keep core network services running, the company's IT team had to hire a resident BlueCat engineer. However, when the engineer left the company, it created a significant knowledge and resource deficit. Further, there were considerable challenges in simply maintaining the IP database. Updates made in the user interface were missing an hour later as if they had never happened. Without a centralized, synchronized, authoritative IPAM database, there were serious reliability problems for network and cross-functional teams. Moreover, the lack of BlueCat optimization required that customizations be coded into the platform at significant additional expense with each successive upgrade. Likewise, the company's optimization requirements also necessitated coding updates at high additional cost. This process added complexity, inefficiency and cost. "Hot fixes" were required for each update which were both scary and expensive, even for the company's extensive IT staff.

Discovery Deficiencies: Due to ongoing inconsistencies, the firm had to disable BlueCat's discovery tool. This development made it impossible to see and manage all of the L2 and L3 assets and device metadata across the network. It prevented the creation and maintenance of a centralized IPAM database and adversely impacted audit, reporting and control.

2. Network complexity escalated without synchronized IPAM, platform optimization and customizations. Customizations had to be rebuilt at cost with each new release;
3. Discovery deficiencies made visibility, automation and control impossible;
4. Retail store Internet access, survivability and redundancy were hindered by outdated Microsoft AD servers;
5. DNS security upgrades were required for malware, ransomware and other cybersecurity threats; and
6. Hybrid and multi-cloud services were needed for agility, efficiency and cost reduction.

WHY INFOBLOX

Infoblox provides decades of market leadership and innovation with reliable, centralized, consistent and automated DDI services. Its NetMRI solution delivers global network discovery, visibility and network change and configuration management. Looking to the future, Infoblox enables:

1. Global redundancy through HA architectures;
2. BloxOne DDI local survivability, access and performance;
3. DNS Security with BloxOne Threat Defense for malware and ransomware protection; and
4. Integrations for orchestration and automation with private/hybrid and public/multi-cloud expansion.

These capabilities empower visibility, automation and control to enable the company to fulfil its mission daily around the globe.

INFOBLOX SOLUTIONS

NIOS DDI, NetMRI, BloxOne DDI, BloxOne Threat Defense, Reporting and Analytics

Local Site and Store Redundancy and Survivability: Thousands of local sites and stores are running on Microsoft Active Directory servers. The company needs to improve agility, customer access experience and network performance, while ensuring local Internet access, local survivability and redundancy. This was not possible with BlueCat.

DNS Security: In view of its critical global shipping and logistics services, the organization is focused on guarding its network against malicious inbound and outbound DNS attacks. It also plans to improve its ability to monitor and terminate any DNS command and control (C&C) and data exfiltration exploits.

Hybrid, Multi-Cloud Expansion: While the company uses VMware for virtualization and private, hybrid cloud deployments, BlueCat's technical limitations impaired the organization's ability to expand workloads through a single control plane to public and multi-cloud environments for agility, efficiency and cost reduction.

THE SOLUTION

Enable network reliability, discovery and expansion

Network Reliability: Infoblox is the market leader with the industry's most robust and comprehensive protocol management capabilities, and innovation proven through decades of mission-critical reliability. Infoblox integrates and automates DDI protocols to ensure network consistency and uptime. DNS and DHCP redundancy are key to network reliability. Infoblox also establishes and maintains a synchronized, authoritative IP database as a centralized repository for network metadata. Infoblox DDI simplifies the complexities of network management through its user interface, backend synchronization and OS hardening to streamline management and upgrade processes resulting in greater network consistency, efficiency, uptime, automated protocol management and control.

Network Discovery: Given the company's challenges with BlueCat's network discovery tool, L2 and L3 device and endpoint discovery was a key priority. Fortunately, Infoblox's NetMRI Network Change and Configuration Management (NCCM, see Figure 1) solution met the need. NetMRI enables compliance policies, gathers network data and assesses network device inventory compliance. Templated and custom reports raise discovery and visibility and support network audits. In addition, NetMRI offers the company additional advantages:

- **Network Auto Discovery and IPAM Sync:** NetMRI automatically discovers, views and synchronizes multi-vendor infrastructure, IP addresses, end hosts, network constructs (L2 physical data, L3 logical data, routes, VLANs, virtual forwarding and routing) and topologies with current and historical information through a single control plane.
- **Change Management:** NetMRI manages change tasks with powerful but simple methods for encoding change logic. NetMRI's automatic change detection saves time and delivers configuration search, historical views and side-by-side comparisons.
- **Configuration Analysis:** NetMRI auto-detects and audits network updates, receives detailed analysis and performs configuration backup, search and date/time stamp correlation of network problems. Analysis and alerts on network performance, configuration and problems save time and speed resolution.
- **Change and Configuration Automation:** NetMRI enables and embeds variable-based jobs and scripts, customizable templates, scripting (CCS, Perl and Python), user-based role access control and job scheduling for further time-saving automation.

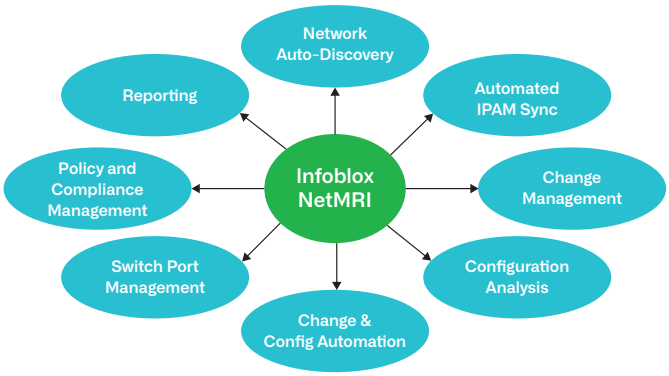

Figure 1: NetMRI Network Change and Configuration Management (NCCM)

- **Switch Port Management:** NetMRI tracks free, available and unused ports. It also provides provisioning, remediates compromised endpoints, monitors connected wired and wireless end-hosts, and supports capacity planning.
- **Policy and Compliance Management:** Another helpful provision is automatic, continuous real-time and historical tracking of network changes against multiple security policies. Embedded compliance rules, best-practice templates, violation detection and remediation tools further assist in resolving conflicts.
- **Automated Failover:** NetMRI provides redundancy and resiliency for data center collectors and appliances to support network availability requirements.
- **Reporting:** Finally, the single-click, pre-built and customizable summary and granular reports, filtering, on-demand, scheduled and role-based access enables IT management the visibility to see and share network information across the ecosystem.

Future Expansion: The organization also selected Infoblox for its existing solutions that solve expanding network requirements when timing is right—including global redundancy, local survivability, security and hybrid, multi-cloud expansion.

- **Global Redundancy:** Infoblox DDI delivers High Availability (HA) and more economically-priced "Power of Three" architectures to enable global redundancy and resiliency for key sites.
- **Local Survivability:** Infoblox also offers BloxOne Cloud including BloxOne DDI for retail and distributed locations to lower network costs while providing local survivability, access and improved service performance over Microsoft AD across retail stores and regional and global sites.
- **DNS Security:** Infoblox Advanced DNS Protection (ADP) guards against malicious inbound and outbound DNS attacks. Further, as part of the BloxOne Cloud, Infoblox BloxOne Threat Defense can be deployed for on-premises security and for continuously updated protection and DNS content category filtering. These tools protect against malware, ransomware, Domain Generation Algorithm (DGA), botnets, Fast-Flux, Zero-Day and data exfiltration. DNS Threat Insight (part of BloxOne Threat Defense) provides sophisticated machine learning for continuous monitoring and termination of DNS data exfiltration. Lastly, Infoblox's Security Ecosystem shares DDI and security metadata with existing security tools for detection, investigation and remediation. Combining Infoblox's core network and value-added services with BloxOne Threat Defense delivers secure, enterprise-grade network solutions to optimize and protect the company's operations around the globe.
- **Hybrid, Multi-Cloud Expansion:** Infoblox supports integrations with VMware, the organization's platform for private cloud. Infoblox also maintains orchestration and automation integrations with Red Hat Ansible, OpenStack, OpenShift, Docker, Kubernetes, Nutanix and Terraform. Further, with vNIOS for AWS, Azure, Google Cloud Platform and Oracle Cloud Infrastructure, Infoblox enables the company to plan its public, multi-cloud expansion strategy with an integrated solution for global network cloud services.

In summary, Infoblox was able to help the transport and logistics company define a multi-phase plan to modernize its global network for uptime and reliability. It also solved its discovery and visibility needs. Looking forward, Infoblox outlined future capabilities for business continuity, security and cloud services so the company can continue its daily mission of bringing people and packages together around the globe for years to come.

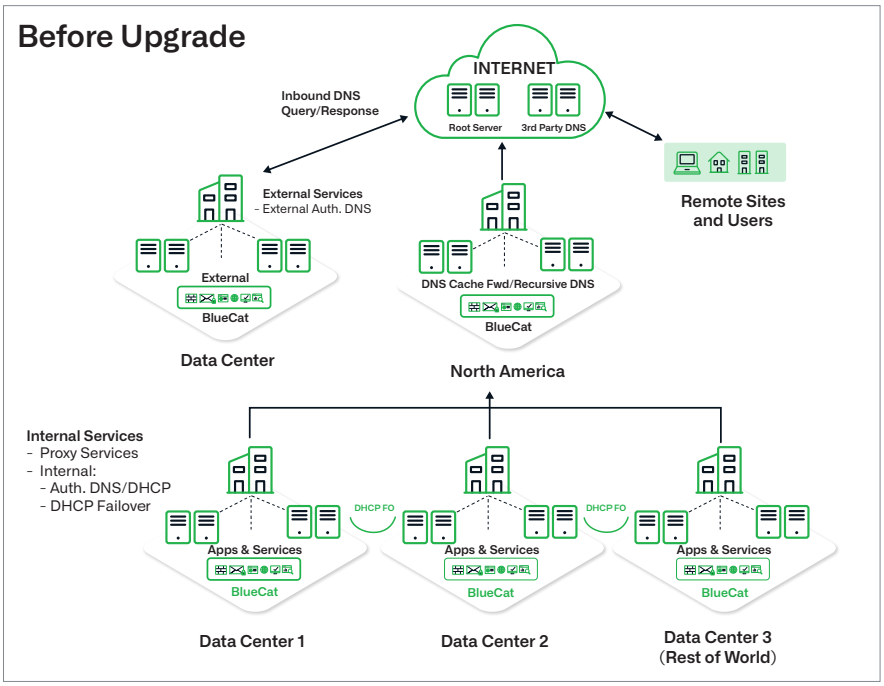

Figure 2: Before the Infoblox Upgrade

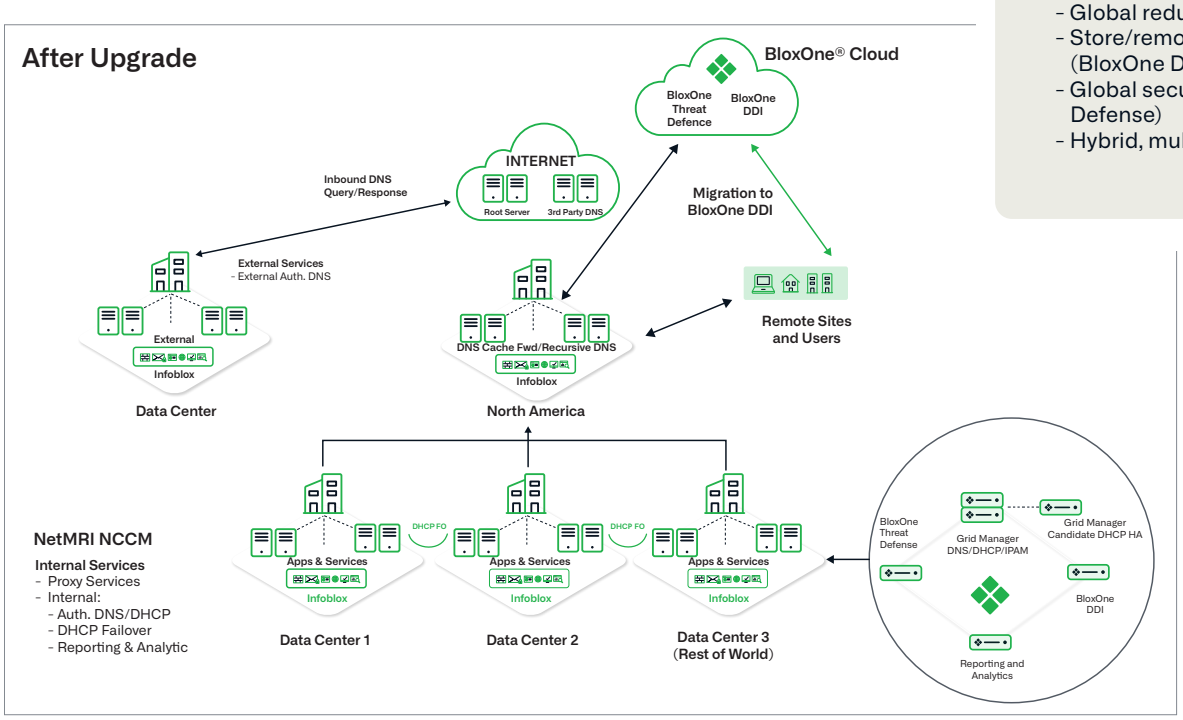

Figure 3: After the Infoblox Upgrade

PAIN POINTS

- Network upgrade challenges
- Global network complexity
- Discovery deficiencies
- Store/remote site redundancy and survivability
- DNS security and global protection against malware and security threats
- Cloud services consistency and expansion

BENEFITS

- Phase 1: Simplified, centralized DDI
- Phase 2: Network discovery and change management (NetMRI)
- Phase 3: Future Expansion
  - Global redundancy (DDI HA)
  - Store/remote site survivability (BloxOne DDI)
  - Global security (BloxOne Threat Defense)
  - Hybrid, multi cloud expansion

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: 20240529v2