infoblox

CASE STUDY

Electric wholesaler empowers service through network modernization and security protection

OVERVIEW

Based in the southeast United States, this family-owned electrical supply wholesaler provides electrical products and service supplies to builder organizations ranging from large-scale, multinational corporations to locally owned enterprises in the commercial, government, industrial, leisure, manufacturing and residential markets.

The company employs over 3,400 workers across 537 locations including more than 1,000 service vehicles in 30 states. In addition to an extensive catalog of more than 170 leading electrical supply brands, it also offers services in renewable energies, exports, government operations, corporate and marine solutions.

SITUATION

Network reliability, expanded branch footprint and increasing security demands

Like many commercial entities, the company ran its core network services on a Microsoft DNS/DHCP "freeware" platform. Initially, Microsoft DNS/DHCP met the company's basic needs, but expanding branch locations, technologies and workplace, social and security factors made it difficult to keep pace. The company was expanding fast, adding new branches at a rate of 50 new locations per year. COVID-19 then presented a virtual overnight explosion of remote workers connecting through VPN tunnels. Increasing network traffic, advancing cloud technologies and growing security risks also presented challenges for the Microsoft platform.

> *"The migration and cutover from Microsoft domain controllers to Infoblox was flawless. You don't have to be a huge company with a large network and security team to see and realize the value of Infoblox. A Microsoft DNS/DHCP migration is less than 40 hours and $10K for services to get secure, world-class DDI. And BloxOne Threat Defense is simple and does a great job keeping us safe from threats and bad actors. For a small IT team, it's simply fantastic."*
>
> **IT Team Lead**

As a result, the company experienced frequent DNS time-outs, which disrupted business operations, introduced supply chain friction and adversely impacted revenue. Further, DNS time-outs were linked to misconfigured Microsoft domain controllers. DNS was so unreliable that IT staff had to hard-code IP addresses into applications rather than using DNS protocols. Further, the company lacked an authoritative IPAM database and visibility into its DNS, DHCP and IPAM (DDI) metadata, necessary for business continuity. Mounting security threats, including daily command and control, ransomware, malware and data exfiltration risks, coupled with the company's expanding branch footprint presented an increasing network attack surface. Existing and prospective customers, supply chain vendors, partners and users expected greater security protection, but the company could not offer a strong, DDI-integrated answer to the increasing security problem.

Without secure, centralized network management, internal authoritative DNS and DHCP failover to provide site redundancy, the company's IT team decided to re-evaluate its network and security platform and invited BlueCat and Infoblox to submit proposals. After formal review, the company decided to implement Infoblox based on its technical DDI functionality, product quality, multi-decade track record, pre-sales support, cloud capabilities, road map and strategic professional services alignment with its strategic IT services partner.

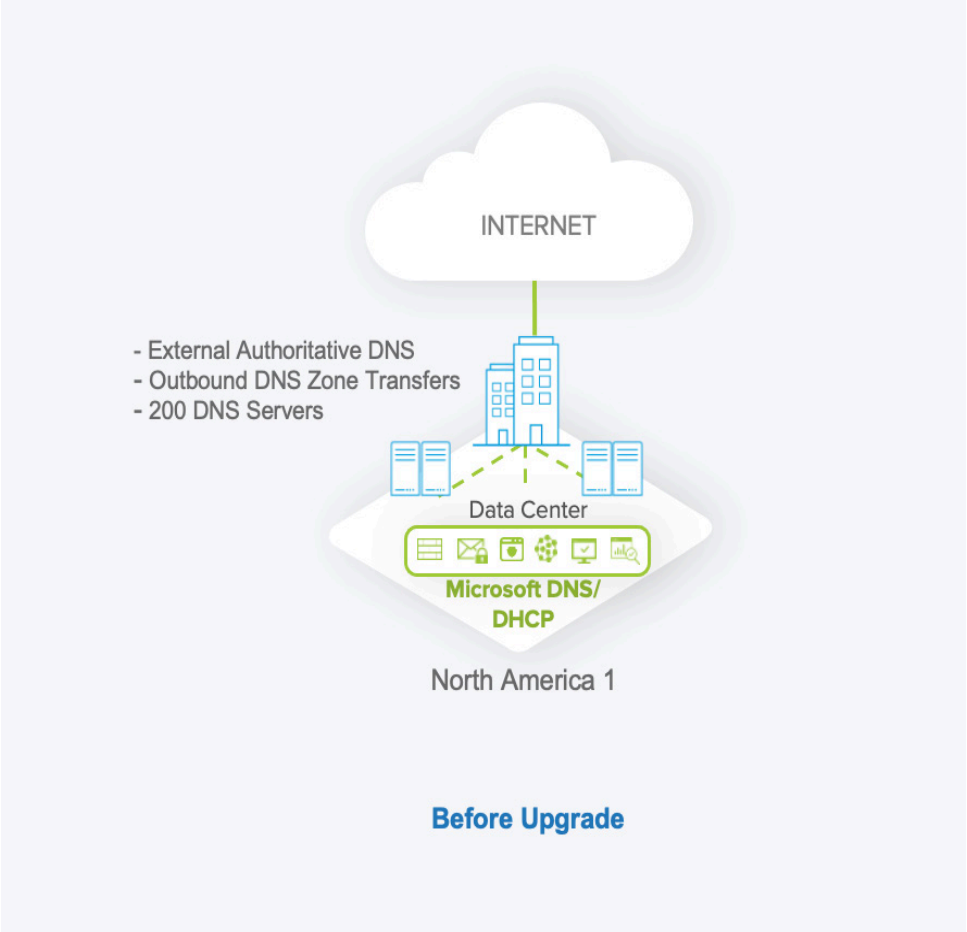

Figure 1: Network map prior to deploying Infoblox

CUSTOMER PROFILE:

- An American electrical parts and equipment wholesaler with over 3,400 employees across 537 branch locations in 30 states, the company serves the trade, working with contractors ranging from multinational giants to local enterprises in the commercial, government, industrial, leisure, manufacturing and residential marketplaces.

SITUATION:

- Network visibility, redundancy, reliability and security are top priorities, so the company sought to replace its outdated Microsoft DNS/DHCP platform and harden its DNS security against command and control, ransomware, malware, DGA and data exfiltration risks.

CHALLENGE:

- The company needed a seamless migration from its Microsoft DNS/DHCP to a modern, NIOS DDI and BloxOne Threat Defense environment to ensure secure, efficient control of its broad, geographically distributed wholesale branch operations. Managing the transition without interruption and protecting customers, vendors, partners and staff were essential to maintain business continuity, revenue streams and the company's reputation.

CHALLENGE

Reliability, visibility and security with seamless network migration

Given prior DNS disruptions, the company's IT team wanted to solve several challenges—in particular, network uptime, visibility and security. The decision makers specified centralized management for visibility, robust, enterprise-grade IPAM and DHCP failover for "always on" service availability. They also required internal authoritative DNS and a secure recursive DNS service for outbound queries. On-demand visibility into network data for historical audit and compliance support, utilization, performance, DNS security alerting and future capacity planning were added priorities.

With more than 500 branches across 30 states, security was also a concern. The company lacked a fully DDI-integrated security solution but wanted to protect its infrastructure, data, vendors and users against command-and-control takeovers, ransomware, malware, domain generation algorithm (DGA), fast flux, DNS Messenger and data exfiltration over DNS. Both network and security requirements called for a modernized DDI architecture.

Smooth, efficient migrations without service interruptions are the gold standard, especially for organizations with strong brand recognition that have relied on known technologies for an extended time. Managing the transition without interruption and protecting customers, vendors, partners and staff in the process were essential to maintain business continuity, revenue and brand value.

SOLUTION

Network modernization, visibility and security

With a very small IT staff, the company required simplicity and "set and forget" reliability. It chose to replace its Microsoft DNS/DHCP platform with enterprise-grade Infoblox DDI including security-hardened appliances to better see and manage its network. It deployed a Grid Manager and Grid Manager Candidate that included fully managed IPAM, internal authoritative DNS, DNS recursion to the top-level domain and DHCP failover for resiliency and redundancy. It also deployed Cisco Meraki SD-WAN to deliver local DHCP to branch locations. These solutions expanded visibility and reliability across the network.

Infoblox Reporting and Analytics was also added to improve on-demand network visibility, gain network insights and make network data more actionable. Rather than being buried in the network, the company's rich DDI metadata is now visible and accessible through templated and customizable dashboards and reports. The IT team can currently perform search, predictive analytics and graphical visualizations for endpoint, performance, security forensics, access logging, audit and compliance data, gaining superior visibility and improved network management to support consistently reliable uptime.

INITIATIVES:

- Upgrade to a modernized, scalable, DDI solution with comprehensive network visibility managed through a single control plane
- Ensure continuous uptime, high availability and redundancy even during network migration
- Enable enterprise IPAM, internal and external DNS, DHCP failover and reporting
- Access on-demand network data for audit/compliance, performance and threat events and predictive analytics
- Deploy DDI integrated security and ecosystem solutions to protect partners, affiliates and end users from malware and cybersecurity attacks

RESULTS:

- Established security from the network up using secure, enterprise grade DDI
- Ensured database redundancy, network resiliency and reliable uptime
- Integrated with existing security capabilities while hardening the system-wide security posture

INFOBLOX SOLUTIONS:

- NIOS DDI with Failover
- Reporting and Analytics
- BloxOne Threat Defense Advanced
- Threat Insight
- Infoblox 1415 Security Hardened and v5005 Virtual Reporting Appliances

For security, the company added Infoblox's on-premises and cloud-managed BloxOne® Threat Defense Advanced for constantly updated protection against command and control, ransomware, malware, DGA, fast flux, DNS Messenger and data exfiltration over DNS. BloxOne Threat Defense Advanced offered proven, market- and time-tested security capabilities to fill a gap and to secure DNS, enhance alerting and protect vendors and users. IT liked its fast and easy administration, the contextual IPAM data combined with threat defense and Infoblox's DDI integration. The company also added DNS Threat Insight with its sophisticated algorithms and machine learning to constantly scan the network for DNS data exfiltration and stop all unauthorized DNS data transmission.

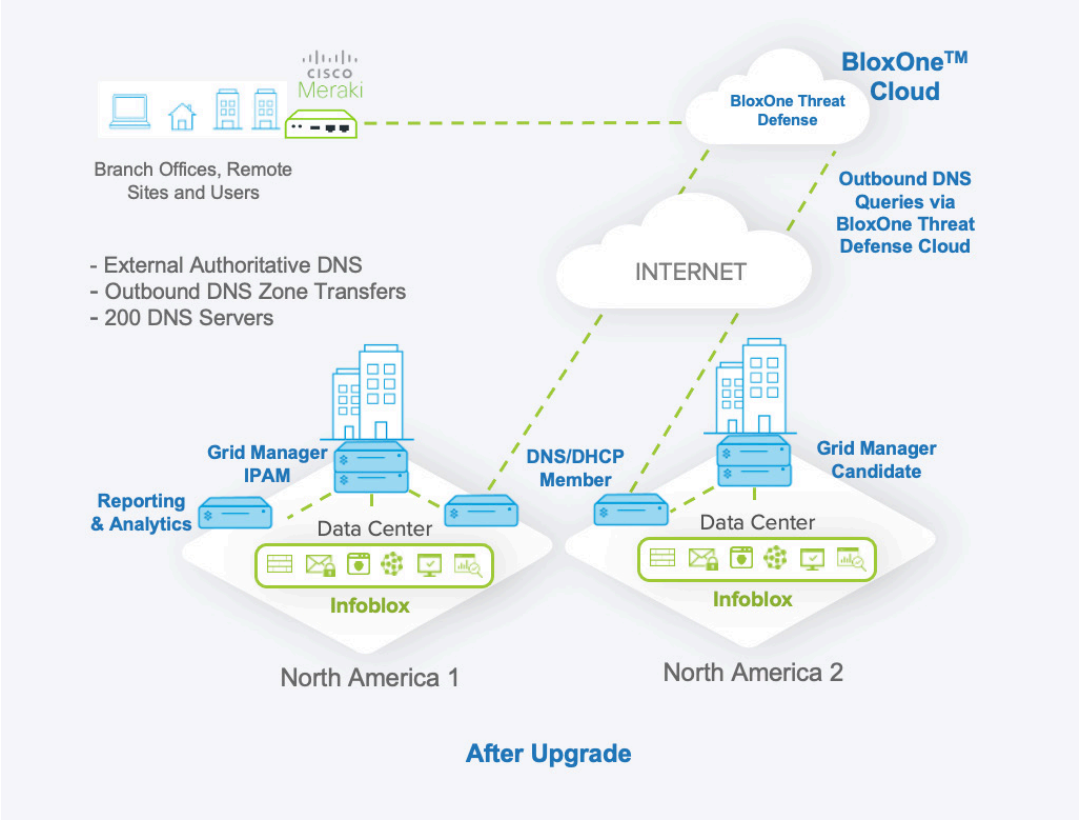

Figure 2: Modernized DDI with reporting and BloxOne Threat Defense Advanced for reliability, central visibility and security

RESULTS

Modernized core network services deliver reliability, visibility and security

As part of its decision criteria, the company engaged a strategic partner to manage the Microsoft DNS/DHCP migration to Infoblox. The DDI migration was flawless. Because the company had other network upgrades in process, it planned a gradual transition over four months. The DNS cutover took one evening. The remaining infrastructure was reconfigured from Microsoft to the Infoblox Grid over six weeks. The IT team redefined all its domain controllers as forwarders to the Infoblox Grid and established an authoritative database. Altogether, the migration took less than 40 hours and required little effort to make DNS safe, secure and reliable.

The technical lead on the project characterized the implementation as a great help to his very busy IT team, saying, "We used to have nothing but trouble with our Microsoft DNS deployment, but since we installed Infoblox, we haven't had one issue. It just works, which is huge for a small team like ours. It's not complicated. And we don't even have a network engineer."

With Infoblox, the company can provide unparalleled dependability, quality, personalized service and support for its electrical supply customers. The Infoblox platform enables the company to deliver locally stocked electrical supplies to the jobsite, saving contractors time, money and hassle. The company now has full network visibility, reliable network availability, uptime and redundancy, plus consistent enterprise DNS for on-site, off-site and connected users anywhere. Further, DDI modernization helps to future proof IT investments while the company plans its migration to the cloud. On-demand data access improves network visibility and management, and it speeds network decision making and response—especially for a small IT team.

From the security perspective, BloxOne Threat Defense Advanced with Threat Insight took less than three hours to deploy. The team lead noted, "Honestly, I have a harder time ordering things off Amazon than I did deploying BloxOne Threat Defense. I even tested it and use it at home. It's easy to set up, easy to use and I like the flexibility. It does a great job keeping us safe. It's world-class security against the bad actors and threats we face daily."

Infoblox security solutions harden the company's security capabilities and help it deliver a strong security response, not only to protect infrastructure, data and remote workers but also to provide the confidence to empower expansion for new vendors, partners and remote users. BloxOne Threat Defense Advanced with Threat Insight enables fast detection, investigation, response and remediation against ransomware, malware and data exfiltration. These security tools and integrations intensify network protection against increasingly frequent and complex security threats across the company's national branch network. By building in security from the network up, the company is able to leverage its DDI metadata for deep contextual visibility and insights. In this way, the IT team is able to improve control and security efficiency, lower security costs and make security tools more effective. With Infoblox's reliable, modernized network and security platforms, the company can continue its four decades of commitment in empowering people to continue building well into the future.

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

+1.408.986.4000
www.infoblox.com