infoblox

CASE STUDY

Leading SIEM data platform expands global reliability, visibility and security in hybrid networks with Infoblox

OVERVIEW

This U.S.-based company produces software for searching, monitoring and analyzing machine-generated data via a Web-style interface.

Its solutions—including one of the leading security information and event management (SIEM) tools in the marketplace—help capture, index and correlate real-time data in a searchable repository from which it can generate alerts, dashboards, reports and visualizations. The company uses machine data for identifying data patterns to provide metrics, diagnose problems and provide intelligence for business operations. An Infoblox customer and OEM partner since 2015, the company recently needed to upgrade and expand its DNS, DHCP and IPAM (DDI) platform to support global operations and enhance its security posture. It chose Infoblox's DDI-integrated BloxOne® Threat Defense Advanced solution to protect its infrastructure, data and users from malware, ransomware and DNS data exfiltration.

SITUATION

Global reliability and expansion

In 2015, the company replaced its Microsoft DNS and DHCP platform with Infoblox DDI for improved network uptime and reliability. In the process, the company became the OEM technology provider for Infoblox's data search and visualization tool, Infoblox Reporting and Analytics. By 2021, however, it was time for a technical network refresh. The company's IT team briefly considered EfficientIP, but with Infoblox's strong reputation and track record for reliability, the company renewed its Infoblox partnership and began building out its 21 regions around the globe. Expansion to the cloud was part of a modernization initiative and road map, but the company's top priority was enhancing core network services. The IT team wanted authoritative IPAM, single control plane visibility, unified management, reduction of extraneous network tools and overhead, simplified workflows and rapid scalability. Accordingly, it continued to expand its services with Infoblox based on the premise that "trust is hard won and easily lost."

> *"It's been said that 'trust is hard won and easily broken.' Fortunately, Infoblox provides secure, reliable world-class DDI that we can trust. It's our platform of choice for global network consistency, single control plane visibility and provides us with the scalability we need to serve our expanding global regions. And BloxOne Threat Defense with its ecosystem integrations, Dossier and Threat Insight is simple to deploy and use. It protects us, our data, infrastructure and users from malware, ransomware, data exfiltration threats and the bad actors we face daily."*
>
> **IT Team Leader**

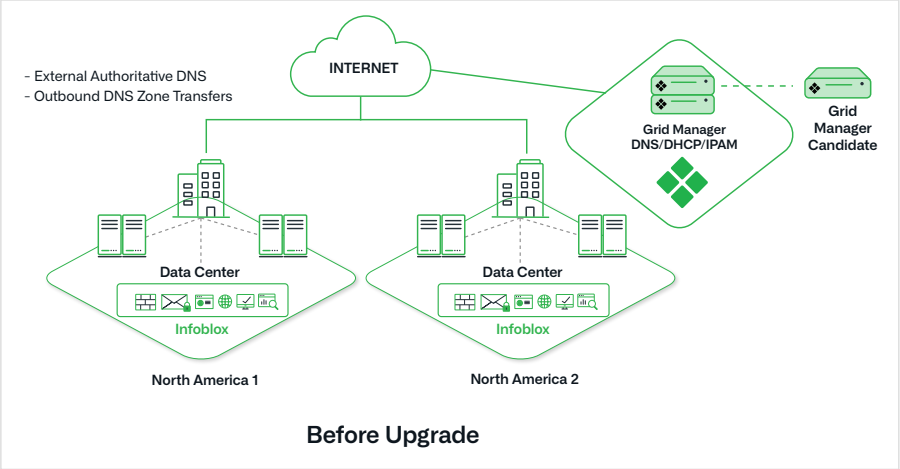

Figure 1: Network architecture before modernizing with Infoblox

CHALLENGE

Upgrading services to expand reliability, visibility and security across the globe

With Infoblox, the company did not suffer any major network conflicts, outages or security events, enabling it to focus on its NIOS DDI technology refresh to extend network visibility, security and uptime to other sites around the globe. It specified centralized management, enterprise-grade IP address management (IPAM) and DHCP failover for "always on" service availability. The company also required internal authoritative DNS and a secure recursive DNS service for outbound queries. While automation was not a driving priority, the IT team focused instead on eliminating extraneous tools, maintenance and overhead. Yet they also prioritized on-demand visibility for historical audit and compliance, utilization and performance metrics, DNS security alerting and capacity planning.

Given expanding security threats, the company prioritized the hardening of its security posture. It decided that DDI-integrated security was the right solution to protect its infrastructure, data, partners and users against command and control, ransomware, malware, Domain Generation Algorithm (DGA), fast flux, DNS Messenger and data exfiltration over DNS. Both network and security requirements called for a transition from its existing deployment (see Figure 1) to a modernized enterprise-grade DDI architecture (see Figure 2).

SOLUTION

Network modernization, visibility, security and scalability

With a very small IT staff, the company required simplicity and "set and forget" reliability. Infoblox's enterprise-grade DDI platform included a combination of hardware and virtual security-hardened appliances to better see and manage its network. They deployed a Grid Manager and Grid Manager Candidate, including fully managed IPAM and internal authoritative DNS on an HA member for optimal visibility. The network design specified dedicated units for inbound Internet DNS queries. Outbound DNS queries (DNS DMZ cache) were forwarded to the cloud for geo-local IP address resolution. In addition, the DHCP failover protocol enabled site redundancy while HA members delivered maximum service availability, especially for VoIP deployments across its global network.

CUSTOMER PROFILE:

- A global company with over 7,500 employees, 850 patents and availability in 21 regions worldwide, this software business offers an open, extensible data platform that supports shared data across any environment. That means all teams in the organization can get end-to-end contextual network visibility for every interaction and business process.

SITUATION:

- The company sought to improve its infrastructure reliability by increasing redundancy and adding DNS Security to integrate with its SIEM offering, ensuring business uptime and app availability.

CHALLENGE:

- IT decision makers realized they needed to expand core network services for single control plane visibility, reliability, management and scalability to serve their end users around the world.

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 cyber security attacks

Infoblox's Cloud Network Automation was added for visibility, management and control in AWS public cloud services. It also added DNS Traffic Control (DTC) for network traffic management, application uptime, ease in deploying new services and API integration.

Not surprisingly, the company was also a heavy user of Infoblox Reporting and Analytics. This solution was helpful for alerting, dashboards and reporting for on-demand network visibility, network insight and improved response time. Rather than being buried in its network, the company's rich DDI metadata was visible, accessible and useful for search, predictive analytics and graphical visualizations for endpoint, performance, security forensics, access logging and audit and compliance to support consistent visibility and uptime.

Although the company had Cisco Umbrella for security, it preferred the idea of using DNS both as its first layer of defense and to enrich its other toolsets. The Infoblox security solution was simple: Start with DNS, add and correlate threat intelligence, block bad actors and in so doing, remove the load off other critical tools. Accordingly, the company's IT team selected Infoblox's on-premises and cloud-managed BloxOne Threat Defense Advanced (Figure 2) for updated protection against such threats as ransomware, DGA, DNS Messenger and data exfiltration over DNS. BloxOne Threat Defense acts as a general resolver in the cloud for geo-local resolution to protect users and remove malware. The solution also offered proven, market- and time-tested security capabilities that filled a missing security gap to secure DNS, enhance alerting and protect business partners 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 Dossier and 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.

RESULTS:

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

INFOBLOX SOLUTIONS:

- NIOS DDI with failover
- Cloud Network Automation
- DNS Traffic Control
- Reporting and Analytics
- BloxOne Threat Defense Advanced
- Ecosystem integration
- Dossier
- Threat Insight
- Infoblox 2225 HA, 1425, v1425, Security Hardened, BITDA and v5005 virtual reporting appliances

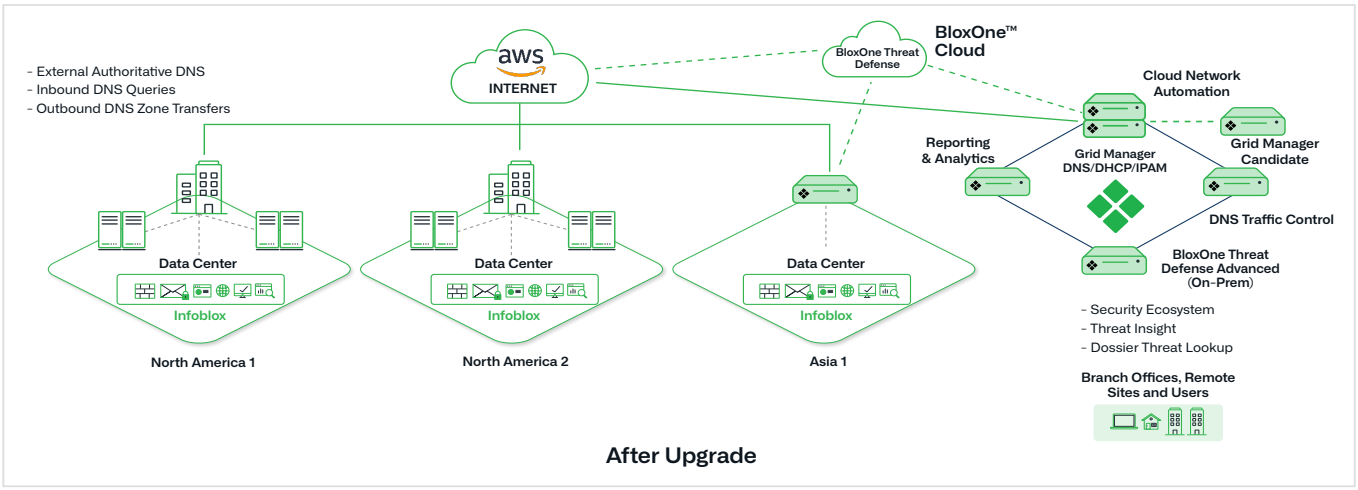

Figure 2: Post-upgrade architecture with modernized DDI, including Reporting and BloxOne Threat Defense

RESULTS

Modernized network services deliver reliability, visibility, security and global scalability

With its Infoblox update, the company is better positioned to deliver on its promise to provide unparalleled dependability, quality, personalized service and support for global software customers. It now has full network visibility, continued application availability, uptime and redundancy along with consistent enterprise DNS for on-site, off-site and connected users anywhere. Further, DDI modernization helps to future proof IT investments as the company plans its migration to the cloud. On-demand data access improves network visibility and management and speeds network decision making and response—especially for a small IT team.

From the security perspective, BloxOne Threat Defense Advanced with Threat Insight is easy to set up and use and offers the DDI-integrated metadata and flexibility needed for world-class security against bad actors and daily security threats.

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 Dossier and 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 security from the network up, the company can leverage its DDI metadata for deep contextual visibility and insights to improve control, security efficiency, lower security costs and make security tools more effective. Using Infoblox's reliable, modernized network and security platforms, the company can continue its decades of commitment in empowering data visibility for security and SIEM applications well into the future.

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

+1.408.986.4000
www.infoblox.com