infoblox

CASE STUDY

Major multinational media and entertainment corporation adopts BloxOne DDI and BloxOne Threat Defense for stronger security and business growth

OVERVIEW

This major American media conglomerate—with holdings in movie production, broadcast entertainment, news and amusement parks—has been an Infoblox customer since 2002.

For many years the firm's network architecture was based on an Infoblox NIOS Grid connecting its primary sites, with legacy branch offices backhauling DNS queries to the Grid. When the firm began bringing a series of new independent studios into the organization, they chose to use Microsoft Active Directory (AD) to manage DNS operations. During a major technology refresh, the firm's IT decision makers chose to reduce their DNS footprint and rearchitect their network for flexibility and speed.

THE FIRST CHALLENGE

Managing Business Growth and Infrastructure Expansion in Parallel

Focused on growth, the company has been expanding operations across locations globally. This expansion included the launch of 26 independent studios and smaller offices around the world. Furthermore, the company is creating a major hub in Europe that includes a new data center, with plans for an additional data center in Asia. The company had settled on using NIOS on premises for their bigger sites but decided to explore other options for their smaller sites. The disparate DNS systems at the studios and smaller offices—NIOS backhaul and Microsoft AD—and the corresponding network architecture was neither ideal nor desirable.

Company decision makers wanted their studios and smaller sites to operate independently. They did not want to backhaul DNS to their main hubs and wished to migrate away from lower performing Microsoft AD for DNS. But NIOS, an enterprise-grade solution, would have been overkill performance-wise for these smaller sites. So, while local survivability was key, there was no interest in maintaining 26 different profiles and policies. Given the large number of sites,

Industry: *Broadcast Media*
Location: *United North America*

INITIATIVE:

- Manage business growth and infrastructure expansion in parallel
- Support a growing network of independent production facilities with more robust networking capabilities
- Secure intellectual property across the global network

OUTCOMES:

- Strengthened security posture—gained the ability to now able to detect and prevent DNS-based data exfiltration
- Hybrid DDI infrastructure supports better network manageability from the cloud
- Automated DNS, DHCP and IP address provisioning across distributed locations from the cloud

SOLUTIONS:

- Infoblox NIOS
- Infoblox Grid
- BloxOne DDI
- BloxOne Threat Defense

ease of configuration and speed of turning up these sites were critical. In addition, ensuring a smooth migration away from Microsoft AD was crucial. Given all these factors, the company determined that moving to the cloud-first BloxOne DDI for its distributed locations would be the ideal solution. Essentially, they could realize full Infoblox performance through the cloud at a price-point much more in line with their legacy AD systems.

THE SECOND CHALLENGE

Securing intellectual property on a global network

Intellectual property, especially the kind of entertainment programming produced by the media conglomerate, remains a high-value target for organized crime and cyber attackers. The company's IT security executives understood that stronger and more resilient threat intelligence was going to be essential to its cyber defense as it expanded overseas. The value and importance of using DNS infrastructure as part of these security efforts was also well known. For these reasons, the responsibility for DNS security was managed closely by the company's chief information security officer (CISO).

Awareness of the negative repercussions of cyber security attacks was high within the CISO's office. Several years before their technology refresh was initiated, the firm's website was breached by hackers that added links to malware within the site. Fortunately, Google's Chrome, Apple's Safari and other web browsers detected the threats and deterred users from clicking through the links and loading the pages. The worst outcomes were avoided, but the attack did become public. The company was compelled to release a statement noting that the incident had been identified, and that no user information had been compromised. As planning for the technology refresh proceeded, the CISO's team began assessing additional security measures they could deploy to better protect foundational network infrastructure and operations. It was at this time that the team began testing BloxOne Threat Defense

THE SOLUTIONS

BloxOne DDI and BloxOne Threat Defense

As planning reached completion, the CISO and team mapped out an ambitious new hybrid architecture employing both conventional on-premises and cloud elements. Infoblox NIOS and Grid would be deployed at five data center sites across North America, Latin America, Europe and APAC; BloxOne DDI would be deployed through the cloud at branch locations and remote offices outside the main data centers; BloxOne Threat Defense would be deployed through the cloud as the foundational element in a new cybersecurity strategy to prevent DNS-based data exfiltration and that could be managed and integrated with existing cybersecurity tools.

Given the company's business growth strategy that depended on multiple independent studios and branch locations, the cloud-first BloxOne DDI was an ideal solution as a cost-effective alternative to full NIOS deployments. The NIOS plus BloxOne DDI hybrid network architecture incorporated several elements that appealed to their architects. First, BloxOne DDI was cost effective for their distributed locations, offered local DNS resolution for direct Internet access, and provided remote sites with local survivability. By eliminating the need for DNS backhaul to the data centers, users at branch and remote locations would be assured of high-performance connectivity when using Microsoft Office 365, Adobe Creative Cloud and other cloud applications.

Second, the NIOS Grid had licensing flexibility to be located both on premise at their private data centers as well as in their multi-cloud locations at Amazon AWS and Microsoft Azure points of presence. With rich APIs and extensive Terraform integration for DevOps, NIOS enabled simple and automated spin up and spin down of containers for their applications in the cloud. Third, using DNS Anycast, the NIOS Grid served as the redundancy layer for their branch sites. Each BloxOne DDI instance at the branch site would recurse out to the NIOS Grid if necessary. Last, if DNS queries further needed to recurse out to the Internet, BloxOne Threat Defense provided a layer of security to prevent clients from going to unauthorized domains.

Flexibility in the use of software license pools was paramount in this architecture. Furthermore, the hybrid NIOS + BloxOne DDI architecture gave the company enterprise-wide consistency for their DNS policies across the globe. In all, the NIOS GRID deployment is made up of 10 hardware appliances installed in pairs at five primary locations. Thirty-six BloxOne DDI virtual appliances comprised the solution for the studios and branch locations.

BloxOne Threat Defense directly addressed the CISO team's strong concerns about potential data exfiltration, and the technology refresh proceeded with the purchase of a 60,000-user license that will provide the company with a strong DNS security layer. With its deep knowledge about the benefits of foundational security, the team wanted to be proactive about deploying a solution that would use DNS infrastructure as a security control point and reduce the risk of data exfiltration. BloxOne Threat Defense delivers exactly that, with the added benefits of Threat Intelligence reporting and automation for rapid response. BloxOne Threat Defense also extended the value of the company's existing cybersecurity investments because it easily integrates with industry standard SIEM and SOAR platforms and other cybersecurity tools.

OUTCOMES

Stronger security posture, better visibility and increased agility to accommodate business growth

With BloxOne Threat Defense in place, the company is now able to detect and prevent DNS-based data exfiltration. Infoblox foundational security also brings behavioral analytics as well as reputation and signature analysis at scale for the cloud. The Threat Defense solution leverages the rapidly growing power of machine learning, making it possible to examine all DNS queries and responses in real-time. Threat Defense's unique DNS-layer design provides architectural efficiency, as most malware and internet connections rely on the DNS service. The new capabilities ensure that the media giant can now proactively protect its users and network resources while automatically preventing data exfiltration that could compromise its valuable intellectual property.

The company expects to benefit further from reduced incident response times through data enrichment of the entire security ecosystem, including SOAR platforms, using the contextual network and threat intel data as well as extensive ecosystem integrations. These initiatives, which are a priority of the CISO team, will be implemented carefully over time. It is also important to note that the team's threat analysts are now more productive. Infoblox BloxOne Threat Defense has strengthened and optimized the firm's security posture from the foundation up, maximizing brand protection.

Overall, the adoption of the Infoblox hybrid solution is facilitating the company's ongoing and future digital transformations encompassing adoption of SD-WAN, IoT and further cloud deployments. The complexity of its network architecture has been reduced and simplified in alignment with the CISO's stated goals, yet is far more powerful and capable than its previous infrastructure that relied on Microsoft AD.

With its hybrid NIOS + BloxOne DDI infrastructure now in place, the company is now able to automate DNS, DHCP and IP address provisioning across distributed locations from the cloud. New studio, production and distribution facilities can be brought online within hours, not days. Moreover, administrators now have clear visibility into end users and devices across the network regardless of their location within the company's vast global network. The Infoblox hybrid solution has put the company on a stronger footing to accommodate fast 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