infoblox®

CASE STUDY

Global weather service delivers accurate forecasts with modernized network and security protection

OVERVIEW

Founded in 1962, this U.S.-based media and meteorology service broadcasts weather forecasts, weather alerts, event analysis and weather-related news to more than 1.5 billion people around the globe.

It shares weather data for every longitude and latitude point on Earth—more than 3.5 million locations—based on over 170 forecasting models and expert analysis delivered through its smartphone apps and cable and satellite television network and affiliates. The company employs 500 weather professionals, including more than 100 meteorologists along with app developers, designers and writers to combine weather data, technology and insights to improve business and public safety, reduce weather-related losses and help people make decisions based on accurate, real-time weather information.

SITUATION

Expanded global footprint, technology advancements and increasing security demands

In 2011, the company upgraded its core network services from Microsoft DNS and DHCP to Infoblox enterprise-grade DNS, DHCP and IPAM (DDI). Over the next decade, it grew its business on Infoblox's stable, reliable and highly available core network services. By 2021, however, network traffic was nearing capacity, and the world had changed. The company's mobile apps and cable and satellite network technologies had advanced to share streaming video, weather forecasts, news and content through network partners and affiliates worldwide. COVID-19 led to more remote workers connecting to the organization's infrastructure through VPN tunnels than ever before.

CUSTOMER PROFILE:

- American global meteorology service with over 500 employees delivering weather forecasts, data, warnings, analysis and news over cable, network and smartphone applications to more than 1.5 billion people worldwide.

CHALLENGES:

- The company needed to modernize its network to expand capacity, ensure global uptime and deliver network visibility, scalability and security against malware, ransomware and data exfiltration. The company aimed to maintain an extensive global footprint while incorporating technology advancements and supporting more network affiliates and mobile app users. It faced these challenges while also coping with COVID-19 remote workplace expansion, increasing security threats and heightened demands for security protection everywhere.

Technological, geographical, workplace, social and security changes greatly elevated the need for comprehensive network visibility. Ever-increasing security threats—including daily ransomware, malware and data exfiltration risks—coupled with the company's expanded global footprint presented an exponentially wider network attack surface. Network partners, affiliates and mobile app users demanded greater security protection, but the company lacked a strong, integrated solution to its growing security problem. Without a solution, the company would have difficulty reaching target expansion goals, so its IT decision makers turned to Infoblox for help.

CHALLENGES

Global visibility, scalability, uptime and security

The company needed to scale its centrally managed core network services with built-in redundancy and backup for mission-critical 24/7 availability everywhere. It required fully managed IPAM and internal authoritative DNS and DHCP failover to deliver "always on" service availability for its comprehensive global locations, partners, affiliates and online and mobile users. On-demand visibility—through network dashboards and custom summary and forensic network data—was also critical, especially for assessing IPAM data, DNS security and alerting, utilization, query logging and trend analysis for capacity planning. The company also needed a way to integrate DNS operations with existing security tools to protect its infrastructure, data, partners and users against ransomware, malware, domain generation algorithm (DGA), fast flux, DNS Messenger and data exfiltration over DNS. In addition, the company wanted to conduct DNS content category filtering to protect off-site workers from Wi-Fi threats and access to websites that could initiate malware, ransomware or phishing attacks. Both network and security requirements called for network modernization.

SOLUTION

Network modernization for comprehensive visibility and security

The company updated its network with a state-of-the-art DDI solution from Infoblox, including security-hardened appliances to better see and manage IPAM and scale to support global operations. It deployed a Grid Manager and Grid Manager Candidate with internal authoritative DNS, DNS recursion to the top-level domain and DHCP failover for resiliency and redundancy. These improvements expanded visibility across the network. The company also added Reporting and Analytics to enhance on-demand network visibility, insights, templated and customizable dashboards and reports, search, predictive analytics and graphical visualizations for endpoint, performance, security forensics, access logging, audit and compliance. In addition to visibility, security was a top priority. The IT team wanted to continue using its existing solutions, so out-of-the-box templated integrations were essential.

The company used Rapid7 security information and event management (SIEM) to collect network data, manage vulnerabilities, monitor malicious behavior and investigate and stop attacks. Infoblox's Cybersecurity Ecosystem with Rapid7 integration and robust API calls was the perfect complement. Not only did Cybersecurity Ecosystem's Rapid7 integration deliver immediate time to value, but it also extended its ROI and added the flexibility to integrate with a broad array of future security and orchestration tools. The company began a two-month proof of concept to test Infoblox's

INITIATIVES:

- Upgrade to a modern, scalable DDI solution with comprehensive network visibility managed through a single control plane
- Ensure continuous uptime, high availability and redundancy
- 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 technologies
- Ensured database redundancy, network resiliency and reliable uptime
- Integrated with existing security capabilities and strengthened and intensified the system-wide security posture

INFOBLOX SOLUTIONS:

- NIOS DDI with failover
- BloxOne Threat Defense Advanced
- Security Ecosystem
- Reporting and Analytics
- TIDE threat feed distribution
- Dossier threat lookup
- Infoblox 1415, 815 and 5005 security-hardened appliances

on-premises and cloud-managed BloxOne Threat Defense Advanced security solution. BloxOne Threat Defense offered proven, market- and time-tested security capabilities, so the company put it directly into production to secure DNS, enhance alerting and protect partners and end users. The IT team liked the visibility of contextual IPAM data combined with threat defense and integrated DNS security within Infoblox's DDI system. It 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. The company incorporated Infoblox's Threat Intelligence Data Exchange (TIDE) for threat feed distribution to connected security systems and the Dossier threat lookup tool.

RESULTS

Modernized core network services deliver reliability, scalability and security

With Infoblox, the company delivers on its promise to combine weather data, technology and human insight to improve lives and business outcomes. Infoblox core network services enable the company to broadcast the latest weather news and information—reliably, around the clock—covering the remotest parts of the Earth. It has full network visibility, enhanced global availability and uptime, redundancy and consistent enterprise DNS for on-site, off-site and connected users everywhere. Further, DDI modernization substantially lowers database utilization, allowing for a significant increase in scalability for global workloads to meet expansion objectives. On-demand data access improves network visibility and management and speeds network decision making and response.

From the security perspective, Infoblox security solutions and integrations fortify the company's security posture and help it deliver a strong security response. Integrated solutions like BloxOne Threat Defense Advanced, Cybersecurity Ecosystem, templated integrations, robust APIs, TIDE and Dossier enable fast detection, investigation, response and remediation against ransomware, malware and data exfiltration. These security tools and integrations intensify network protection against increasing and complex security threats across geographies. By building security from the network up, the company can leverage its DDI metadata for deep contextual visibility and insights to improve control and security efficiency, lower security costs and make its SIEMs, SOARs and other security tools more effective. By using Infoblox's reliable, modern network and security platforms, the company can continue its 60-year commitment in helping people handle changes in weather and make the best weather-related decisions.

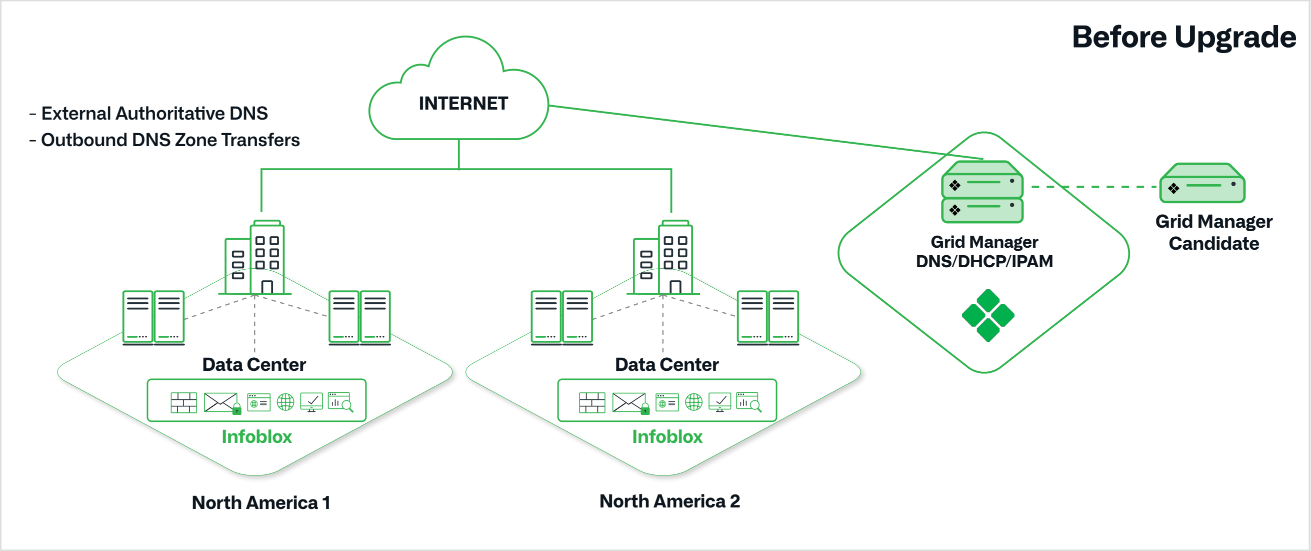

Figure 1: Network Architecture Before Upgrade

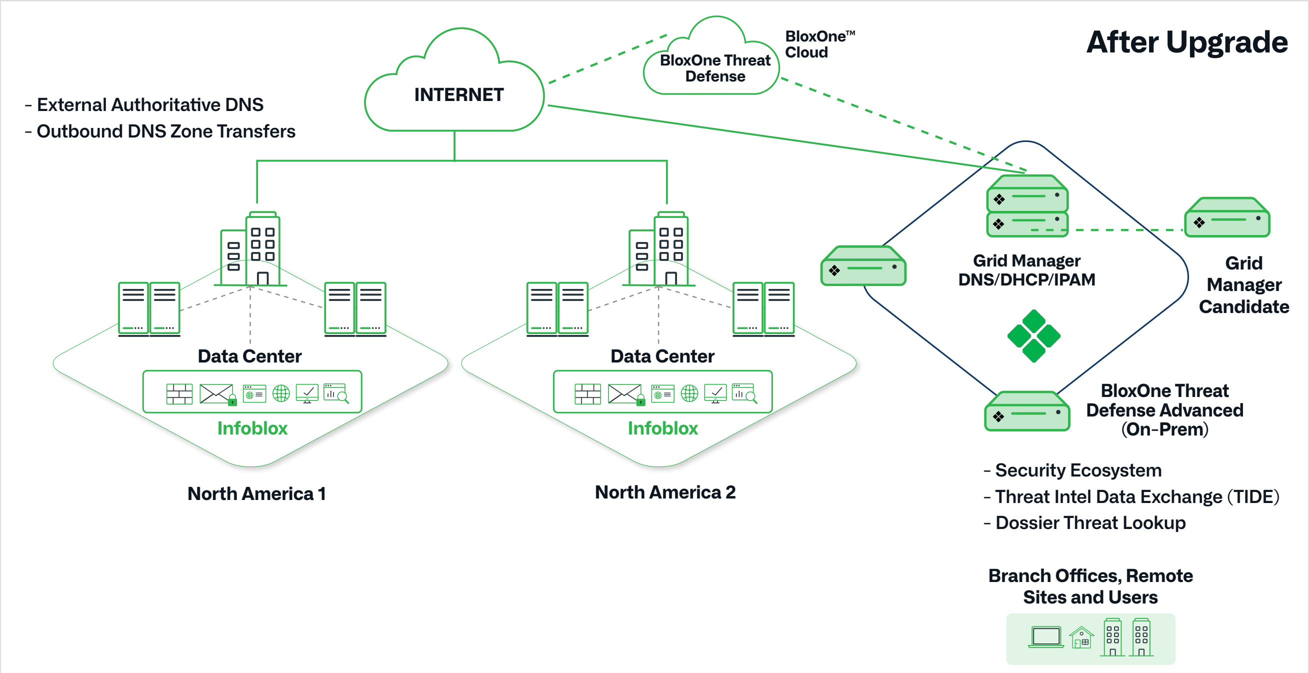
After Upgrade
INTERNET
BloxOne Threat Defense
BloxOne™ Cloud
- External Authoritative DNS
- Outbound DNS Zone Transfers
Data Center
Infoblox
North America 1
Data Center
Infoblox
North America 2
Grid Manager DNS/DHCP/IPAM
Grid Manager Candidate
BloxOne Threat Defense Advanced (On-Prem)
- Security Ecosystem
- Threat Intel Data Exchange (TIDE)
- Dossier Threat Lookup
Branch Offices, Remote Sites and Users

Figure 2: Modernized DDI with Reporting, Ecosystem, and BloxOne Threat Defense for central visibility, scalability, security and control

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