infoblox

CASE STUDY

Energy, oil, and gas leader expands hybrid networks for secure remote access, scalability, unified control, and cost savings

THE CUSTOMER: GLOBAL ENERGY, CHEMICAL, OIL, AND GAS LEADER

With oil and gas exploration on six continents and operations expanding to most countries, a global leader in energy and chemical manufacturing depends on its network to develop next-generation fuel technologies to meet world demand and advance globally recognized brands.

In 2011, it selected Infoblox DNS, DHCP, and IPAM (DDI) to begin replacing parts of its VitalQIP network infrastructure. Since then, global mergers and acquisitions, growth, disparate systems, and technology advancements have added network complexity across on-premises data centers, remote locations, the cloud, and SaaS applications. In 2017, the company suffered a month-end, four-hour OpenDNS outage that knocked operations offline. Unable to perform query resolutions, it missed required external payments, resulting in SLA penalties and multi-million dollar losses per hour from this one outage alone.

To prevent costly future outages, management decided to transform its network infrastructure for greater visibility, security, redundancy, local access, efficiency, and cost control. It launched a massive multi-phase, multi-year DDI modernization project to unify and transform its global network. The first phase involved upgrading outdated, conventional DNS/DHCP architecture and disparate systems with a virtualized Infoblox environment wherever feasible. Its goal was to sunset inefficient infrastructure and deploy a secure, agile, cost effective, globally distributed architecture. The second phase simplified and unified management by adding Network Insight discovery and replacing Microsoft DNS/DHCP with BloxOne DDI at over 200 remote locations. This stage delivered authoritative IPAM, enhanced geo-local response, and virtually eliminated errors and trouble tickets. It also enabled scalability for new sites and functionality, ensured high availability and redundancy, improved efficiency, and significantly reduced remote site management costs. Phase three shifted focus to zero trust and never-fail, hybrid on-premises and cloud security. Because its existing recursive, cloud-only solution could not prevent data exfiltration, the company chose to test BloxOne Threat Defense at considerably less cost than its existing Cisco Umbrella solution. The Infoblox solution also provided superior DNS lookup, tighter security, and higher-performing technology without the need for direct platform management. Combined, these enhancements improved visibility, simplified management, increased security and control, and lowered costs to enable industry leadership for years to come.

THE CHALLENGE

The Hidden Costs of Freeware

As an industry leader, the company faces ongoing competition from other well-known, globally branded competitors, so it depends on network visibility, always-on reliability, efficiency, and control to drive global operations and meet customer demand. Its network processes an average of 2 billion queries per day. Due to worldwide growth and mergers and acquisitions, the company's network included Microsoft DNS, DHCP, and other disparate systems deployed across the company and managed by separate departments. This architecture prevented centralized management, hindered validation, troubleshooting, and root cause analysis, and failed to quickly resolve network disruptions. Microsoft required multiple servers, maintenance, and reboot cycles; it also delayed Active Directory (AD) replication and had trouble managing DHCP boundaries. In addition, its network asset discovery tools did not detect all assets or work consistently across on-prem and cloud environments, resulting in zone, DHCP, and IP conflicts.

Existing freeware DDI could not scale to meet global needs and was generating over 30 labor-intensive trouble tickets per month. Further, limitations with Azure made DNS difficult to manage. Given its size and scale, even an hour offline could cost millions of dollars. This scenario escalated in 2017 when a four-hour OpenDNS outage knocked operations offline at month-end, preventing external payments and resulting in vendor SLA penalties and tens of millions in losses from this single network outage. To solve these challenges, representatives from the company's IT team joined Infoblox's technical advisory board to define a new architecture and plan for transforming its environment to avoid future network outages and optimize global presence and geo-local response.

The company initiated a multi-billion dollar technology upgrade for headquarters, data centers, and subsidiaries. Its global network connects thousands of on-prem and remote valves, flow control, programmable logic controllers, telemetry, and a host of other oil, gas, and chemical devices and machinery. Many of these systems require IoT sensors for monitoring and control, and they must be reliably operational 24 hours a day, seven days a week. Discovery, visibility, redundancy, and resiliency are critical, and if any system goes down, speedy recovery and the continued ability to make changes are essential. These needs were proven during a hurricane when a refinery and chemical plant were knocked offline. DNS and DHCP locally were unavailable due to a communications failure with the data center, causing lengthy and costly delays.

Network security, especially data exfiltration, was also a prime concern. So, the company used internal and third-party security resources for rigorous and ongoing testing of its existing Cisco Umbrella security platform, along with BloxOne Threat Defense. During the tests, BloxOne Threat Defense discovered and shut down data exfiltration attempts within 18 packets, so that they could not be breached, while the more costly Cisco Umbrella solution missed the attack entirely. Ironically, testers thought BloxOne Threat Defense failed, but in fact, the solution worked so well that data exfiltration attempts could not pass on-prem appliances and were stopped almost instantly—and well before reaching the cloud.

Customer: *Leader in Energy, Oil, and Gas*
Industry: *Mining*
Region: *Global*

OBJECTIVES:

- Adopt a modern, scalable, and high availability infrastructure
- Eliminate costly network outages
- Enhance visibility and connectivity at 200+ remote locations through virtualized network services
- Extend cloud-managed security to protect users, data, and infrastructure
- Increase scalability to support 2 billion queries / day

RESULTS:

- Virtualized on-prem, hybrid, multi-cloud network architecture
- Reduction in trouble tickets from 30 to less than 1 per month
- Reliable, high availability system, saving millions on previous network outages
- Enhancements improved visibility, simplified management, increased security, and lowered run cost by 50%
- Stronger security posture, greater SecOps productivity, and lower threat defense costs

PRODUCTS

- BloxOne DDI
- BloxOne Threat Defense
- NIOS DDI
- Trinzic appliances
- Dossier
- Network Insight
- Cybersecurity Ecosystem

Driven by the need for global visibility, automation, control, and security, the company began moving toward a hybrid on-prem and cloud-managed DDI subscription architecture for global presence, capacity, and geo-local response. IT set up a lab to test SD-WAN and explore secure access service edge (SASE—the future of cloud security), the cloud-native, container-based framework that integrates networking and security services in the cloud. Applying big data analytics near endpoints for faster access and control was also a goal, but achieving these changes required a new network architecture and modern technology transformation.

THE SOLUTION

A Virtualized Environment with Hybrid, Cloud-Managed DDI

The company chose Infoblox to replace its existing DNS/DHCP infrastructure using a prioritized, cost-driven, multi-phase approach. In phase one, the aim was to replace disparate systems, dedicated physical WAN circuits, manual static DNS/ DHCP configurations, inefficient processes, departmental silos, and centralized, perimeter-based security with a hybrid, virtualized Infoblox environment. It included adding hybrid, cloud-managed DDI and deploying a secure, agile, cost effective, globally-distributed architecture.

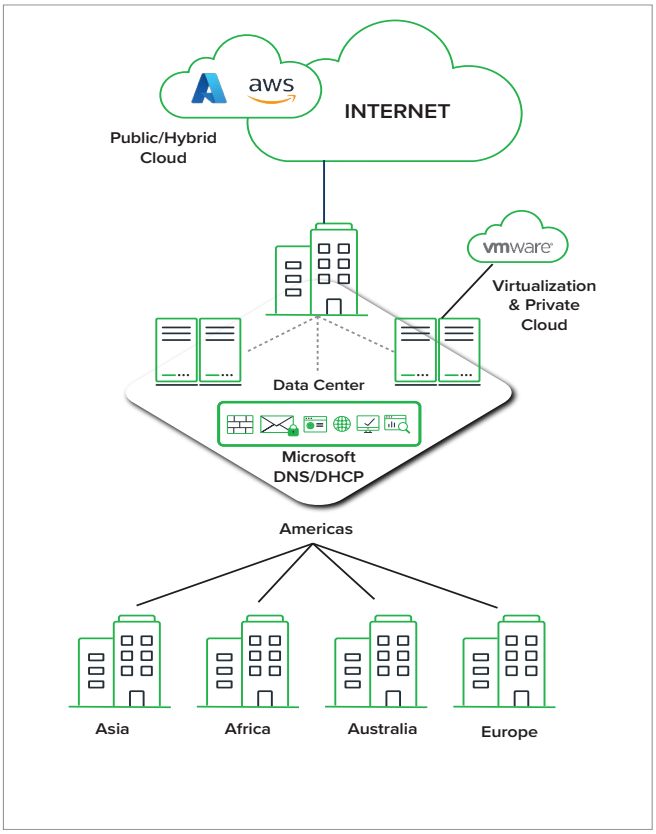

Figure 1 – Traditional DNS Backhaul ModelModel

Starting in 2019, the company began its phase two Infoblox rollout, upgrading hundreds of small, medium-size, and large appliances with NIOS DDI virtual machines in corporate, data center, subsidiary, and remote sites wherever possible. It eliminated over 200 Microsoft servers running AD and DNS. For smaller, on-premises remote sites and data centers with cloud SaaS environments, it installed cloud-managed BloxOne DDI for centralized visibility, an efficient, cost-effective deployment, and localized access, performance, and resiliency. Additionally, it rolledout Anycast to BloxOne, so its sites continue to work even if connectivity is disrupted.

With its focus on visibility, the company also chose to roll out Network Insight worldwide. Deployed by one of its subsidiaries, the company knew its power for discovering network assets, integrating layer-2 and layer-3 visibility, syncing IPAM device, end-host, and network port data, providing switchport management, detecting rogue and compromised assets, and resolving conflicts across devices and network ports. Network Insight reveals where all devices are connected, validates what's discovered versus what's on the network, flags the conflicts, and establishes authoritative IPAM for automation based on a trusted source of truth. It also correlates DDI data used by cybersecurity applications for a stronger, more proactive security posture.

In phase three, the company started its BloxOne Threat Defense deployment. Because of the company's size and stature, it knows it's going to be attacked multiple times daily. BloxOne Threat Defense uses DDI metadata for user and device visibility and improves SecOps productivity through automated data sharing. It uses DNS as a "signal" for security events and control point for protection everywhere—critical for a global operation. BloxOne Threat Defense also reduces the cost of threat defense by detecting and blocking malware and C&C attacks, closing infrastructure and data protection gaps, distributing threat intelligence, and improving SOC efficiency through integrated automations.

During the phase 3 rollout, Security Ecosystem was also being deployed to connect existing platforms (e.g., advanced threat detection, threat intelligence, SIEM and SOAR solutions, vulnerability management, network access control, endpoint security, next-generation firewall, etc.) to automatically notify the ecosystem of real-time events, trigger remediation, and share network context. DNS analytics provides even greater insight and threat protection. Unlike cloud-only solutions that fail when offline, BloxOne Threat Defense's hybrid architecture combines on-prem and cloud DNS capabilities to supply reliable, industry-leading protection and recursive access to the Internet for normal, continued business operations.

Finally, the company also installed Dossier and is using it extensively for contextual information to display data from multiple sources in a single view, which speeds threat investigation, aligns with threat-hunting workflows, and predicts future attacks. Dossier includes open source, proprietary, and premium commercial sources, and visibility into historical registration, reputation, and infrastructure relationships for greater context and insight.

THE RESULTS

Secure Uptime, Visibility, Efficiency and Lower Cost

With Infoblox, the company modernized its on-prem core and cloud-managed network services and strengthened its security posture. It deployed a cloud-managed BloxOne DDI environment that replaced siloed, error-prone, inefficient, non-scalable, and non-enterprise-grade Microsoft platforms. Infoblox helped enable network discovery and visibility into everything on its network and established authoritative IPAM—its single source of truth—to deliver centralized network visibility and empower automation for trusted accuracy and efficiency. As a result, costly Microsoft-related trouble tickets dropped from 30 to less than one per month, enhancing availability, eliminating disruptions, and significantly reducing support costs. The company also greatly simplified its network. Because oil companies work in diverse parts of the world with various constraints, flexibility is critical. Some places prohibit virtual server resources. While in other places, physical data center servers are not mandatory, so the flexibility of virtual deployments greatly simplifies management.

For remote and direct Internet access sites, the energy company deployed BloxOne DDI for centralized deployment, control, and locally survivable access to SaaS apps and services. This solution keeps services available and avoids adverse business continuity issues. Since BloxOne DDI is cloud managed through the portal, the IT team doesn't have to manage infrastructure. Updates don't take weeks; they are all done in minutes through the cloud, saving time and not requiring Change Advisory Board (CAB) cycles or approval. If needed, IT can configure and deploy a new BloxOne DDI hardware appliance in five to seven minutes and even less for virtual deployments. BloxOne DDI delivers authoritative and recursive DNS, DNSSEC, active-active or active-passive DHCP, and authoritative IPAM, and it scales to tens or thousands of locations—perfect for the company's global operation. In addition, it's reliable, doesn't generate trouble tickets, and keeps churning out DNS, even if it's not connected to the cloud. Best of all, BloxOne DDI substantially lowers costs for acquisition, deployment, and management. The company saved more than 50% in annual run cost over former Microsoft servers, and for public cloud deployments in AWS, BloxOne DDI scales at a fraction of the cost to deliver central visibility and control.

Regarding security, the company realized immediate results with its new BloxOne Threat Defense deployment. When first launched, it was deployed on more than 500 corporate campus desktops. It immediately detected over 100 devices connecting unencrypted DNS over HTTPS (DoH) on port 443 instead of port 53 and DNS over Transport Layer Security (TLS) (DoT). This meant that user communications were bypassing the local DNS server and security policies and connecting directly to Internet DNS clients without encryption, leaving the company vulnerable to snooping, interception, and data exfiltration. IT had no idea of its exposure until BloxOne Threat Defense uncovered the risk. In response, IT initiated an emergency workshop to enable encryption through the network DNS resolver to meet security and content policy requirements. Since then, BloxOne Threat Defense has proactively caught data exfiltration attacks and locked down the Grid so malware and bad actors can't wreak havoc throughout the company.

With Infoblox, the company's network now delivers consistently reliable uptime, full network discovery and visibility, authoritative IPAM, automation efficiency, and centralized control. It provides secure, flexible, highly scalable, high-performing local access, resiliency, and redundancy for disaster recovery, all at significant cost savings across the data center, remote locations, hybrid cloud, and around the globe. Infoblox's modern network solution allows the company to maintain and expand its industry leadership, focus on energy and chemical manufacturing, and develop next-generation fuel technologies to meet world demand.

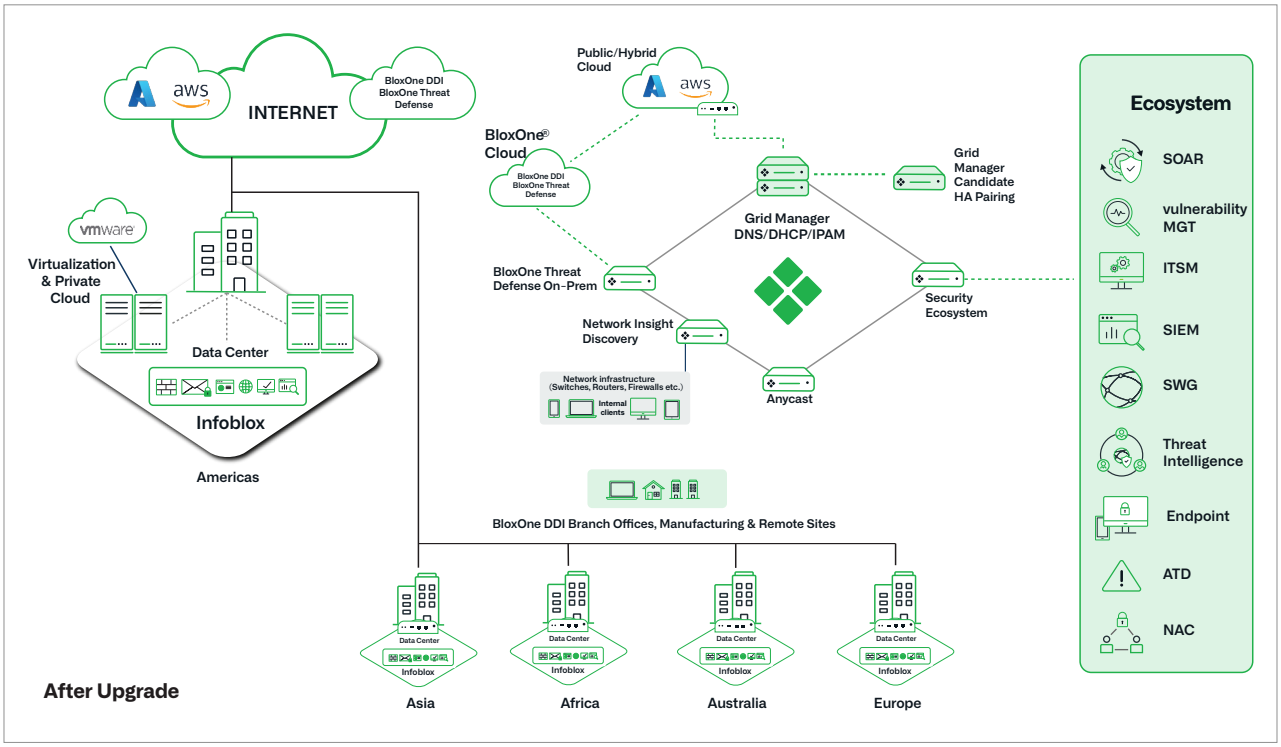

Figure 2 – Modern Distributed Model

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

+1.408.986.4000
www.infoblox.com

Version: 20240227v1