infoblox

CASE STUDY

Satellite broadband firm modernizes with Infoblox

Business continuity and simplification needs drive Microsoft DNS/DHCP replacement

OVERVIEW

This global provider of high-speed satellite broadband services and secure networking systems is a leader in the new defense industrial base for SATCOM and Cybersecurity.

The company delivers secure defense communications across the globe. It offers a range of multi-band, flexible SATCOM terminals, anti-jam Link 16 radios, and electronic warfare (EW)-resistant networks that enable resilient, end-to-end communications across domains and missions.

The company maintains many lines of business, with most running Microsoft Active Directory for DNS and DHCP. One of these businesses, however, used an Infoblox NIOS solution running on two Trinzic 1425 devices to manage IP address management (IPAM), and provision their private cloud using Openstack. The API support in NIOS made it ideal for this application. The company also ran Infoblox DNS Traffic Control (DTC) on the Trinzic appliances. An integrated DNS Global Server Load Balancing solution, DTC ensures business continuity through reliable application uptime, network performance and seamless failover. It distributes network traffic loads across geo-diverse, on-premises, public and hybrid cloud environments for e-commerce, customer-facing portals, web and internal business-critical applications for business continuity and disaster recovery in the event of a catastrophic event.

Industry: *Telecommunications*
Location: *Global*

INITIATIVES:

- Improve DDI management capabilities
- Automate DNS, DHCP and IP address provisioning across distributed locations from the cloud
- Detect and block a broad range of exploits, phishing, ransomware and other modern malware

OUTCOMES:

- Strengthened security posture
- Better network manageability from the cloud
- Faster deployment of DDI services to accommodate new devices and IP addresses

SOLUTIONS:

- Infoblox NIOS
- BloxOne DDI
- BloxOne Threat Defense
- Trinzic Appliances
- Infoblox DNS Traffic Control

THE CHALLENGE

Putting in place better performing technology to avoid network disruptions

When the company shut down its Openstack project, the decision was made to reassess its overall DDI situation. Its first consideration was to go with open-source Docker, BIND and Kea, but the IT team agreed to do a proof of concept (PoC) with BloxOne DDI from Infoblox. While the BloxOne DDI concept was highly successful, the team lacked the resources and motivation to execute the PoC to completion. Around the same time, the company encountered a WAN outage that broke their API capabilities and disrupted their DHCP services. The decision was then made by the firm's VP of Technology and their DNS architect to replace Microsoft Servers across the board with Infoblox technology.

THE SOLUTION

Hybrid architecture with cloud-native DDI from Infoblox

Because the DNS architect had joined Infoblox's Customer Advisory Board, the company was privy to the BloxOne DDI roadmap and heard from other Infoblox customers about their experiences with BloxOne DDI. These insights were instrumental in the firm's decision to go with NIOS virtual appliances for their main data centers as well as their public cloud deployment, and BloxOne DDI instead of Trinzic 825s in a few branches, replacing the Microsoft Servers. In all, the company purchased 42 BloxOne DDI licenses, 13 vNIOS subscriptions, and two 14x5 physical Trinzic appliances for high availability.

The firm also deployed BloxOne Threat Defense from Infoblox to optimize network security. BloxOne Threat Defense operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle. It is now a mandate at the firm to include BloxOne Threat Defense for all DNS deployments. The company is also using DNS Anycast and will eventually want Anycast DHCP, but hub-and-spoke functionality is sufficient for now.

THE RESULT

Stronger network security, better manageability from the cloud

With its hybrid NIOS + BloxOne DDI infrastructure in place, the service provider is now able to orchestrate and automate DNS, DHCP and IP address provisioning across distributed locations from the cloud. It is also now able to deploy DDI services to accommodate new devices and IP addresses faster than ever before, and it has clear visibility into end users and devices across the network regardless of their location.

With BloxOne Threat Defense the company has strengthened its security posture. It is now more adept at securing its work-from-anywhere workforce and has lowered its overall total cost for cybersecurity defense. Through pervasive automation and ecosystem integration, BloxOne Threat Defense drives efficiencies in SecOps, and uplifts the effectiveness of the legacy security stack. BloxOne Threat Defense uniquely combines advanced analytics based on machine learning, highly accurate and aggregated threat intelligence and automation to detect and prevent a broad range of threats, including DGA families, data exfiltration, look-alike domain use, fast flux and many others.

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

+1.408.986.4000
www.infoblox.com