A multi-national industrial conglomerate takes flight with security and DDI from Infoblox

THE CHALLENGE - CYBERATTACKS FROM MULTIPLE SOURCES

This multi-national industrial conglomerate has multiple business units and divisions within its portfolio.

Across its divisions, the company has over 200 locations distributed across 75 different countries. A global organization involved in aerospace manufacturing and defense technologies, the company supports over 35,000 users and 114,000 IP addresses that make use of the company's MPLS enterprise network.

With such a large global network footprint, the company represents a highly attractive target for threat actors. It's also the case that the company's network has become increasingly complex over time, requiring more advanced and more reliable performance for network operations, including DNS administration, DHCP and IP address management (IPAM)—collectively known as DDI.

When first engaging with Infoblox, the company had been increasingly facing attacks from multiple sources, including advanced persistent threats (APT) by nation-state actors. There was a need to introduce a new control point for security to help reduce the attack surface and mitigate risk in the face of the steady stream of attack traffic volume.

As their cybersecurity lead reflects, "We wanted a way to shut down noisy botnet traffic and other things that DNS is really good at. In fact, we identified DNS as a risk area but also a key area for improved control and combating threats."

Customer: Multi-National Industrial Conglomerate
Industry: Manufacturing, aerospace
Location: United States of America

INITIATIVES:

- Improve network visibility
- Detect and block more potential security risks
- Improve network resiliency

OUTCOMES:

- Improved security posture
- Reduced operational overhead for security management
- Simplified network operations

SOLUTIONS:

- Subscription-based Grid Technology
- BloxOne Threat Defense
- BloxOne DDI

THE SOLUTION

Improving network resilience with Infoblox

The company initially moved to Infoblox for security and threat mitigation but realized that the technology could also solve performance challenges it was facing with its DDI infrastructure. Their cybersecurity lead explained that there were various problems with the company's network zones that in some cases resulted in domain failures.

He noted that before migrating to Infoblox for DDI, the company was using multiple Windows servers to support its network operations. They moved all of their network domain zones up into the Infoblox infrastructure and eliminated the need for the Windows systems it was using for DDI. By migrating to Infoblox for DDI, the company saved money, improved performance and got a lot more resilience.

"We found that while a handful of Windows servers were unable to handle the load, just a single Infoblox appliance that we were already using for caching and security was more than capable of taking the same load without any real issue. The key was migrating to the Infoblox NIOS platform to manage all our DDI operations."

Keeping ransomware at bay

Among the most impactful types of threats that affect organizations today is ransomware. The organization's cybersecurity lead noted that ransomware has been one of its biggest concerns from a security perspective. He relates that "the work we do in defense technology is highly sensitive, which makes us a prime target for state-level actors. BloxOne Threat Defense from Infoblox is such an effective solution for us because it's specifically designed to combat the most sophisticated ransomware."

With some forms of ransomware, which can be highly automated, the malware will attempt to connect back to a command and control (C&C) server for instructions on how to advance an attack once a successful incursion has been made. This outbound traffic would necessarily involve activity at the DNS layer, presenting an opportunity to identify and stop such an attack. "With BloxOne Threat Defense, we're now able to identify if and when a ransomware dropper is attempting to connect to a C&C server, and we can instantly block that connection," says the cybersecurity leader. "In our view, Infoblox provides an extremely cost effective anti-ransomware solution that doesn't require decryption, rather it just sits inline and blocks attacks from being successful in the first place. Ransomware would sometimes get backed up by some of our other security appliances, but it could never get past Infoblox."

THE RESULTS

Five years of unbroken uptime

Network operations need to always be available and that's a function that Infoblox has helped to enable for the whole company. The organization has enjoyed over five years of unbroken uptime thanks in no small part to its deployment of Infoblox. With a high volume of DNS traffic, the company has confidently relied on Infoblox as a foundational element of its DDI infrastructure. The IT network and cybersecurity team has been able to "set it and forget it"—especially on the threat prevention side, as the technology works seamlessly to reduce risks. "We get on the order of 150,000 requests per second all day every day," explains the cybersecurity lead. "Infoblox handles the load without any issues at all."

A refreshing customer experience

The company has enjoyed a positive experience and strong security and DDI performance thanks to its Infoblox deployment. That superior customer experience led them to bring in Infoblox as part of a refresh cycle for their network. The company periodically does an evaluation and deployment review of its network services, which also includes two other vendors that also have DNS security solutions.

As part of the refresh, the company is taking advantage of the latest Infoblox software-as-a-service capabilities, including BloxOne Threat Defense and BloxOne DDI. BloxOne Threat Defense provides an always-on, highly scalable and easy to deploy approach for threat detection and mitigation.

BloxOne DDI provides low-cost network services to remote locations for better performance and improved user experience. "Right now we're not finding a compelling reason to add another vendor into the space," says the IT lead. "What we have with Infoblox works, and the price point is about what we want for this technology."

Exceptional professional services and support

A cornerstone of the positive relationship with Infoblox comes from the value of support, training and professional services. In the few cases where the team has encountered problems or where their implementation didn't work as expected, the Infoblox support team has been responsive and able to resolve whatever issues were encountered.

On training, the feedback from the team has all been very positive. Some of the company's analysts have even gone so far as to say that Infoblox has provided the best DNS and DHCP training they have ever received. Concludes the IT lead: "I think what you're seeing is the difference between the quality of the professional services engagement and the technology—that's why we're expanding the relationship we have with Infoblox."

For more information

Core Networking

To learn more about how you can easily deliver better networking experiences from anywhere, visit the Infoblox website or try Infoblox for free today.

BloxOne DDI

Learn more about how you can simplify your cloud experience and unleash the full potential of SD-WAN. Speak with an Infoblox Cloud Specialist or start your free trial for 60 days today.

BloxOne Threat Defense

Learn more about how you can proactively detect malware and protect your users and data via DNS. Speak with an Infoblox representative or start your free trial of our BloxOne Threat Defense technology today.

---

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