infoblox

CASE STUDY

An online dating company achieves scale and security while migrating network services to AWS

EXECUTIVE SUMMARY

An online dating company with a worldwide geosocial networking application has millions of users, over a billion dollars in revenue and has grown quickly.

During the Covid-19 pandemic, the number of online dating users increased as users became more isolated.

Management has aggressive plans to increase their product offerings and grow their number of users. They are rolling out products with features to provide more information, improve safety, and deliver more ways to connect socially with other users utilizing the latest cutting edge technology.

The company migrated an Infoblox vNIOS DDI (Secure DNS, DHCP, and IP Address Management) network services subscription license into the Amazon Elastic Compute Cloud (Amazon EC2). They had purchased BloxOne® Threat Defense to improve their network security which is also deployed in the Amazon Web Services (AWS) cloud. With the utilization of BloxOne Threat Defense, they were able to improve their security posture and leverage contextual data to more quickly identify and resolve threats.

BloxOne Threat Defense is a welcome addition to the company's line of defenses to provide DNS security and address the many data breach and crypto mining attacks targeting the online dating industry.

THE CHALLENGE

The company was an existing Infoblox customer running vNIOS DDI on on-prem appliances. They recently moved to a new headquarters which was very tight on rack space. They needed to reduce their on-premises footprint.

RESULTS:

- Achieve centralized control of core networking services - DNS, DHCP, and IPAM for AWS environments as well as improve their security using DNS.
- Leverage integration with Splunk and security event metadata that could accelerate their Mean Time to Detection (MTTD) and Mean Time to Remediation (MTTR).
- Manage their own custom blacklists and IOCs by building a custom list to block employees from going to sites where attackers could launch attacks to steal data or get access to cloud privileges for the purpose of mining bitcoin.
- Improve their security posture and take core services like DHCP off the critical path for the move-in project.

Moreover, online dating companies gather very sensitive customer information. Customers want to keep their online conversations, location, pictures and other personal data private. Hackers can use the information to blackmail the company or their customers. Customers may discontinue service or not sign up in the first place if they don't have confidence that their information is being kept secure. The reputation of the company and revenue can be severely impacted by a successful cyber attack.

In 2015, hackers compromised the personal customer data of another popular online dating site. The security breach made the national news, and the data was posted publicly. This resulted in a multi-million dollar lawsuit, and customer embarrassment. Due to the severity of the data breach, this was undoubtedly a wake up call that prompted the breached company and others in the industry to revisit their security strategy and improve their security solutions.

Due to the large number of customers and sensitive information at online dating companies, they are prime targets for hackers.

In addition to protecting their data, the company is particularly concerned by attacks where hackers get access to cloud credentials that can then be used to create new compute instances for crypto mining.

How can the company keep their servers and data safe from ongoing attacks?

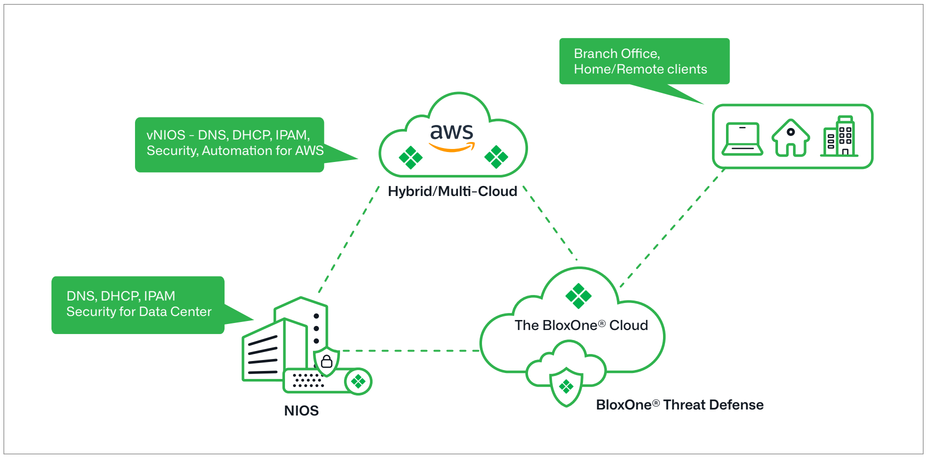
THE SOLUTION

Infoblox worked with the company to install BloxOne Threat Defense in AWS cloud. That in addition to their NIOS based DDI AWS cloud deployment, provided them with a complete DDI and security solution that helped them achieve centralized control of core networking services - DNS, DHCP, and IPAM for AWS environments as well as improve their security posture.

Their Infoblox Solution Architect was able to show them how to build and manage custom lists that included both information from Infoblox feeds as well as their own curated block lists from indicators on their network.

The company could also now rapidly access contextual data across their cybersecurity ecosystem via Infoblox's integration with Splunk, and the availability in Splunk of Infoblox RPZ hits information. The desire to move to a SOAR enabled environment, integration with Splunk, the adoption of the MITRE ATT&CK framework, and the need for a strong defensive cloud security solution resulted in the implementation of BloxOne Threat Defense along with NIOS DDI which met their key objectives.

The new staff had experience with Infoblox and knew that NIOS DDI along with BloxOne Threat Defense in the AWS cloud would give them a solution that would meet their needs.



OUTCOMES

This online dating company has successfully migrated enterprise grade core networking services - DNS, DHCP and IPAM - to their AWS environments as well as improved their security posture. Moving to AWS provided them with an easy to maintain, scalable solution.

Being particularly concerned by attacks where bad actors get access to customers' cloud credentials that can be used for crypto mining, the company was able to reduce their risk by using Infoblox threat intelligence feed for crypto mining, as well as their own IOCs (Indicators of Compromise) they want to block in custom block lists. And their MITRE team appreciates the Infoblox integration with Splunk to have visibility to Infoblox RPZ hits.

BloxOne Threat Defense also improves key SOC and network operations performance metrics such as Mean TIme to Detection (MTTD) and Mean Time to Remediation (MTTR). Granular visibility and accurate timestamping ensures properly informed priority. This will decrease the amount of time spent by the security team researching threats and result in a strong return on investment (ROI) for the company.

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