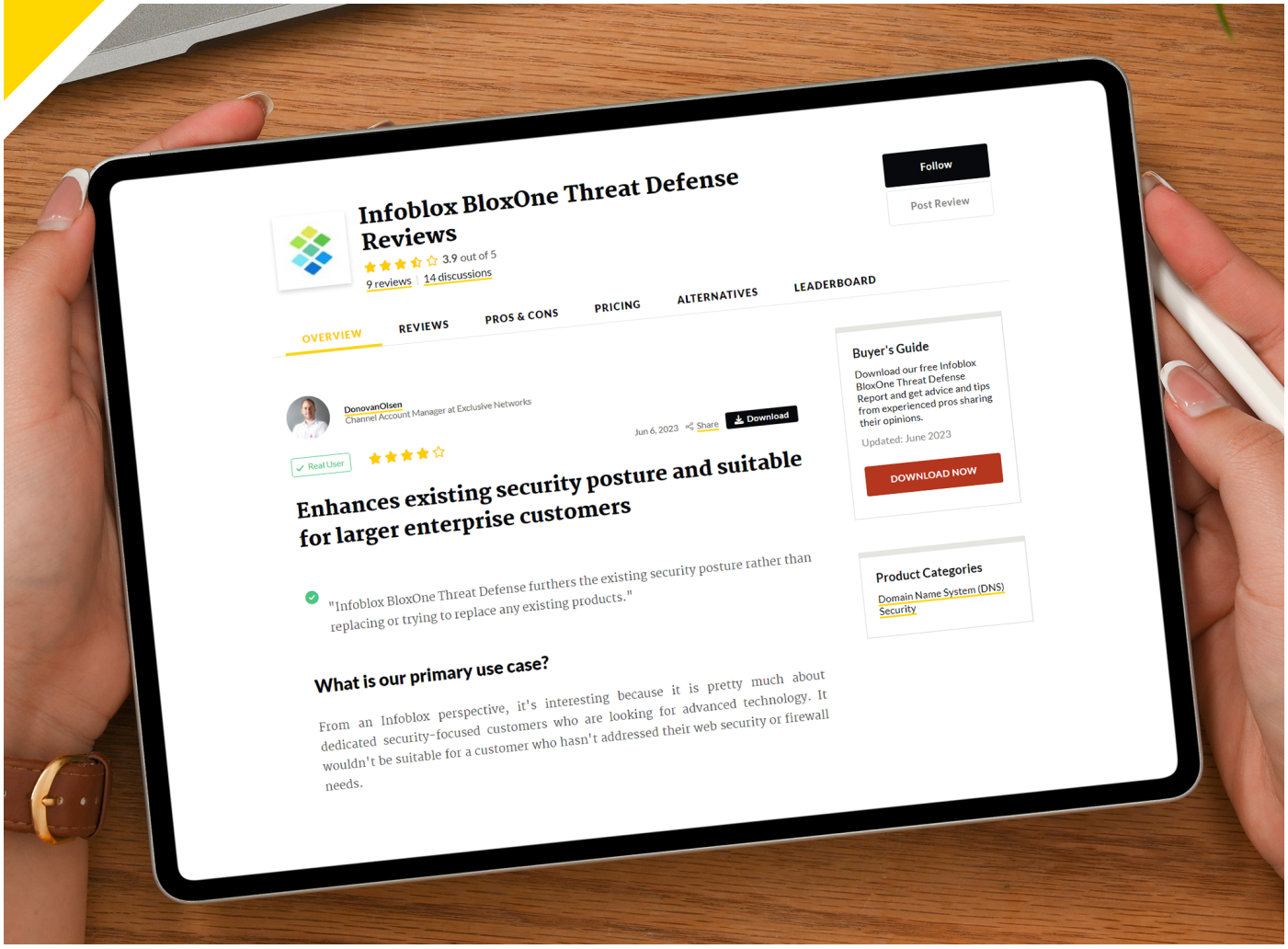
PeerPaper™ Report 2023

Based on Real User Experiences with Infoblox BloxOne

How a Unified View of NetOps and SecOps Enables Improvements in Performance and Protection



PeerSpot

Contents

Introduction

Network operations (NetOps) and cybersecurity overlap to such a great extent that they are often virtually the same workload. This is particularly the case with Domain Name System (DNS) processes, which affect both NetOps and security operations (SecOps). Security is indeed an important factor at the DNS level. Security and network managers need to apply strategies across the security tech stack to achieve alignment between NetOps and SecOps. Automating relevant data processes allows this to happen in real time. In this paper, users of Infoblox BloxOne Threat Defense and Infoblox NIOS DDI—which unifies DNS, DHCP and IPAM across premises—discuss how these solutions enable them to achieve a unified view of NetOps and SecOps. These users have realized gains in both operations and security by leveraging a solid foundation for DNS protection and DHCP protection, coupled with DNS monitoring, visibility, detection, and response processes.

Except where noted, the companies featured in this paper have over 10,000 employees.

The paper uses the following acronyms:

- DDI — DNS, DHCP and IPAM
- DHCP — Dynamic Host Configuration Protocol
- DSCP — Differentiated Services Code Point
- DSTP — DataSocket Transfer Protocol
- IPAM — IP Address Management
- NIOS — Network Identity Operating System

Infoblox Use Cases

PeerSpot members are putting Infoblox solutions to work in a variety of use cases, realizing the value of applied security at the DNS level to protect their organizations in the process. For example, a Technology Manager at a tech services company uses Infoblox IPAM for DSCP IP assignments and DNS host records. The solution helps him maintain the complete network database for the company.

A Lead Engineer at a tech services company utilizes IPAM mostly for internal DNS appliances. He said, "The designs vary as we have different layers of structures that we run, but in general, we have branches, the data center and we also have block storage on the cloud. We're using a combination of all Infoblox products that we manage both on the cloud and on-premises."

"Our primary use case is for all security-type query activities," said a Principal Engineer who uses BloxOne Threat Defense at T-Mobile, a comms service provider. He added, "So, if somebody is trying to hack or infiltrate us, that is why we use Threat Defense in the cloud. We use it to monitor queries coming in and out of our company."

BloxOne Threat Defense acts as a firewall for DNS traffic at a recruiting/HR firm. According to their Network Engineer, "If a domain has malware on it, it [BloxOne Threat Defense] can intercept that even before it gets to our firewall. We don't give any response to dangerous domains."

Firewall for DNS traffic

Eli K.
Principal Engineer
at T-Mobile

"If somebody is trying to hack or infiltrate us, that is why we use Threat Defense in the cloud. We use it to monitor queries coming in and out of our company."

Read review »

DNS is the most important part of networking for a Senior Network Architect who uses BloxOne Threat Defense for DNS protection at the State University of New York (SUNY) at Stony Brook. As he put it, "We point our local domain name servers to it and it has a feed for 'bad character' domain names. We protect our end-users that way."

He went on to say, "Not so many people see it that way, but if you can't resolve, say, 'cnn.com,' nothing works. If your DNS doesn't work correctly, nothing is going to work correctly on your network. It is one of the first layers that comes into play when going to a website or using email."

CNN also figured into the use case of a Virtualization/ Datacenter Engineer who uses BloxOne Threat Defense at a healthcare company. He said, "It looks at all our DNS queries and activity going out of the company." Like BloxOne customers on PeerSpot, this user leverages DNS protection to stop critical threats earlier in the attack cycle than was previously possible. He added, "Anytime that someone is looking up CNN or something like that, this cloud solution looks at it and decides if it's a known spam, malware, virus or phishing site. If it is any of those things, it will just simply not allow the DNS query. So, it is a great addition to our firewall and network security. It is just another layer. Why let the PC go to the bad website or access the bad IP address when it can just block it right there in the DNS?"

Visibility Benefits

The automation of DDI management brings increased, real-time visibility to NetOps and SecOps teams—helping to bolster their network performance and protecting their organizations. Indeed, visibility is critical to success with both NetOps and SecOps. In this vein, Infoblox users praised how the solutions enabled them to focus and view user access and new devices on the network. As an IT Infrastructure Specialist who uses BloxOne Threat Defense at a transportation company put it, "We have more visibility, granularity, and contextual information about threats." Figure 1 captures this capability.

Infoblox BloxOne Threat Defense helps T-Mobile's Principal Engineer improve the way his team looks at data as it comes in and out. He said, "We monitor and manage queries from every device that sits inside our company, e.g., every user, every laptop and every query. When you type something into the web, Infoblox will scan or manage that." From there, he shared that if the query is going somewhere bad, Infoblox will block it. He added, "From a metrics perspective, it gives us data, letting us go back and find those impacted or infected clients to either clean their devices or remove them from the network."

Real-Time Visibility

Onur P.
Network & Security
Specialist at Infrasis

"There are many tools on the market; however, the other products don't combine DNS, DSTP and IP management in one solution."

Read review »

Combined features for visibility are what mattered to a Network & Security Specialist who uses IPAM at Infrasis, a small tech services company. He said, "There are many tools on the market; however, the other products don't combine DNS, DSTP and IP management in one solution. The power of Infoblox IPAM is that it offers all of those, opening up capabilities such as creating IP management tables and providing an overview of the network infrastructure." He then said, "The best feature is the Discovery feature, which provides enhanced visibility over the entire network infrastructure and automatically creates DNS records for discovered IP addresses."

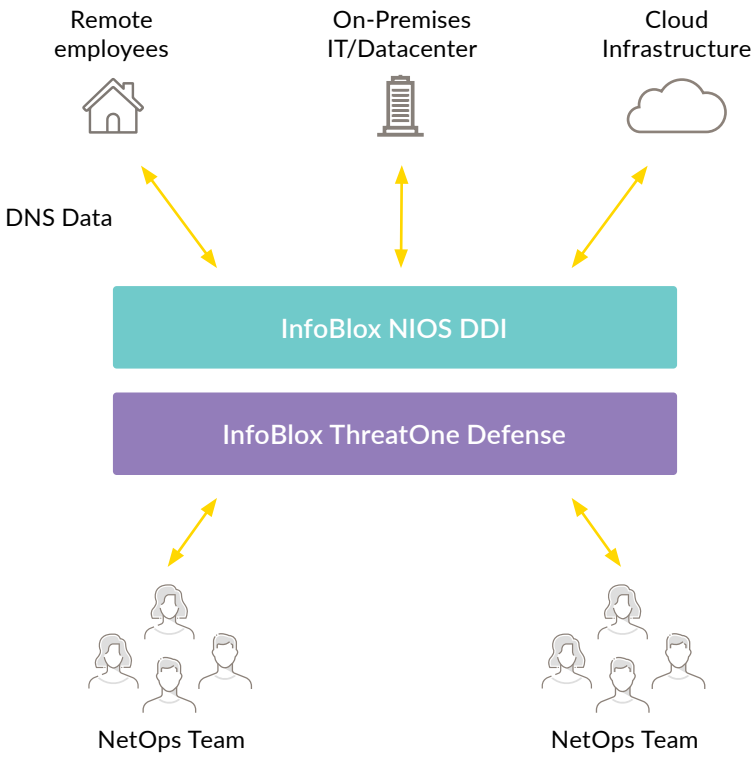


Figure 1 – Infoblox NIOS DDI and ThreatOne Defense provide NetOps and SecOps teams with detailed DNS information from remote employee locations, on-premises IT, and datacenters as well as cloud infrastructure.

Other notable comments about visibility included:

- "IPAM's best features include the view of how many soft nets are filled from your container and the grid master. It's also excellent for server management." - NOC Technical Lead who uses IPAM at NCR Corporation, a tech services company
- "The Discovery feature provides a clear network overview, while the solution also provides security options with features like robust DNS security." - Network & Security Specialist who uses IPAM at Infrasis
- "There's reporting and monitoring in the portal itself, and what customers can view. Additionally there are add-on programs specifically for Infoblox programs that go with Splunk. There are several tools available that add extra visibility." - Principal Network Engineer who uses BloxOne Threat Defense at Pegasystems, a software company with more than 5,000 employees

Onur P.
Network & Security Specialist at Infrasis

"The Discovery feature provides a clear network overview, while the solution also provides security options with features like robust DNS security."

Read review »

NetOps Gains

IT organizations tend to struggle with efficiency in NetOps. It's an area of IT that contains more than one complex workload. It also demands expertise, which can be hard to find. Solutions that improve NetOps productivity and effectiveness earn praise from users and their managers. In this context, PeerSpot users found that Infoblox made it possible for NetOps to function better through ease of use and a unified interface.

The transportation company's IT Infrastructure Specialist put it this way: "DDI affects our network and operations in a very positive way." In contrast to companies that use public DNS servers, his firm separates its traffic on its VPN using Threat Defense. He added, "With Threat Defense, we are controlling the DNS traffic. We can make sure that certain DNS domains are resolved only over our internal DNS service."

NetOps Efficiency

"Before IPAM (IP Address Management) came into the picture, every user had to depend on an Active Directory engineer to get an IP assigned," said the tech services company Technology Manager. Infoblox allows him, and others, to improve efficiency and automation by simplifying the manual management of networks. To this point, he then said, "With Infoblox IPAM, there's automation or auto assignment of IP addresses which is a valuable feature. There's also the capability of storing many networks in one place through the solution. Infoblox IPAM solved the major issue of needing an Active Directory engineer to assign an IP."

Darrin B.
AVP Technology Network Engineer at LPL Financial

"Having that in a single pane of glass where everyone in IT can see it is a huge benefit for us."

Read review »

This user also remarked, "My rating for Infoblox IPAM is ten out of ten because you can use it to combine the work of ten employees into one. You won't need ten Active Directories because you only need one Infoblox as it's able to handle the complete Active Directory environment of your organization." For him, Infoblox was an improvement over depending on Windows Active Directory for IP requirements.

Ease of use was an operational benefit for SUNY Stony Brook's Senior Network Architect. His team found the solution and graphical user interface (GUI) easy to use and intuitive to navigate, letting people "do whatever it is that you want to do with the system."

An AVP Technology Network Engineer who uses IPAM at LPL Financial, a financial services firm with more than 5,000 employees, put the management challenge in context, saying, "There are an enormous number of IP addresses." With that in mind, as he said, "Having that in a single pane of glass where everyone in IT can see it is a huge benefit for us."

Detection and Response Processes to Help SecOps

The faster and more efficiently a SecOps team can detect and respond to a threat, the better the organization's security posture will be. BloxOne Threat Defense supports this goal, benefitting SecOps by improving users' threat detection and response processes.

For instance, T-Mobile's Principal Engineer shared that the solution has reduced the amount of effort involved for their SecOps teams when investigating events. He elaborated, saying, "Infoblox has probably helped clean up about 35% to 40% of the time that our SecOps team has to spend tracking down bad actors since the system will automatically take care of it for them." Figure 2 depicts this outcome.

Easier to Troubleshoot

This user further stated that BloxOne Threat Defense allows his SecOps and support teams to monitor and manage any alerts in the cloud. He said, "If something goes down, then they are alerted. Administration is done by the data center engineers. This is just a handful of people, maybe 25 people at the most." In other words, a small team can take care of threats at a large company.

He then spoke to the solution's threat data management capabilities. Infoblox is known for automation that delivers real-time data, allowing near real-time responses for SecOps. He commented, "Infoblox, as a whole, has been able to allow our SecOps teams to better manage data coming in and out of our network. Before, they had to do a lot of that work manually using several different systems to manage that traffic. Now, all traffic is sent to a logging system, then that logging system parses all that data and spits out things that may need attention."

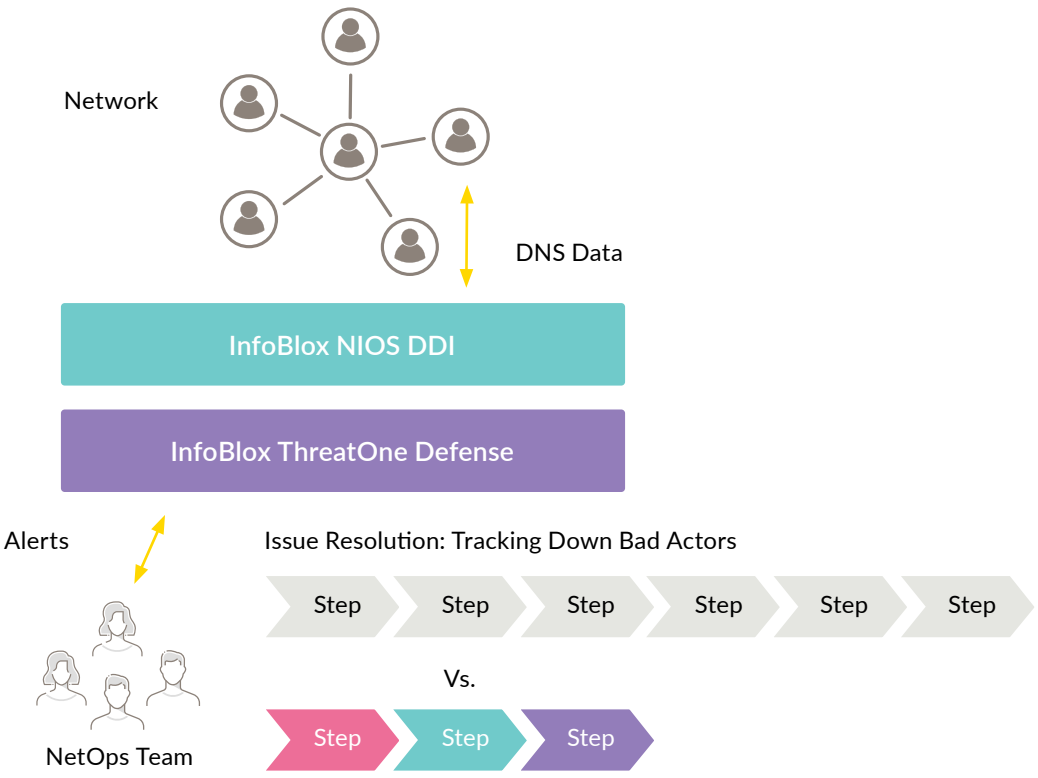


Figure 2 – Using Infoblox NIOS DDI and ThreatOne Defense enables SecOps teams to resolve issues, such as tracking down bad actors, more quickly than was previously possible.

Reduction in SecOps team investigative efforts is what stood out to SUNY Stony Brook's Senior Network Architect. He said, "Overall, it's much easier to log, detect, and troubleshoot those aspects of the network. The number of false positives is very low, close to none. More than once it has detected new names or lookalike names and protected us and saved us from bad characters."

The transportation company's IT Infrastructure Specialist contrasted the solution to its predecessor for monitoring, detection and response processes. He shared, "When it comes to the DDI side of things, we now can work more granularly. We have a more controlled way of doing DNS resolutions. Before, we used Microsoft DNS and Microsoft DHCP, and those Microsoft products don't have the features that Infoblox has."

His company had also previously used BlueCat, which lacked Infoblox's feature set as well as the ability to scale. He then noted, "BloxOne Threat Defense is very good at helping to detect DNS threats." Using the solution on a daily basis, they have identified possible data exfiltration events already. He added, "It can detect threats that cannot be detected by the other security tools that we have evaluated."

Behzad B.
Senior Network Architect at
SUNY at Stony Brook

"Overall, it's much easier to log, detect, and troubleshoot."

Read review »

Network Engineer
at a recruiting/HR firm with
10,001+ employees

"If a domain has malware on it, it [BloxOne Threat Defense] can intercept that even before it gets to our firewall. We don't give any response to dangerous domains."

Read review »

"BloxOne [Threat Defense] has positively affected our monitoring and detection response processes because it gives us a clearer picture of what's happening in our environment and it simplifies forensics," said a DNS Guru at a healthcare company. This resulted in a reduced effort required by the company's SecOps team because, as she said, "It gives them additional information that they didn't have access to before."

She went on to reveal that her company has benefitted from BloxOne Threat Defense because it enables the SecOps team to more rapidly identify and respond to potential issues that their other security tools haven't discovered, or discovered later. She stated, "It has given us a better security posture than we would have, using only the other tools that we have."

"I'd say we had 100% [improvement]," said a Principal Network Engineer who uses BloxOne Threat Defense at Pegasystems. That's how much the solution helped the company's SecOps team cut its time on investigating events.

Security Gains

Infoblox users spoke to the benefits of improving DNS security layer by getting better at detecting, preventing, and managing threats. They explained how their overall security became more robust through the adoption of NIOS DDI and BloxOne Threat Defense. As the healthcare DNS Guru explained, "The most valuable feature is the security aspect, which is why we bought it. As a healthcare company, we're a potentially high-value target, and this helps provide an extra layer of security, especially with people working from home, where we can help prevent them from accidentally or intentionally reaching some of the malicious sites, and either having their machines compromised or being part of data exfiltration and infiltration attempts."

She further stated, "This type of DNS-specific tool is an important part of a security solution that is not covered by other security tools, such as a next-generation firewall." For her, the protocol-agnostic nature of BloxOne Threat Defense is a significant advantage when it comes to the web traffic that it blocks. "For example," she said, "it finds purely DNS traffic that's in a lot of cases, missed by firewalls. This is important because it gives us another layer of protection. It's another vector for us to implement our security policies so that we're not reliant on a single technology or a single vendor."

Extra Layer of Protection

IT Infrastructure Specialist
Infrastructure Applications
at a transportation company with 10,001+ employees

"We have more visibility, granularity, and contextual information about threats."

Read review »

DNS tunneling is the security threat that was most on the mind of Infrasis's Network & Security Specialist. He shared that this threat had proven to be difficult to protect against based on their tests with other types of security devices. "However," he said, "Infoblox eliminates this issue and provides excellent security against a difficult threat. We chose this product because it provides us with IP management and a DNS and DSTP solution. From a security engineer's perspective, Infoblox DNS security is the best in the industry."

In functional terms, security benefits arose for PeerSpot members from BloxOne Threat Defense's integration capabilities and ease of use. The healthcare DNS Guru related that the product integrates with other security solutions, such as vulnerability scanners, which her team is working to leverage more fully. She said, "The integration gives us a single pane of glass, where it brings together all of the information into a single platform where we can view and evaluate it. This is important because it gives our InfoSec team a better handle of what's going on and where problems might be, and how to address them."

The healthcare company's Virtualization/Datacenter Engineer liked the solution's client, which can be installed on mobile laptops and configured to forward all DNS queries from those laptops to the DNS servers, no matter where they are. He observed, "No matter where somebody is… the protection of their laptops are going with them. Using the reporting, we can tell that we have gained an extra layer of protection. Just by looking at it, we can see what is being blocked before it even makes it to the firewall. It is definitely working."

Conclusion

Effective DNS management, DHCP and IPAM are critical for success in NetOps. Implemented the right way, they also effect better security outcomes by offering a single view of NetOps and SecOps. Infoblox NIOS DDI and BloxOne Threat Defense realize this potential, as PeerSpot members described in their reviews of the solutions. Using NIOS DDI and BloxOne Threat Defense, they have been able to achieve better visibility into networks and potential threats—aligning with the solutions' purpose of providing real-time visibility and control over who and what connects to the network. Detection and response processes also get better, helping SecOps in the process and enabling customers to build safer, more resilient environments. PeerSpot members further found that NIOS DDI and BloxOne Threat Defense helped them improve NetOps efficiency.

About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Infoblox

Infoblox unites networking and security to deliver unmatched performance and protection for a world that never stops. By providing real-time visibility and control over who and what connects to the network, we use intelligent DNS and user context to stop threats other solutions will miss, enabling organizations to build safer, more resilient environments. We're continually supporting more than 13,000 customers—including 92 of Fortune 100 companies, as well as emerging innovators—by building the brightest, most diverse teams and by thoughtfully engineering intelligent networking and security solutions for an increasingly distributed world. Visit infoblox.com, or follow-us on LinkedIn or Twitter.