

CASE STUDY

EagleView soars with improved DNS security from Infoblox



With headquarters in Bellevue, Washington, EagleView assists organizations around the world with access to high-resolution aerial imagery and data analytics.

With EagleView Reveal, the company provides its customers with highly detailed aerial images with a ground sample distance (GSD) of 5cm or better—a level of resolution up to 4x the detail of standard aerial imagery. EagleView’s product portfolio also includes solutions to help its customers conduct virtual property assessments.

EagleView’s customer base crosses multiple industry verticals, including government, insurance, construction, solar power and utilities. Outside the United States, the company has offices in Bangalore, India, and Perth, Australia.

THE CHALLENGE

Transitioning to support a remote workforce

With the onset of the global COVID-19 pandemic, EagleView shifted its approximately 1,000 employees to a remote work model, which it wanted to proactively secure with visibility and remediation tools extending to the network’s farthest edges.

Leveraging DNS security

EagleView first engaged with Infoblox to increase overall network visibility and make full use of DNS security, frequently a blind spot for many enterprises. “Infoblox helped us close the DNS security gap that otherwise might have exposed us to potential risk,” says Chris Burch, the chief information security officer at EagleView.

“Infoblox was a great help in making it easy for us to proactively get the visibility and security remediation we needed across our expanded remote environment. We appreciated the speedy and easy deployment as well as the cost efficiency.”

Chris Burch,
Chief Information Security Officer,
EagleView

Beyond gaining visibility into DNS security, EagleView has, by engaging with Infoblox, improved security automation and threat intelligence, helping the IT team better understand and mitigate a spectrum of potential risks. One result is that remote workers now benefit from enhanced security that proactively protects them and EagleView.

THE SOLUTION

Rapid security rollout for remote workers

EagleView needed a security solution that could be deployed rapidly to help secure both the company and its employees. With most staff working remotely, the solution had to roll out nimbly and scale to cover users wherever they were located.

Infoblox BloxOne Threat Defense Advanced was the ideal solution for EagleView because the IT team was able to deploy it quickly to supply users with an unprecedented level of protection. The cloud-managed service readily onboards users and gives administrators an optimal approach to manage users. EagleView simply forwards recursive Internet DNS queries to the BloxOne Threat Defense solution, which enables an agile and flexible deployment model.

“The shift to a majority remote workforce created a security gap in our on-premises infrastructure that Infoblox resolved through the cloud, simplifying deployment on my team,” says Burch.

A security solution for Today’s challenges

BloxOne Threat Defense maximizes brand protection by working with existing, in-place defenses to protect network resources and automatically extend security to digital imperatives, including SD-WAN, IoT and the cloud. It powers security orchestration, automation and response (SOAR) solutions, slashes the time to investigate and remediate cyberthreats, optimizes the performance of the entire security ecosystem and reduces the total cost of enterprise threat defense.

The solution turns core network services into valuable security assets. These services, which include DNS, DHCP and IP address management (DDI), play a central role in all IP-based communications. With Infoblox, they become the foundational common denominator that enables the entire security stack to work in unison and at Internet scale to detect and anticipate threats sooner and stop them faster.

THE RESULTS

DNS security for remote users

Prior to implementing Infoblox, workers’ use of a virtual private network (VPN) to help secure traffic back into EagleView’s network exposed a security gap. Although the DNS lookup was going to the corporate DNS servers over VPN, some traffic went over the home connection because VPN allowed split tunneling.

With split tunneling, the existing corporate proxy servers could not see all network traffic from that one location, making them unable to block potentially bad traffic. Now, with BloxOne Threat Defense, if a user looks up a potentially malicious site, it is blocked, and the user cannot traverse from their home network to that site because typing in the web address results in a redirected name resolution.

Customer: EagleView
Industry: Aerial imagery, data analytics
Location: Bellevue, WA

INITIATIVES:

- Improve security for both remote and internal users
- Increase visibility into network operations
- Prevent users from accessing malicious websites

OUTCOMES:

- Removed DNS security blind spot
- Mitigated threats, including ransomware, malware, botnet communications and unintended data exfiltration
- Enhanced security for all users

SOLUTIONS:

- BloxOne® Threat Defense Advanced

Threat intelligence and content protection get a boost

BloxOne Threat Defense also enables EagleView to benefit from enhanced security capabilities. Part of the overall solution are advanced threat intelligence capabilities that help to inform and protect EagleView and its employees from threats.

The threat intelligence provided by Infoblox gives EagleView insights into potential risks from different hosts, domains and IP addresses. BloxOne Threat Defense integrates over 27 different threat intelligence data feeds that provide actionable insights. Those insights have made EagleView and its employees safer by continuing to give them deep threat intelligence to help defend the organization.

BloxOne Threat Defense can automatically mitigate multiple types of threats, including ransomware, malware, botnet communications and unintended data exfiltration. EagleView now has extended visibility across its organization, including on-premises, cloud and remote users.

Security without hassles

“Infoblox was a great help in making it easy for us to proactively get the visibility and security remediation we needed across our expanded remote environment,” says Burch. “We appreciated the speedy and easy deployment as well as the cost efficiency.” By integrating Infoblox technology into the organization, EagleView was able to quickly solve a number of its key security challenges, without any “heavy lifting” or disruptive software installation. Forwarding DNS traffic from EagleView’s internal DNS servers to the cloud was the fastest way to put security in place.

An Eagle’s eye view of the future

DNS security and the need to quickly protect remote workers are the foundations of EagleView’s next-level network experience with Infoblox. But the IT team will be considering additional technologies, such as the cloud-native BloxOne DDI platform to simplify and optimize networking for the borderless enterprise.

For more information

To learn more about how you can improve your organization’s network reliability, simplify network management with a unified platform for your core network services and more, visit the [Infoblox website](#) or try [Infoblox for free](#) today.



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