infoblox

CASE STUDY

Oxnard Union High School District Leverages Network Intelligence to Enable Proactive Security with Infoblox

OVERVIEW

The Oxnard Union High School District (OUHSD), located in Ventura County, California, consists of 13 schools serving students in grades 9–12.

The district encompasses the Oxnard Plain, including the cities of Oxnard, Port Hueneme, and Camarillo, as well as the nearby unincorporated communities of El Rio, Somis, and Channel Islands Beach.

> *"With BloxOne Threat Defense, we feel much more confident in our ability to protect each user and device across the entire district from cyberattacks and prevent incidents before they happen"*
>
> **Juan Castano**
> **Senior Network Administrator, Oxnard Union High School District**

THE SITUATION

Disparate Networking Operations

The district provides each of its nearly 17,000 students and 1,900 faculty and staff with the technology and support they need to maximize learning outcomes. For Juan Castano, senior network administrator for OUHSD, it is a collaborative undertaking. "Everyone works together to get things done."

Schools in the district provide students with either Chromebooks or Windows laptops, along with internet connectivity, online portals, and other digital services. From a networking and security perspective, OUHSD must also accommodate the diverse range of additional laptops, tablets, and other personal electronic devices used by students and faculty throughout the day.

Against this backdrop, the district's landscape for managing critical network services had evolved over time to include disparate solutions, including Microsoft DNS and Active Directory, along with custom domain controllers. The district also used Infoblox NIOS for certain networking zones. On the security front, Castano and the 15 field technicians he works with had no reliable means of detecting and stopping security events before they occurred.

OXNARD UNION HIGH SCHOOL DISTRICT
Creating Prosperity through Equity, Inquiry, and Wellness

THE CHALLENGE

DNS Conflicts and Time-Consuming Security

When Castano stepped into his current role two years ago, it was clear that OUHSD's network infrastructure had been hindering efficiency. To streamline operations, he and his co-workers began eliminating outdated servers and services that were obsolete. However, as that work began, they started encountering failures and certain services became unreachable. "Things just would not work," he recalls.

The root cause was soon traced to disjointed solutions for DNS, DHCP, and IP address management—collectively known as DDI—that make all modern network interactions possible. As the district's IT infrastructure evolved over time, DNS traffic had been configured to route to Microsoft DNS servers and Infoblox NIOS servers. The resulting DNS conflicts affected network performance. Additionally, basic functionalities, such as Network Time Protocol (NTP), which synchronizes computer clocks on network devices, were also running on multiple systems. "Things were pointing to each other. It was a huge mess," Castano says.

In addition to network management concerns, OUHSD also faced pressing issues with security due to time-intensive threat investigation and response processes. When Castano and his colleagues received a security alert, they had to embark on a lengthy, multi-step investigation, jumping between multiple tools to identify the device(s) involved, uncover details about the threat, and initiate containment or other response actions. This process was not only time-consuming but also very reactive. "By the time we completed all the investigation work, it was already too late, and we had to bandage the issue," Castano notes. "There's a whole phase where it's nothing but research and discovery of that one malware, and then you're hoping that it's just that single malware. The average investigation time was four hours."

The district's reactive security posture, which was already a concern, became glaringly evident when the Department of Homeland Security (DHS) came calling. The agency alerted the district that one of the machines on its network had been flagged for activity that was indicative of a potential ransomware attack. A student had accessed a business website to download a template for schoolwork, which contained a malicious executable.

OUHSD's security measures did not detect the activity, but the FBI's did. While the machine in question was quickly remediated without harm, the incident got the district's attention. "It was a really rude awakening," Castano says.

Customer: ***Oxnard Union High School District***
Industry: ***Education***
Location: ***Oxnard, California***

OBJECTIVES:

- Resolve the networking conflicts created by having multiple systems for DNS, DHCP and IPAM
- Reduce server sprawl and increase operational efficiency
- Decrease the manual effort required to manage the network and investigate threats

RESULTS:

- Consolidated DNS management into a single, simple-to-use solution
- Simplified critical network services management with a web interface that requires no training
- Reduced average threat investigation from 4 hours to 20 minutes

PRODUCTS:

- NIOS DDI
- BloxOne Threat Defense

THE SOLUTION

DNS Consolidation, Proactive Threat Detection, and Comprehensive Visibility

For Castano, the answer to the district's chronic networking woes was to consolidate all DNS and NTP responsibilities into the solution they already had, which could handle all their DDI needs—Infoblox NIOS. "Instead of this overcomplicated setup where we have records on certain Windows machines, records on Infoblox, and trying to synchronize between them, we decided to push all of it to the NIOS Grid," he recalls.

The migration involved moving key DDI functionality from Microsoft DNS and additional domain controllers to Infoblox. Castano credits Infoblox Professional Services for helping his team ensure that the migration ran smoothly and without disruption. "The support has been amazing. It's been really great transitioning over." Today, all of the district's DDI and NTP functions are managed through the NIOS Grid running on two virtual NIOS servers. In the wake of the ransomware incident, OUHSD sought a solution that would eliminate the blind spots that previously allowed threats to go undetected, while also enabling Castano and his team to be more proactive, finding and neutralizing threats early in the attack cycle before they could be activated. The district worked with Infoblox Professional Services to deploy BloxOne Threat Defense Advanced on a proof-of-value basis. The solution provides centralized visibility and control for every device connected to the district's network infrastructure, AI and machine-learning behavioral threat detection, and comprehensive event investigation and response features. From the moment the solution was up and running, it began spotting threats and anomalies that had eluded the district's existing malware and threat detection tools. "It was eye-opening. The number of unique detections was surprisingly high," Castano says. "There was a lot more going on that we were not seeing."

THE RESULT

Elevating Efficiency, Bolstering Security

By eliminating unnecessary hardware and consolidating DDI functionality with Infoblox, the district's networking infrastructure is far leaner and more efficient. Castano and his network technicians now have a single platform to manage networks at each of the district's schools. "Now that everything is centralized on NIOS," Castano says, "all of my networks are in one spot. I can easily access each network, view reserved IPs, fixed IPs, and leases."

Along with a simpler environment, NIOS provides Castano and his IT organization with unprecedented simplicity and ease of use, beginning with the web interface. "It requires zero training and it's very obvious what's going on. It makes things really easy to replicate whenever you need to add a new school or a new site. Everything just works flawlessly."

For Castano, safeguarding the district's users and data has also become much more efficient thanks to Infoblox. For example, the filtering capabilities of BloxOne Threat Defense automatically block students and faculty from accessing malicious domains, enabling OUHSD to avoid alarming events like the one that drew the attention of Homeland Security. The feature leverages Infoblox's massive store of DNS data and up-to-date threat intelligence, which flags security issues other solutions cannot see. As a result, Castano can easily block destinations associated with hacking, malware, NX domains, and dubious IP addresses with a high degree of accuracy, ensuring that legitimate traffic flows unimpeded. The proactive nature of Infoblox filtering gives Castano peace of mind. "With BloxOne Threat Defense, we feel much more confident in our ability to protect each user and device across the entire district from cyberattacks and prevent incidents before they happen."

Today, when security events happen, the comprehensive threat visibility Castano gains from Infoblox slashes his response time. "What would typically take me four hours now takes about 20 minutes." Critical device context is automatically collected from the IPAM solution and provided with security alerts. The Dossier feature in BloxOne Threat Defense automates many of the previously painstaking threat investigation steps to help analysts understand more about the threat, the actors behind it, WHOIS data behind the hosting site, and more. "It's tremendously helpful to have everything collected for me and presented in one place instead of having to manually hunt all this information down. It's a huge time-saver."

When it comes to cybersecurity or network management, time is everything. Thanks to Infoblox, Castano and his co-workers are able to save even more time with a single environment that makes it easy to navigate between networking and security tasks—a crucial benefit for small and medium-sized organizations like theirs where everyone is forced to wear multiple hats. For instance, when suspicious DNS activity arises on a machine in the network, Castano can quickly investigate the DNS history of the device for inappropriate behavior, suspicious web app use, or actual cyberthreat activity. The rich device data from NIOS automatically provides context around these events, including extensive user and device details. “Because I have everything in NIOS so neatly compartmentalized, I can quickly narrow an event down not only to the location but to the particular building at that location.” Once cyberthreat activity is pinpointed, the team can rely on the rapid capabilities of BloxOne Threat Defense to automatically isolate and remediate an impacted device.

Uniting networking and security with Infoblox not only helps OUHSD improve network performance and protection, it also gives Castano and his associates the freedom to innovate. “I’m not spending a huge chunk of my day just making sure that everything’s going well,” he observes. “Infoblox frees me up to plan for the future, and those time savings are really important because, without them, I would just be spinning my wheels, fixing day-to-day processes.”

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

+1.408.986.4000
www.infoblox.com

Version: 20241004v1