infoblox.

CUSTOMER STORY

San Francisco sharpens visibility into Network Operations to strengthen its Security Posture

OVERVIEW

San Francisco has a rich history of innovation, cultural progress, and notable events.

From the mid-19th century Gold Rush to the Summer of Love and the emergence of the tech industry in the digital age, San Francisco has long been regarded as a hub of business and technology innovation. However, that elevated global profile also makes the city and its IT infrastructure prime targets for hackers and malicious attacks. Nathan Sinclair, Cyber Defense Operations Manager for the City and County of San Francisco, knows this all too well. Fortunately, with the help of Infoblox, Sinclair and his team have been able to maintain an excellent record of uninterrupted uptime and service availability for the city's more than 17,000 employees, first responders and elected officials, as well as more than 800k citizens and millions of visitors who frequent city-maintained websites and online services every year.

THE CHALLENGE:

Protecting the San Francisco Brand and Maintaining Public Services

As with many municipalities in recent years, ransomware has been a core focus of the city's cybersecurity efforts. Yet unlike many other cities across the United States that experience outages from ransomware attacks and endure slow recoveries in restoring online services, San Francisco has been fortunate in avoiding the worst effects of cyberattacks. "With ransomware emerging as a significant security concern within our industry, it naturally drew the attention of our IT leadership," explained Sinclair. "Ultimately this organization-wide focus helped us to drive strategic initiatives to better combat these attacks."

Customer: *City and County of San Francisco*
Industry: *Government*
Location: *San Francisco, California*

INITIATIVES:

- Improve network visibility for enhanced defense against ransomware, phishing, and web spoofing attacks.
- Strengthen the team's ability to detect and counteract the impact of lookalike domains.
- Ensure uninterrupted network uptime for over 17,000 employees, first responders, elected officials, and residents in the city.

OUTCOMES:

- By automatically collecting log data from the city's DDI infrastructure, BloxOne Threat Defense delivers instant, comprehensive insights into inbound and outbound traffic flows, eliminating DNS blind spots for superior security.
- Continuous threat intelligence allows the team to immediately enforce new blocking rules, stopping attacks in their tracks and preventing potential damage.

Sinclair and the San Francisco team have also had to cope with relentless phishing and web spoofing attacks. On a weekly basis, they see dozens upon dozens of phishing attacks, some of which could be ransomware exploits, but more often are blunt attempts to get recipients to initiate the processing of fraudulent transactions. In a similar vein, attackers have repeatedly set up fraudulent websites closely mimicking the look and feel of genuine City of San Francisco web properties. The extensive online presence of the city's web properties, including multiple pages within the core SF.GOV domain and related sites, creates a significant attack surface, especially in terms of exposure to lookalike domain exploits.

"We've seen multiple instances where attackers set up lookalike websites to pretend that they are a city organization, either for collecting personal information or for paying traffic fines and similar," said Sinclair. "Some are amateurish and easy to spot, but many look remarkably real. We did have some security tools in place that could detect and block these types of activities, but not at the DNS layer. It was a blind spot that BloxOne Threat Defense enabled us to resolve and strengthen our security posture."

- BloxOne Threat Defense ensures adaptable security for remote workers and endpoints, providing peace of mind regardless of location.

SOLUTIONS:

- BloxOne Threat Defense

THE SOLUTION:

Expanding the City's Infoblox Implementation with BloxOne Threat Defense

San Francisco has been using Infoblox NIOS, running on Trinzic appliances, for many years to manage its core DNS, DHCP and IPAM (DDI) operations. However, despite being a long-time customer, Sinclair and his security team were not very familiar with Infoblox's security offerings. This was largely due to conventional IT best practices where networking teams are responsible for managing DDI infrastructure while security teams are responsible for managing security information and event management (SIEM) systems, as well as security orchestration, automation, and response (SOAR) systems. This organizational approach gives the security team only minimal visibility into what is happening on the network side. However, in the post-Covid world, where remote work and cloud/hybrid architectures have become mainstream, this division of duties was no longer sustainable. The need for closer collaboration between the networking and security teams became apparent.

"With the segregation of duties we had in place, my only real exposure to Infoblox was that we'd get nominal amounts of networking data from the NIOS instance to ingest into our SIEM/SOAR stack to check for suspect traffic," related Sinclair. "But then in consulting with one of our client organization departments, they'd recently adopted BloxOne Threat Defense and gave us a demo. Immediately we recognized that here was a solution that provide complete visibility into network vulnerabilities. It would be a powerful tool for blocking exploits, stopping incursions before they could do damage, and strengthening our defenses overall."

BloxOne Threat Defense operates at the DNS level to identify and uncover threats that other solutions cannot and stop attacks earlier in the threat lifecycle. Through pervasive automation, machine learning and ecosystem integration, BloxOne Threat Defense also drives efficiencies in SecOps to uplift the effectiveness of the existing security stack built on SIEM/SOAR capabilities. "We immediately realized that from a functional standpoint, BloxOne Threat Defense would boost our security capabilities on two fronts," said Sinclair. "First, because it integrates with NIOS, it's a tool that allows my team to do their job without ever needing to ask the networking team to give

us access to the actual appliances they manage. We see all that data, whether it's IP address management appliances or core DNS. And second, if the network team does want to forward rules to us for addressing emerging threats, for instance, we have a tool now that lets us carry out our own security processes. It's our tool, we own it."

RESULTS:

Better Visibility, Rule Enforcement and Protection for Remote Workers

Sinclair and the San Francisco security team see the BloxOne Threat Defense implementation bringing dramatic improvements to the city's cybersecurity in three main areas:

Overall Visibility – As mentioned above, BloxOne Threat Defense automatically collects all logging data from the city's DDI infrastructure. It then instantly renders that data into easily understood graphs, charts and hierarchies to paint a comprehensive picture of exactly what's flowing in and out of the network's DNS systems. Previously, DNS operations were a blind spot for Sinclair and team. This lack of visibility was a major security weakness as malicious hackers in recent years have focused more of their attacks at the DNS layer. As much as 80% of malware today uses DNS to initiate C2 procedures that can be used to steal data and spread malware (Unit 42 research). DNS tunneling and malware using domain generation algorithms have become widely embraced as well.

Enforcement of Blocking Rules — Prior to the deployment, enforcing new blocking rules to tighten security required Sinclair and the security team to work with multiple stakeholders across the organization to ensure uniform enforcement. Today, they can enforce new rules without having to ask another team. As Sinclair put it, "With BloxOne Threat Defense, we have threat intelligence from Infoblox and from partners continuously feeding into our security stack, which enables us to act on threats faster than ever before. That intelligence enables BloxOne Threat Defense to alert us to critical threats, so we know when we need to immediately block imminent threats. In the past, we weren't always able to get those things done in a timely fashion. This is a huge advancement for us."

Protections for Remote Workers — As for most organizations rocked by Covid, supporting remote workers was a huge challenge for the SF team. "In the beginning, we were scrambling because everything we had traditionally in our security stack was designed for protecting our workers in office buildings within San Francisco," said Sinclair. "But it also helped us accelerate a lot of projects. We got BloxOne Threat Defense in place in short order because we had to have it in place in order to protect our users. That protection is now in place wherever our users work—whether they're back in the office or still working from home."

Sinclair and team have experienced multiple improvements since implementing BloxOne Threat Defense. Enhanced network visibility, improved enforcement capabilities, and better protections for remote workers have all proven to be valuable benefits. However, the biggest game changer has been the peace of mind that BloxOne Threat Defense offers. The team now has more confidence in their ability to detect and stop critical threats earlier. "With BloxOne, we have much more complete context around and insight into our security data. Instead of us trying to figure out and correlate the data and understand something like, how are DNS requests going to this website? Before, it was a lot of work to do that. But not anymore. BloxOne took that guesswork out."

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

+1.408.986.4000
www.infoblox.com

Version: 20231120v1