infoblox

CASE STUDY

Public safety use case: North American communications service provider

Internet & communications technology industry

MEETING THE HIGHLY SPECIALIZED NEEDS OF PUBLIC SAFETY CUSTOMERS

For communications services providers, meeting the needs of public safety customers such as police, fire and public health agencies requires capabilities and service-level commitments that go above and beyond standard commercial offerings.

At the same time, public agencies—like any customers —have choices, and they select communications providers based on a range of factors. Pricing, is always a key consideration, but quality, reliability and security can all be as critical to decisionmakers who select which service provider to work with and are responsible for sending people into difficult situations.

THE CHALLENGE

Layered security for first responders

One communications services provider in particular established as a primary goal to help protect and support first responders by making their communications as easy, secure and fast as possible. Besides providing services built exclusively for public safety, the company—a long-established multi-national telecommunications carrier—also provides responder-specific 4G LTE services on a network that segregates public safety data traffic from customer traffic. The carrier wanted to offer proactive security capabilities on top of public safety network services to bring enhanced services to first responders. Specifically, the service would provide layered security to automatically protect end-user equipment with anti-virus capabilities, warning alerts when users visited potentially malicious sites and denial-of-service protections.

THE SITUATION

Safety first, but with flexibility for the modern first responder

Fast and reliable device connectivity is a must for public safety. Access to networks is necessary during an emergency, but protection for the network and endpoint devices is just as critical. The service provider already had existing public safety network customers but wanted to create a layered security offering on top of its public safety wireless offering with network-wide range and subscriber awareness.

Providing these organizations with enhanced security capabilities to protect a variety of first responder endpoint devices would favorably position the carrier against competing solutions and reduce customer churn. It needed a cost-effective and low-touch network service that also supported bring your own device (BYOD) and IoT via an easily attached, cost-effective, scalable agentless solution.

THE SOLUTION

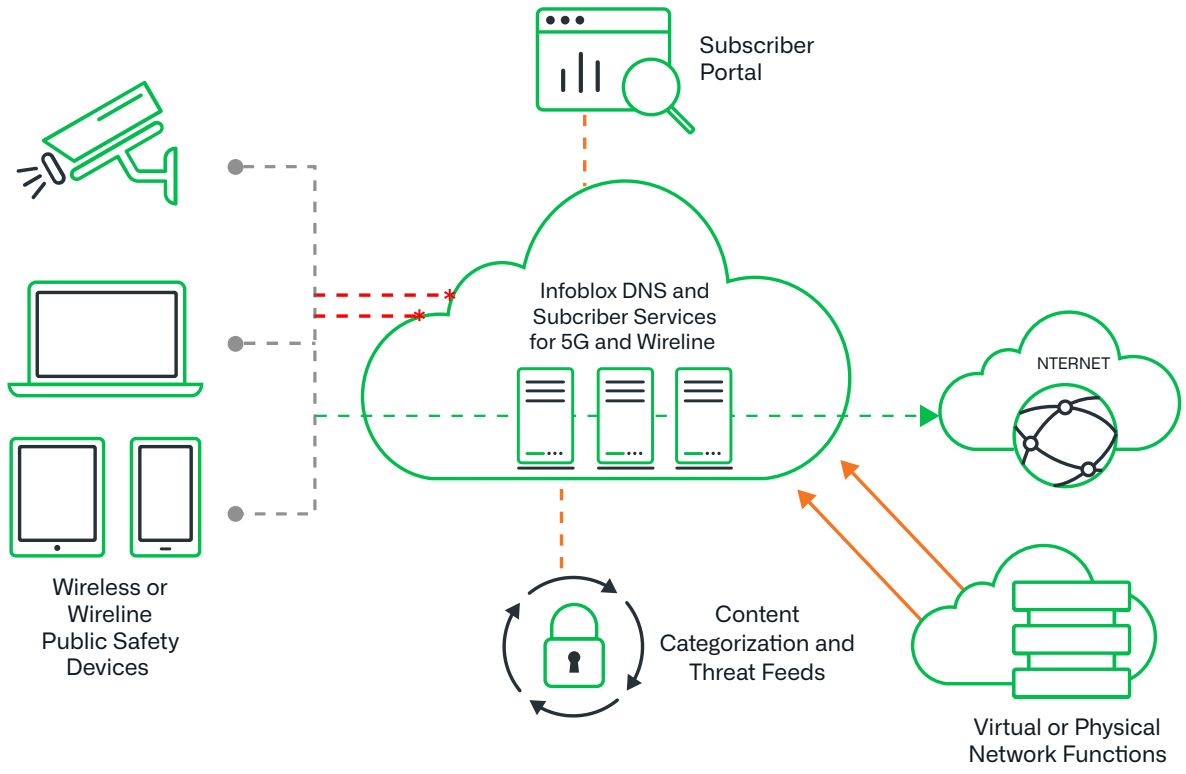
Building up from core Infoblox DNS solutions

The carrier, a long-standing Infoblox customer, leverages Infoblox DNS and DNS Cache Acceleration to power its 4G and 5G wireless networks. Working with the team at Infoblox, the company explored ways to use existing DNS capabilities to create new value-added services and execute its layered security offering. What started as a discussion with the carrier's wireless team turned into a collaboration among multiple groups within the organization, including product management, product marketing and network planning. Ultimately, these talks led to an understanding of how it could leverage existing core network infrastructure and additional Infoblox capabilities to power new value-generating services for its public safety network customer base.

The Infoblox solution combined several key capabilities to protect the first responder network and devices:

- Foundational for this carrier were Infoblox Trinzic Flex virtual appliances and Infoblox Grid™ activation licenses. These were explicitly purchased by the service provider for its public safety network to provide a flexible and scalable infrastructure to handle dynamic requirements. These acquisitions enabled the organization to leverage the Infoblox DNS queries per second (QPS) capacity on orchestrated virtualized network functions from existing Infoblox Trinzic Flex licenses. Now it could scale up as many DNS virtual machines as needed for its public safety core carrier Advanced DNS Protection (ADP) to guard the DNS services by automatically detecting and stopping the most extensive external/internal DNS-based attacks while maintaining DNS integrity and service availability. By application of ADP, attacks directed toward the DNS services to cripple or compromise network communications are thwarted.
- BloxOne® Threat Defense Premium Security provided a baseline threat intelligence capability to secure a wide range of first responder devices from smartphones to any IoT device needing a network connection. These devices are protected from malware, viruses, access to malicious sites and data exfiltration threats.
- BloxOne Threat Defense Advanced Security to leverage additional threats and enable specialized capabilities.
- Infoblox Reporting and Analytics combined and packaged valuable core network services information into actionable intelligence.
- Subscriber Policy Enforcement, part of the Subscriber Services portfolio, enabled subscriber awareness and allowed public safety entities to access security reports specific to their enterprise. Each entity can also control endpoint access, increase security and improve network performance by ensuring that first responder devices can only access unrestricted content.

Leveraging its lab and Trinzic Flex licenses, the carrier has the flexibility to test capabilities such as subscriber policy enforcement to clearly understand how far it wants to develop subscriber awareness. The carrier can also test and leverage Infoblox threat intelligence capabilities as an additional path to revenue, with the ability to upsell an extra layer of threat feeds that may appeal to specific agencies.



THE RESULT

Secure end-to-end DNS-based layered network security

The communications services provider is now on target to release a DNS-based layered security solution on top of its existing public safety wireless network that can be offered in numerous phases. The carrier can enable first responders with underlying endpoint security to report on blocked malicious attacks, define security policies and level of service, expand content filtering options and handle more granular reporting. Infoblox is an integral part of a suite of services whereby the company will supply secure end-to-end layered network services for public safety agencies.

Why Infoblox

Infoblox enables next-level network experiences with its unique, patented solutions. Infoblox Grid ensures network reliability by providing resilient network services, failover, recovery and seamless maintenance for Infoblox deployments within a single building, across a networked campus or between remote locations. Infoblox Advanced DNS Protection defends against the widest range of DNSbased attacks, such as floods, exploits and DNS hijacking. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity.

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

+1.408.986.4000
www.infoblox.com