SOLUTION NOTE

INFOBLOX FOR LAW ENFORCEMENT AND PUBLIC SAFETY

MODERNIZATION IN LAW ENFORCEMENT AND PUBLIC SAFETY

As data-intensive endeavors, law enforcement and public safety have rapidly moved to the forefront in embracing new technologies and driving modernization efforts. The pace of technology adoption has brought many new systems, software and IoT-based connectivity to patrol cars, attached to officers' uniforms and into precinct stations and facilities. The rapidly expanded use of Internet of Things (IoT) devices has contributed to increased cybersecurity risks and vulnerability. And expansion of data sharing has also raised the imperative for better and more efficient security solutions.

Infoblox solutions can help law enforcement and public safety organizations accelerate their deployment of modernized digital services while enhancing security, protecting services continuity, reducing costs, increasing operational efficiency and improving outcomes.

Cyberthreat Activity Escalates and Targets Law Enforcement

The Metropolitan Police Department of the District of Columbia was hit by a ransomware attack in 2021.[1] A threat actor group known as Babuk may be responsible for the attack. The Russian-speaking hacker gang specializes in ransomware. In this instance, the cyberthieves claimed to have over 250 gigabytes of confidential law enforcement data, including details about gangs, gang-related activity and police informants. There were reports that the ransomware group had initially compromised the police department's networks, exfiltrated the data and then finally encrypted the data on the police servers with ransomware. Babuk's intention was to force the D.C. PD to pay ransom to regain access to their highly confidential data and prevent it from being leaked to the public. In the case of law enforcement, the potential financial damage and impact on the criminal justice system of such an attack can be devastating.

The D.C. PD is not alone in facing such ransomware attacks. In 2021, we will have seen dozens of similar attacks on government agencies. The attack on the Metropolitan Police Department was immediately preceded by attacks on the police departments in Presque Isle, Maine, and Azusa, California (near Los Angeles). Threat actors have determined that due to the highly sensitive information protected by law enforcement, they have potentially high leverage in a successful attack, so we expect a trend to emerge and escalate.[2] Law enforcement organizations must protect their highly sensitive data and look for innovative ways to reduce risk and vulnerability—while using available resources and budgets.

New technology initiatives using various IoT devices and increased network connectivity have created much more risk and exposure for law enforcement infrastructure. Many of these technologies include digital voice, laptop and tablet computers, Internet connections, keyboards, video recording and archive equipment, automated chain of custody software tied directly to device data collection, special radio equipment and even the use of drones, which can be quickly activated and released from patrol car trunks. Officers are often equipped with uniform-mounted cameras and recording equipment, communications equipment and GPS tracking technology.

1 https://www.nytimes.com/2021/04/27/us/dc-police-hack.html

2 https://apnews.com/article/ransomware-gangs-hacking-police-cybercrime-pipeline-3a38c27c4fafe0c39461fb71bf91a42a

Police departments also deploy technologies at the community level, such as GPS, incident reporting, gunshot detection, license plate scanning, and surveillance cameras, among others. For all of their use in law enforcement, IoT technologies pose substantial risks when it comes to network security. That's because most IoT devices lack adequate security protection. They are also interconnected—to the cloud and to the Internet. The resulting attack surface is vast, creating significant potential for data breaches and damage to the public trust.

During the pandemic, while many people have been able to work from anywhere (WFA), many law enforcement officers have remained on the front line in the communities they serve.in communities. At the same time, however, administrative and other office workers have been working from home. This shift to remote work has increased vulnerabilities within law enforcement network infrastructure.

WFA users lack the same level of sophistication protecting them that they have within state and local government facilities with next-generation firewalls, intrusion detection, deception technology and machine-learning-based security controls. Remote work exposes a much broader attack surface because it uses home BYOD and mobile devices that share home and public Wi-Fi networks, often with a much larger variety of Internet of Things (IoT) devices than in the standard law enforcement workplace. Public Wi-Fi networks present a higher probability that authentication and credentials may be accidentally compromised.

Law enforcement support for necessary WFA continues to be re-engineered and modernized to meet new requirements more securely and at a lower cost.

LAW ENFORCEMENT PRIORITIES

Among the many issues that law enforcement faces, the following three are of special concern today:

- **Public trust and confidence:** Law enforcement and community stakeholders seek to promote open communications, transparency and partnership together.
- **Faster and better incident response:** Improved procedures, better-trained law enforcement teams and the use of digital technologies can enable a faster and safer response to incidents. Rapidresponse correlates to improved outcomes.
- **Community and citizen safety:** Safety of the community is of paramount importance as is the safety of law enforcement personnel.

LAW ENFORCEMENT TECHNOLOGY-BASED INITIATIVES

Law enforcement priorities, in turn, drive requirements for a multitude of IoT technology-based initiatives that require modernization and transformation for police work and public safety services. They include:

- **Modernized cyberdefenses to protect confidential data and maintain 24 x 7 operations:** Law enforcement is moving forward to modernize networks and improve its cyberdefenses in all areas. This initiative has two goals: to protect highly sensitive and confidential data and to maintain the high availability that law enforcement operations require.
- **Advanced software systems:** New software systems bring digital technologies that can help store, manage and share digital evidence. These digital technologies can also help properly maintain and preserve the chain of custody for critical evidence. Software systems can support real-time access to data by officers and integrate this within patrol cars.
- **Modernized video systems:** Next-generation video systems may be mounted on patrol cars, officers, drones, and remote-controlled robots. These are automated and integrated into software systems to provide an end-to-end transparent and comprehensive view of law enforcement and suspect activity.
- **Tablet-based computing platforms and displays:** Big clunky laptops and keyboards have started to be replaced by tablet computers with high-resolution displays. This change enhances interconnection with many information systems and accessibility for officers both within and outside of patrol cars. These devices can accompany officers, as required, to address almost any situation in real time.
- **AI and facial recognition systems:** A new generation of AI systems is enabling police officers to rapidly identify suspects, especially those who might represent a high threat to the community and the officers themselves.

- **Drones and other robotic systems:** Already important law enforcement tools within larger cities, drones and robotics are rapidly working their way into the smallest municipalities. Bomb disposal robots and off-the-shelf drones are in wide use. These digital devices need integration into chain of custody management so they are tightly integrated into critical law enforcement networks.
- **License plate readers:** Patrol cars are using license-plate reading and recognition technology to accelerate the time to identify stolen vehicles and other potentially dangerous situations.
- **Facility infrastructure management:** Advanced systems, software and smart IoT devices can automatically control police facility HVAC, security and other building systems.

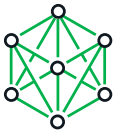
INFOBLOX FOR LAW ENFORCEMENT AND PUBLIC SAFETY

Infoblox Benefits

Infoblox can help meet your modernization requirements for secure, resilient and flexible network core services and DNS security—including reaching 100 percent business continuity, preventing unplanned expenses related to breaches and protecting the public trust.

Our solutions help IT and SOC teams maintain important compliance over people, devices and the systems they use, improving operational efficiencies and driving deeper interdepartmental visibility and data integrity.

Infoblox Technology Solutions



DDI (DNS, DHCP & IPAM)
Deliver business-critical network services

Network Service & Protocol Delivery (DDI)
- Core Network Services
- Application Load Balancing (DTC)
- Reporting
- Configuration Management
- DoT/DoH

Security
Protect the organization in new threat landscape

Foundational Security Everywhere
- Visibility and discovery
- Detect and block malware, data exfiltration
- Threat Intelligence Optimization
- Security Automation and Orchestration, SOC efficiencies

Infoblox is the industry-leading provider of DNS, DHCP and IPAM (DDI) services, meeting the needs of any enterprise architecture, with appliance-based or SaaS-delivered solutions built for performance, scalability, security and reliability.

BloxOne® Threat Defense is Infoblox's hybrid security offering that strengthens and optimizes your security posture from the foundation up, using DNS as the first line of defense. It detects and blocks malware C&C and data exfiltration, and it leverages the data within DDI to enhance your entire cybersecurity ecosystem. BloxOne Threat Defense protects IoT devices and helps secure on-premises, cloud and hybrid environments and the WFA users who access them.

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

+1.408.986.4000
www.infoblox.com

Version: 20231030v1