SOLUTION NOTE

UNIFIED NETWORKING AND SECURITY FOR PUBLIC TRANSPORTATION

MODERNIZATION IN PUBLIC TRANSPORTATION

Public transportation helps ensure that people can reach jobs, schools, healthy food outlets and healthcare facilities, safely and reliably. Public transportation services play an important role for people who are unable to drive those without access to personal vehicles. This can include children, individuals with disabilities, and older adults.

Public transportation has accelerated the pace of embracing new technologies and driving modernization efforts to better serve the public. Public transportation can include a wide variety of services and transportation modalities for their communities. Transport offered in the community may include intercity light rail (trams), high-speed rail, regional rail, subways, urban rail transit, cable car, city buses, trolley buses, school buses, aerial tramways, maritime transport, special taxi service, and more. All of these modalities will be positively impacted by modernization.

The pace of technology adoption has brought many new systems, software and IoT-based connectivity to public transportation infrastructure. The rapidly expanded use of Internet of Things (IoT) devices has contributed to increased cybersecurity risks and vulnerability. Data sharing has also raised the imperative for better and more efficient security solutions.

Infoblox solutions can help public transportation 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 PUBLIC TRANSPORTATION

Public transportation has been in the cyberattacker's bullseye for quite awhile. As an example, railroads have increasingly been targeted by cyber attackers, both from organized crime and nation-states, as they are part of critical national infrastructure. The importance of rail transportation to the U.S, Japan, the United Kingdom, and Europe economy, the potential for massive disruption and damage to both freight and passenger traffic, and the vulnerability of the entire system are all making the railroads a target of choice for cyberattack and nation-states.

In 2016, an attack was experienced by San Francisco's light rail system. The attackers opened all station gates across the network, froze ticketing machines, and shut them down. The supervisory ticketing systems in the station agent's offices also crashed. This attack brought most San Francisco light rail line operations down for over two days.

> *"We believe that DNS security is critical to providing a strong return on investment we see with [our rail] program. Foundational security will better secure our networks and the 100,000+ IoT and process control components it contains. It makes intuitive sense to block threats up front, early in the potential attack cycle. Infoblox provided strong value with a clear well-positioned proposal for the success of our mission."*
>
> **Major Rail Transit System Security Operations Center Team Lead**
> **Using Infoblox DDI and BloxOne Threat Defense**

Similarly, the German national rail network was targeted and hit with an attack on its critical infrastructure in 2017. The WannaCry virus impacted 450+ Deutsche Bahn computers, controlled security and CCTV networks, ticketing machines, and passenger information systems. Worse yet, this attack was subsequently used against the national railway systems in both China and Russia. Protecting public transportation rail networks from attackers like this is vital.

New technology initiatives using various IoT devices and increased network connectivity have created much more risk and exposure for public transportation infrastructure. Many of the 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 public transportation employees 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 the public transportation 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 public transportation workplace. Public Wi-Fi networks present a higher probability that authentication and credentials may be accidentally compromised.

PUBLIC TRANSPORTATION PRIORITIES

Among the many issues that public transportation faces, the following seven are of special concern today:

- **Capacity expansion:** Many public transportation systems are projecting the need for substantial growth over the coming years. This must be done reliably and securely.
- **Intelligent automation:** Intelligent automation backed by digital technologies will increase efficiency, track delays in real-time, and help make safe and fast decisions about managing these situations.
- **Community and citizen safety:** Safety of the community is of paramount importance as is the safety of public transportation personnel.
- **Cybersecurity risk:** Cybersecurity risk has moved to center stage. To guard against cyberthreats and unauthorized access to data centers and other computerized systems, you need a secure DNS infrastructure for secure government operations.
- **Physical risk:** Physical risk to public transportation infrastructure from terrorism has been on center stage and needs to scale to greater levels of detection, protection and resilience.
- **Energy efficiency program:** Local governments are collaborating with utilities, state or regional energy efficiency programs to design efficiency programs for public transportation, and to improve the efficiency of their own facilities.
- **Work from anywhere (WFA):** The pandemic has created a need for a secure WFA environment for office and administrative workers seeking access to public transportation resources from a variety of endpoints, both work and personal, as well as mobile devices. This access requires high availability, safety, security and resilience.

PUBLIC TRANSPORTATION TECHNOLOGY-BASED INITIATIVES

Public transportation priorities, in turn, drive requirements for a multitude of technology-based initiatives, many of which require IoT, that require modernization and transformation. They include:

- **The digital railway:** To meet these increasing needs for capacity, reliability, and security, many public rail systems have started an initiative for what may be described as the digital railway. The digital railway can deliver substantial improvements in reliability and other areas at lower cost by modernizing train command, control, and signaling systems designed in the pre-digital age. The digital railway will also include digital signaling and more sophisticated and secure train controls. In most municipalities, this network will be heavily IP-based. Some public transportation systems must manage many tens of thousands of IP addresses and the control systems that use them. In some cases the digital railway initiatives have required the safe management of over 100,000 IP addresses.
- **Modernized cyberdefenses to protect confidential data and maintain 24 x 7 operations:** Public transportation 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 public transportation operations require.
- **Modernized video systems:** Next-generation video systems may be mounted on public transport buses, trains, stations and control facilities. These are automated and integrated into software systems to provide an end-to-end transparent and comprehensive view of public transportation assets and passengers.
- **Drones and other robotic systems:** Drones and robotics are more frequently being used in support of expanded security initiatives and for the inspection of train lines.
- **Tablet-based computing platforms and displays:** Big clunky laptops and keyboards are being replaced by tablet computers with high-resolution displays. This change enhances interconnection with many information systems and accessibility for public transportation workers.
- **Facility infrastructure management:** Advanced systems, software and smart IoT devices can automatically control public transportation facility HVAC, security and other building systems.

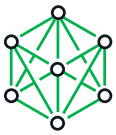
INFOBLOX FOR PUBLIC TRANSPORTATION

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.

infoblox.

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

Version: 20231030v1