SOLUTION NOTE

MODERNIZING MUNICIPAL UTILITIES WITH UNIFIED NETWORKING AND SECURITY

MODERNIZATION IN MUNICIPAL UTILITIES

Municipal utilities 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 deployed within facilities, vehicles, and personnel.

The rapidly expanded use of Internet of Things (IoT) devices has contributed to increased cybersecurity risks and vulnerability. The digital transformation to modernize equipment and also provides malicious attackers with new targets within a broader attack surface. Data sharing has also raised the imperative for better and more efficient security solutions.

Infoblox solutions can help Municipal utilities 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 MUNICIPAL UTILITIES

Recent research[1] noted that 44 percent of global ransomware attacks in 2020 targeted municipalities. The numbers in 2019 were almost identical, at 45 percent. 15 percent of the municipalities that were subject to ransomware attacks in 2020 have actually paid the ransom.

According to a recent industry survey[2] of 1700 municipal utility professionals 56 percent of utilities have faced a cyberattack in the last year. Those events included at least one shutdown or operational data loss. Of the survey respondents, only 42 percent rated their cyber readiness as high. 64 percent said that sophisticated attacks are a top challenge and 54 percent said they expect an attack on critical infrastructure in the next 12 months.

Municipal utilities provide cyberattackers with high value targets such that the extortion of ransom is potentially most lucrative. Municipal utilities also present a relatively undefended target of opportunity. Cyberattacker access is relatively easy, there is a wide variety of opportunities across states, counties, and local governments. Finally, the careless growth of IoT to support this ongoing digital transformation has dramatically expanded the attack surface and increased the number of exploitable vulnerabilities.

> *"New cybersecurity challenges related to the use of the Internet of Things (IoT) devices in the construction of new services are also worth emphasizing. The significance of these new challenges was also emphasized by the report of the internal working group … that IoT without cybersecurity poses a greater threat … than giving up the use of IoT."*
>
> Member of the Executive Board of an Energy Utility
> **Using Infoblox DDI and BloxOne Threat Defense**

1 https://www.infosecurity-magazine.com/news/local-government-targeted/

2 Report by Siemens and the Ponemon Institute

Many critical infrastructure municipal utility facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation. In order to develop more resilience and reduce risk, the implementation of cybersecurity best practices is critical for municipal utilities.

The cyberattacks targeted against municipal utilities come from a diverse variety of sources. Utility systems and servers are frequently impacted by denial of service and distributed denial of service (DoS/DDoS) attacks. A wide variety of malware may be used including ransomware, trojans, and backdoors. Municipal utilities are also frequently subjected to targeted phishing email campaigns.

As an example of the current threat environment, one potentially dangerous attack on a municipal water facility happened earlier in 2021. Cyber attackers were reported to have targeted and accessed the information technology system responsible for controlling a water treatment facility located in the southeastern United States.

In this attack, the attackers choose to upset treatment and conveyance processes around the dosage of sodium hydroxide by opening and closing valves. Attacks like these can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence, and result in financial and legal liability.

New technology initiatives using various IoT devices and increased network connectivity have created much more risk and exposure for municipal utility 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 municipal utility workers have remained on the front line in the communities they serve. At the same time, however, administrative and other office workers have needed to work from home. This shift to remote work has increased vulnerabilities - many of the operational technology controls are accessible using remote access. Remote work exposes a much broader and more vulnerable attack surface because it uses home BYOD and mobile devices that share insecure networks, often with a much larger variety of Internet of Things (IoT) devices than in the standard municipal workplace. Public Wi-Fi and home networks present a higher probability that authentication and credentials may be accidentally compromised.

MUNICIPAL UTILITIES PRIORITIES

The municipal utilities sector is changing rapidly. Growing demand for renewable energy and clean sustainability is merging with priorities for smart cities, electric mobility, and one technology. Among the many issues that municipal utilities face, the following six are of special concern today:

- **Renewable energy:** Renewal energy will become much more important across state and local governments as legislation moves to emphasize green energy sources and address global warming.
- **Energy efficiency programs:** Local governments are collaborating with utilities, state or regional energy efficiency programs to design efficiency programs for homes and businesses, and to improve the efficiency of their own facilities.
- **Intelligent automation:** Intelligent automation backed by digital technologies will increase efficiency.
- **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.
- **Work from anywhere** (**WFA**)**:** The pandemic has created a need for a secure WFA environment for office and administrative workers seeking access to municipal resources from a variety of endpoints, both work and personal, as well as mobile devices. This access requires high availability, safety, security and resilience.
- **Physical risk:** Physical risk has been on center stage and needs to scale to greater levels of protection and resilience.

MUNICIPAL UTILITIES TECHNOLOGY-BASED INITIATIVES

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

- **Smart home and smart meters:** New software systems bring digital technologies that can help store, manage and share digital data on energy consumption. Software systems can support real-time access to data. This will enable customers to monitor real-time energy consumption and potentially manage energy costs by switching systems between home devices.
- **Facility process control monitoring and management:** Advanced systems, software and smart IoT devices can automatically control the municipal utilities operational technologies processes.
- **Facility infrastructure management:** Advanced systems, software and smart IoT devices can automatically control the municipal utilities' facility HVAC, security and other building systems.
- **Modernized video systems:** Next-generation video systems are automated and integrated into software systems to provide an end-to-end transparent and comprehensive view of physical security and plant activity.
- **Modernized cyberdefenses to protect confidential data and maintain 24 x 7 operations:** Municipal utilities are moving forward to modernize networks and improve cyberdefenses in all areas. This initiative has two goals: to protect highly sensitive and confidential data and to maintain the high availability that municipal operations require.
- **Online payments and self-service kiosks:** Most consumer transactions with municipal utilities are being moved to online and self-service systems.
- **Tablet-based computing platforms and displays:** Municipal utilities are rolling out applications that run on tablet computers and mobile devices with high-resolution displays. This change enhances interconnection with many information systems and accessibility for municipal utility workers. These devices can enable municipal workers, as required, to address almost any situation in real time.
- **Drones and other robotic systems:** A new tool just emerging into use that enhances physical security in managing large plants and also assists with inspection and assessment of operations.

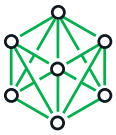
INFOBLOX FOR MUNICIPAL UTILITIES

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