SOLUTION NOTE

MODERNIZING NETWORKING AND SECURITY FOR PUBLIC HEALTH AND HUMAN SERVICES

THE DIGITAL TRANSFORMATION IN PUBLIC HEALTH AND HUMAN SERVICES

Public health services are at the forefront of embracing digital technology. Public health has accelerated the pace of technology adoption to address HIPAA compliance, cybersecurity, and the rapid growth of IoT-based medical devices, which has contributed to cybersecurity vulnerability. Finally, SD-WAN deployment and expanded information sharing have also raised the imperative for better and more efficient security solutions.

Infoblox solutions can help your public health service organization accelerate its deployment of digital services while enhancing security, protecting services continuity, reducing costs, increasing operational efficiency and improving patient outcomes.

CYBERTHREAT ACTIVITY ESCALATES

Public health has been hit by ransomware over the past two years, even within the federal government. In March of 2021, cyberattackers overloaded the U.S. Department of Health and Human Services with millions of hits. Such denial-of-service (DDoS) attacks can shut down all operations. DDoS attacks and ransomware both have caused major disruption to public health institutions over the past year.

New technology initiatives using various Internet of Things (IoT) devices have created much more risk and exposure for public health IT infrastructure. Most IoT devices installed within state and local governments today are poorly protected, if at all, creating significant potential for data breaches and damage to the public trust.

Work from anywhere (WFA) environments continue to bring an increased risk for public health services infrastructure. WFA will continue, perhaps long after the pandemic, for non-essential functions. Organizations and technology supporting WFA continue to be re-engineered to meet new requirements more securely and at a lower cost.

> *"This children's hospital is one of the top hospitals in the United States heavily dedicated to children's care. It selected BloxOne Threat Defense to leverage capabilities for expanded protection on-premise, within the cloud, and across networks utilizing SD-WAN and IoT. IoT protection is critical as this children's hospital continues to add many IoT connected medical devices to its internal networks. Infoblox technology has also positioned this children's hospital to utilize the benefits of hybrid security to support many future initiatives, both on-premise and in a variety of cloud architectures."*

Children's Hospital Healthcare Provider, U.S.

PUBLIC HEALTH AND HUMAN SERVICES PRIORITIES

- **Vaccine distribution:** New secure, trackable and auditable applications and processes in support of vaccine distribution are essential to counter the pandemic.
- **COVID-19 testing:** COVID-19 testing, government-based and in close coordination with private industry partners, is also essential to fight the pandemic.
- **Contact tracing:** New secure applications and processes to support contract tracing are also important.
- **Patient communications:** Such communications must meet the needs of compliance and provide rapid and reliable access to public healthcare.
- **Cybersecurity for standard and non-standard medical devices:** You need to protect Internet-connected medical devices from cyberthreats. Because many medical devices communicate via IoT, visibility into these devices, and additional security are necessary for expanded public programs. A secure DNS infrastructure is critical for resilient public health operations.
- **Telehealth and virtual care from anywhere:** The public demand for telehealth and virtual care has grown as the pandemic limited face-to-face provider/patient interaction for most routine care. Healthcare workers are also seeking access to enterprise resources from a variety of endpoints, both work and personal, as well as mobile devices. This access needs to be safe, secure and resilient.
- **Compliance with HIPAA:** Governance and compliance remain important issues; public health organizations must fully comply with the data privacy and security mandated by HIPAA regulations.

PUBLIC HEALTH AND HUMAN SERVICES TECHNOLOGY-BASED INITIATIVES

Public sector priorities, in turn, drive requirements for technology-based initiatives that require modernization and transformation for public health and human services; they include:

- **Enhanced patient outcomes:** New digital healthcare technologies can improve patient outcomes, which include maintaining patient safety, satisfaction, quality of life, attainment of functionality and ultimately recovery.
- **Better patient monitoring:** Monitoring patients, within facilities and remotely, relies on a variety of digital technology to improve the quality and speed of care.
- **Modernization to support medical devices**: New medical devices are often IoT-based and require modern network services and foundational security to protect them.
- **Lowered costs of delivered services**: The use of new technologies across healthcare can support cost effectiveness.
- **Facility security improvement**: Equipment and data within public healthcare facilities can be better protected with new security technologies, which often rely on networks and IoT devices.
- **Facility infrastructure management**: Advanced systems, software and smart IoT devices can automatically control public facility HVAC, security and other building systems.

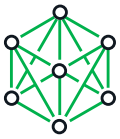
INFOBLOX FOR PUBLIC HEALTH AND HUMAN SERVICES

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: 20231031v1