Infoblox

SOLUTION NOTE

Education

The Digital Transformation in Education

As someone who works in education, you know it has moved rapidly to deploy digital solutions for remote and distance learning in response to the pandemic. Remote learning continues to be part of hybrid learning models that schools are adopting. Schools need better solutions to manage the wide variety of untrusted and personal platforms in use. They also need to improve students' access to safe content and the security of traffic and protect the integrity of institutional data.

Infoblox solutions help education organizations modernize their deployment of digital services while increasing security, protecting continuity of services, reducing costs, enhancing operational efficiency and improving student safety and educational achievement.

Cyberthreat Activity Escalates

Over the past two years, threat actors have increasingly used ransomware to attack educational institutions, and this trend continues. In March of 2021, the Broward County Public Schools were hit with hackers demanding $40 million from the district. In the same month, the University of California announced that a ransomware group may have stolen the personal information of students and staff members. This threat group has also been sending threatening emails across the student population.

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

> *"All public schools in their jurisdiction needed to be connected to the Internet through a centralized connection. It became the ISP for 100+ of public schools and thousands of students. BloxOne® Threat Defense Advanced provided protection against malware mitigation, web content filtering, and data theft over DNS prevention. BloxOne Threat Defense Advanced protected thousands of staff members, teachers, and students whether they are on-premises, or remotely accessing the school resources from home."*
>
> Department of Education

Data supporting the incremental risk of remote learning environments is circulating from a growing variety of sources. For example, the ed-tech advocacy group the Consortium for School Networking (CoSN), creates and publishes surveys on cyber technology issues. According to Keith Krueger, CEO of CoSN, cybercriminals are using phishing scams to target remote students and educators, which often appear to come from recognizable email addresses at first glance. “In a school environment, about 3 percent of teachers click inappropriately on phishing scams,” Krueger said. “That was jumping to 15 to 20 percent from home, so a lot of cybercriminals are getting into the network.”[1]

Remote learning environments necessitated by the pandemic continue to bring increased risks for educational institutions, students and faculty. Your challenges include ensuring that schools and the technology supporting remote learning continue to be re-engineered to meet new requirements more securely and at a lower cost.

Education Priorities

- **Remote learning:** Remote learning educators seek access to school resources from a variety of endpoints, both work and personal, as well as mobile devices. This access requires safety, security and resiliency.
- **Cybersecurity for bring your own device (BYOD) and IoT:** To guard against unauthorized access to data centers and other computerized systems, you need a secure DNS infrastructure for resilient education operations.
- **Student safety:** Improved safety for students is essential—both physically, within educational institutions, and when online, with a safe browsing experience.
- **Bandwidth and connectivity:** Educational traffic requirements for bandwidth grow each year. As schools begin to face an IPv4 address shortage, they require additional Internet addresses.

Education Technology-Based Initiatives

Public (and private) school priorities, in turn, drive requirements for technology-based initiatives that require modernization and transformation. These initiatives for education include:

- **New e-learning devices to improve education outcomes:** Enhanced educational outcomes are supported by new e-learning devices, often networked and IoT based, that include tablets and scanners.
- **Secure video conferencing for remote learning:** Schools must deliver the full suite of video conferencing safely and securely to their students. Faculty and staff also need access to video conferencing facilities from anywhere to support students.
- **Student website filtering and monitoring:** Over 50 percent of malicious website traffic and dangerous URLs can be filtered out by new technology sets such as DNS security. Core network services (DDI) also provide the visibility necessary to better protect the student population.
- **School facility infrastructure management and efficiency:** To improve the operations and energy efficiency of school buildings, IoT devices can control smart card access, monitoring of study hall, security cameras, connected lighting, RFID on school devices and much more.

[1] https://www.governing.com/security/cyber-attacks-on-schools-in-2020-were-record-breaking-report.html

Infoblox for Education

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 is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

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

+1.408.986.4000 | info@infoblox.com | www.infoblox.com