SOLUTION NOTE

SECURING WORK FROM ANYWHERE FOR THE PUBLIC SECTOR

SECURING REMOTE STATE AND LOCAL GOVERNMENT WORKERS

If you work in state or local government, you have faced unprecedented challenges since March 2020 due to the coronavirus pandemic. Many government agencies quickly reconfigured systems and policies to enable work from anywhere (WFA) environments for employees, a solution not without problems.

Remote workers continue to seek access to enterprise resources from a variety of endpoints, both work and personal, as well as mobile devices. But many of the cybersecurity procedures used within enterprise facilities won't work from remote locations without substantial changes, preparation and planning.

WORK FROM ANYWHERE BRINGS NEW SECURITY CHALLENGES

Today, your public sector security solutions primarily involve protecting data, devices, resources and users within office environments, and they are not optimized to provide the same protections for remote workers. Given recent government-mandated in-home quarantines and the uncertain nature of when employees will return to offices, government organizations clearly require a consistent security architecture that is designed, deployed, managed and applied the same way across all environments.

Most government applications are in the cloud, and you and other government workers no longer need to use VPN to access corporate applications and email. But you still access and store government data on your devices, which means you need to secure your Internet activity. Work from anywhere also changes the setting for teams, and this change to their behavior can cause problems, including communication difficulties, lower productivity and exposure to many new security risks.

Remote work also 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 workplace. Public Wi-Fi networks present a higher probability that authentication and credentials may be accidentally compromised.

Data supporting the incremental risk of WFA 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]

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.

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

PROTECTING WFA WITH BLOXONE® THREAT DEFENSE

BloxOne Threat Defense is an Infoblox security solution that uniquely solves several difficult problems for all state and local governments, including the challenge of a large remote workforce. It provides a highly cost-effective and integrated solution to protect users, applications and data using DNS as the first line of defense.

BloxOne Threat Defense protects public sector users, devices and systems no matter where they are, strengthening and optimizing your security posture from the foundation up. It detects and blocks phishing, exploits, ransomware and other modern malware, and it prevents your teleworkers from accessing objectionable content restricted by policy.

Using DNS as an essential control point ensures that every Internet request is inspected to determine if it is malicious, as identified by our integrated threat intelligence, analytics and machine learning. DNS also gives you scalable web and content filtering and reduces your overall threat defense costs.

By deploying BloxOne Threat Defense, and leveraging cloud capabilities, the public sector can easily extend the benefits of this protection to all users globally without having to rely on VPNs or other traffic steering techniques. BloxOne Threat Defense sends only DNS queries for inspection, meaning client traffic goes directly to the application without any additional latency. Malicious destinations identified by threat intelligence in the BloxOne Threat Defense cloud are immediately blocked, negating the need for processing by other security software.

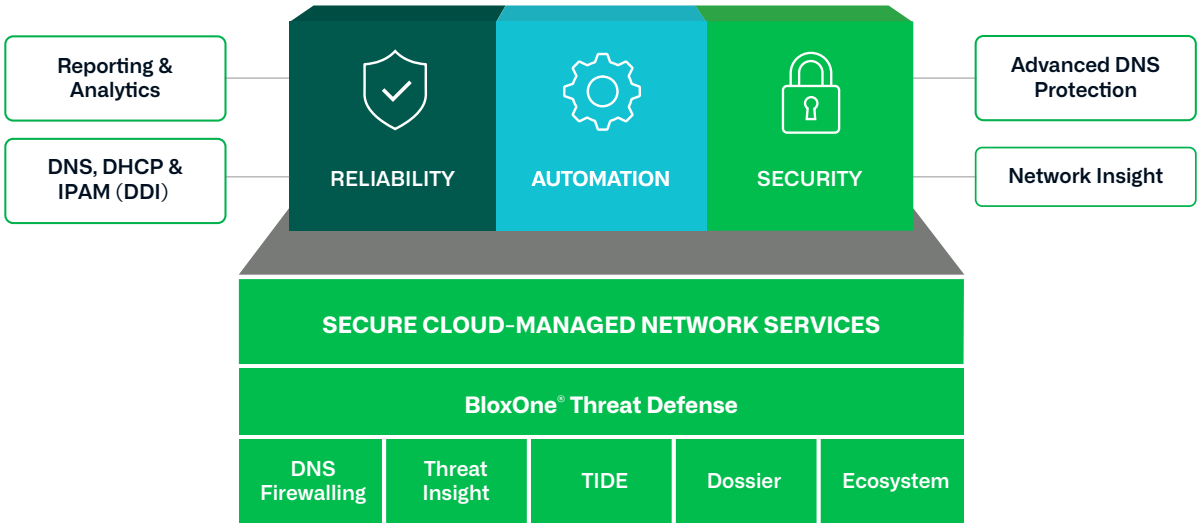

Figure 1: An overview of BloxOne® Threat Defense and key foundational security components

Other BloxOne Threat Defense capabilities include:

- **Broad support for API-based integration:** Built-in APIs enable you to share event data across your internal security ecosystem.
- **AI/ML-based analytics:** AI/ML-based analytics on DNS data is used to detect threats that cannot be otherwise detected. These include lookalike domains, zero-day DNS tunneling, domain generation algorithms (DGAs) and fast flux.
- **Lookalike domain defense:** Phishing websites often feature domains that impersonate the real brand. These are crafted to resemble the legitimate brand's domain. Character substitution is a popular technique employed by cybercriminals. BloxOne Threat Defense Custom Lookalike Domain Monitoring enables the public sector to proactively stop lookalike socially engineered attacks.

- **Domain generation algorithms:** DGAs are used to methodically generate domain names, which are then used to facilitate communications with cybercriminals' command-and-control servers. Cybercriminals also embed DGAs directly within malware to generate the list of domains they can use for command and control. BloxOne Threat Defense Threat Insight uses behavior analytics combined with machine learning to perform real-time analysis of incoming DNS queries, including entropy, n-gram, lexical, size and frequency analysis to detect DNS tunnels. Threat Insight also reduces false positives by detecting benign use of DNS tunnels.
- **DNS tunneling:** Two methods detect DNS tunneling—using threat intelligence to find known tunnels (for example, known malicious IPs and known bad domains) or using behavior-based analytics to detect known or previously unknown methods of DNS tunneling. The Infoblox solution uses both methods and our patented detection algorithms to uncover previously unknown attacks. Other solutions rarely use more than a threat intelligence method, limiting their ability to catch new attacks and protect WFA workers.
- **Content filtering:** When you need to protect a large remote workforce, scale and cost-effectiveness become vital considerations. When your employees are working from home or other off-premises locations, ensuring that the content they are accessing from corporate devices remains compliant with public sector policies is critical. The challenge with such large implementations is that it could require dozens to hundreds of secure web gateways to filter content, increasing costs and latency if all traffic must be funneled through these systems. BloxOne Threat Defense allows you to filter content at the DNS level, ensuring that connections do not happen to any website out of compliance with government policy.
- **DNS over HTTPS (DoH):** DOH is a new feature increasingly being supported by major Internet browsers like Firefox. Unfortunately, DoH does this by contravening enterprise security best practices and enabling encrypted DNS traffic. By enabling DoH, devices send all of their DNS traffic to an external third-party DNS resolver, bypassing internal enterprise DNS infrastructure and any DNS security controls in place. BloxOne Threat Defense and Infoblox threat intelligence services include a special feed called "DoH Public IPs and Hostnames" to help detect attempts to access unmanaged DoH resolvers and block them, forcing browsers to failover back to the organization's managed DNS without interrupting user activity. This feature ensures that an employee working from home, or any remote location, who may be on Firefox or other applications that default to DoH resolvers will still be protected against data exfiltration and malware communications.

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

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc.
All other marks are the property of their respective owner(s).

Version: 20231031v1