

WHITE PAPER

Securing Remote Workers in the Age of Teleworking

Using Foundational Network Infrastructure



Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.

Contents

Executive Summary.....	4
The Security Challenges of Teleworking.....	5
Targeted Threat Intelligence	5
Protecting Teleworkers with BloxOne™ Threat Defense.....	6
Important Technical Considerations.....	7
Lookalike Domains	8
Domain Generation Algorithms.....	9
Fast Flux.....	9
DNS Tunneling.....	9
Content Filtering	10
DoH.....	10
Hybrid Architecture	11
Recommendations.....	12

“Most disturbing, in the midst of this health crisis, the situation is further aggravated by a growing number of scams and malware threats specifically targeted to COVID-19. COVID-19 related phishing attacks and websites are increasingly being used as the attack vectors of choice for cyberthieves to leverage the situation to their benefit. Threat intelligence research has shown definitively that malware-laden email is one of the most used vectors for launching these attacks.”

Anthony James, Vice President of Product Marketing, Infoblox, Inc.

Executive Summary

Commercial and government enterprises are facing unprecedented challenges due to the coronavirus pandemic. Many private enterprises and government agencies quickly started preparations to enable teleworking for employees.

In a recent survey, approximately 44 percent of consumers with full-time employment have already felt the impact of coronavirus on their business operations, approximately 55 percent have already canceled travel plans, and about 40 percent are reducing face-to-face meetings and increasing the use of video conference tools.¹

Remote workers are seeking access to enterprise resources from a variety of endpoints, both work-provided and personal, as well as various mobile devices. The challenge, of course, is that many of the cybersecurity procedures used within enterprise facilities won't work from remote locations without substantial changes, preparation and planning. Unfortunately, due to the abrupt nature of this pandemic, organizations have had very little time to prepare and plan their cybersecurity measures to support a large-scale remote workforce.

As organizations work to support their growing remote workforces, it is important to consider the risks in consumer Wi-Fi connections, document shares on cloud folders and home browsers configured with plug-ins and applications that may introduce substantial risk. Home routers are usually not secure and not patched to the level suggested by their manufacturers. Workers at home tend to view personal email and other non-business websites more often than they do at the office. Such viewings only increase the probability that they will run into “malvertisements” (malware-laden advertisements) that could compromise a worker's device and eventually the enterprise. Further, attackers are leveraging the widespread thirst for information about the severity of the situation. Workers can easily fall victim to malware-laden links in online forums, social media and small publications whose websites have been compromised. These challenges will remain a constant threat, especially to remote users.

This white paper will address these challenges and share solutions on how to quickly ramp-up security using foundational network services to meet the needs of your enterprise and the rapidly growing remote workforce.

1. Forbes.com. Remote Work Advocates Warn Companies About COVID-19 Work-From-Home Strategies. March 5, 2020. <https://www.forbes.com/sites/laurelfarrer/2020/03/05/ironically-remote-work-advocates-warn-companies-about-covid-19-work-from-home-strategies/#744aaae22051>

The Security Challenges of Teleworking

Recent health risks with coronavirus have driven organizations into supporting remote work environments without adequate analysis and consideration of the cyberthreats in teleworking environments. Today's enterprise security solutions are primarily designed around protecting data, devices, resources and users within office environments, and they are not optimized to provide the same protections for remote workers. Given the reality of government-mandated in-home quarantines, it's become clear that organizations today require a consistent security architecture that is designed, deployed, managed and applied the same way across all network segments.

Most enterprise applications are in the cloud, and most people no longer need to use VPN to access corporate applications and email. But these remote workers still access and store corporate data on their devices, which means they need to secure their Internet activity.

Teleworking environments also change the setting for teams, and this change to their behavior can cause various problems, including communication difficulties, lower productivity and exposure to many new security risks. Teleworking also exposes a much broader attack surface as workers use 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 found in the work environment. Public Wi-Fi networks present a higher probability that authentication and credentials may be accidentally compromised. These users are substantially outside the reach of perimeter-based controls and will have an even higher risk of compromise by malware-based attacks.

Certainly, teleworking employees often lack the same level of sophistication protecting them that they have at the office with next-generation firewalls, intrusion detection, deception technology and machine-learning-based security controls.

Targeted Threat Intelligence

Coronavirus-themed cyberattacks are already taking advantage of the disrupted workplace. COVID-19 has become the subject line of choice for cybercriminals seeking to take advantage of displaced teleworkers who already have a heightened level of fear and concern.

During the first week of March, our threat intelligence team noted that LokiBot Infostealer joined the list of malware campaigns being distributed by cybercriminals taking advantage of the fear and interest in the spread of coronavirus.² From March 3 to 6, we observed two malicious spam email campaigns distributing LokiBot under the guise of providing information on the coronavirus impact to supply chains.

LokiBot has become popular with cybercriminals as an information stealer that collects credentials and security tokens from infected machines. LokiBot targets multiple applications, including but not limited to Mozilla Firefox, Google Chrome, Thunderbird and FTP.

The email messages of the primary campaign had two subject lines, one of which alleged to be a supply chain update in the context of coronavirus (COVID-19). The other subject had a more typical payment transfer theme. Both sets of messages had attached files with the same filename that delivered the malicious code.

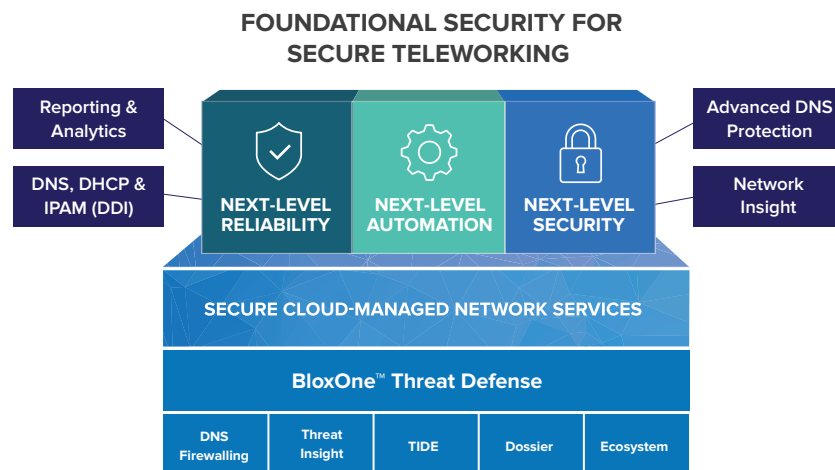
2. <https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence-62>

Protecting Teleworkers with BloxOne™ Threat Defense

BloxOne Threat Defense protects enterprise users, devices and systems no matter where they are, strengthening and optimizing your security posture from the foundation up. Our unique hybrid architecture extends pervasive protection across your on-premises, remote locations and teleworking environment. It detects and blocks phishing, exploits, ransomware and other modern malware, and it prevents your teleworkers from accessing objectionable content restricted by policy. Unique patented technology prevents DNS-based data exfiltration, to keep protected data safe, monitors for advanced threats (including lookalike domains) and automates incident response so that your security ecosystem can remediate any incidents quickly. Wherever you are, and whatever you do, Infoblox controls enforce your policies and protect your teleworking users.

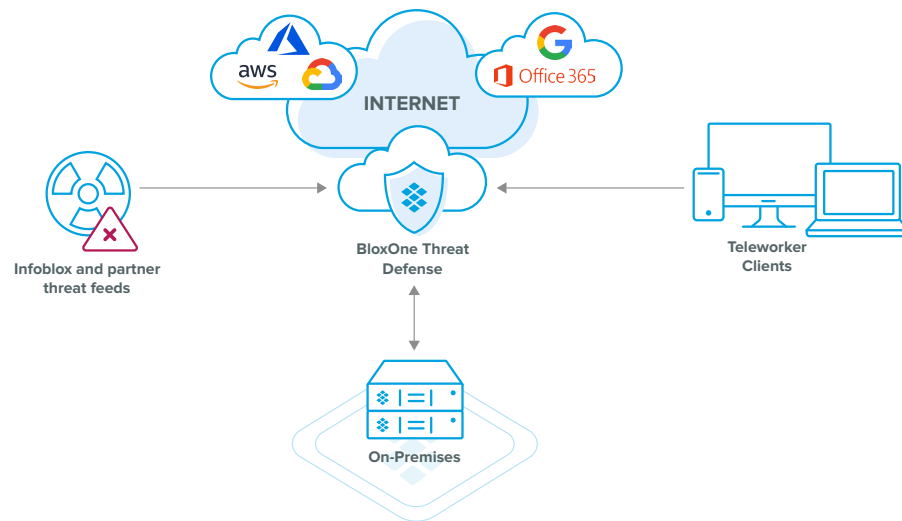
Using DNS as an essential control point ensures that every Internet request is inspected to determine if it is malicious, as identified by our integrated threat intelligence, analytics and machine learning. DNS also gives you scalable web and content filtering and reduces your overall threat defense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

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



By deploying BloxOne Threat Defense, and leveraging cloud capabilities, enterprises can easily extend the benefits of this protection to all users globally without having to rely on VPNs or other traffic steering techniques. The BloxOne Threat Defense client is both lightweight and easily deployed. Unlike other client technologies, 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 2: BloxOne Threat Defense extends protection to remote workers.



BloxOne Threat Defense provides one architecturally efficient and centralized point of control and visibility to any traffic that requires resolution of DNS services. You secure brand protection by locking down your networks and get the security you need to implement critical components of digital transformation, such as the cloud, SD-WAN, mobile platforms and the sprawling mix of IoT devices. BloxOne also gives you comprehensive integration with security orchestration, automation and response (SOAR) solutions, and it reduces the time to investigate and remediate threats. BloxOne Threat Defense increases the performance of your entire security ecosystem and lowers the total cost of ownership for your enterprise threat defense.

Important Technical Considerations

BloxOne Threat Defense is a security solution that uniquely solves several difficult problems for all environments, 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.

When BloxOne Threat Defense detects security threats, built-in integration allows administrators to seamlessly trigger additional actions from external tools to ensure that users' systems are remediated. Built-in APIs can push event data into these ecosystem tools quickly. These integrations enable automation of such actions as:

- Remote vulnerability scanning
- Remote antivirus scanning
- Protection from newly detected threats across all remote users and ecosystem integrations

When it comes to guarding against new and evolving threats, BloxOne Threat Defense uses AI/ML-based analytics on DNS to detect threats that cannot be otherwise detected. These include lookalike domains, zero-day DNS tunneling, domain-generation algorithms (DGAs) and fast flux. In addition, newer privacy trends like DNS over TLS (DoT) and DNS over HTTPS (DoH) have unwanted security implications. Content filtering at the DNS control point can be a cost-effective, low-latency solution to restrict workers at home from accessing specific types of web content. We will discuss these types below.

Lookalike Domains

Cybercriminals are moving to lookalike domains to fool victims in their efforts to impersonate the target organization or brand. Phishing websites often feature domains that impersonate the real brand. These are crafted to resemble the legitimate brand's domain.³

Character substitution is a popular technique employed by cybercriminals. The goal is to manipulate users into exposing credit card numbers, passwords and other sensitive data. Characters such as “1” may be replaced with an “l” (capital i). Many character substitutions can be detected, but we tend to see what we expect to see. By cleverly replacing just a character or two in your URL, the number of deceptions runs high. Multi-character substitutions also provide another opportunity to hijack your brand. For example, replacing the letter “m” with “rn” will fool many customers.

“YAHOO” is not the same as “YAHOO”

But more than 136,000 Unicode characters are used to represent common domain name letters and symbols in 139 modern and historic scripts, such as Latin, Cyrillic, Greek, Ukrainian and even Cherokee. Many of these character substitutions could be detected under close inspection. But, as with optical illusions and magic shows, the human eye tends to see what the mind expects to see. While surfing the web, few people will realize that “YAHOO” is not the same as “YAHOO”.

Researchers also find that cybercriminals are using valid Transport Layer Security (TLS) certificates in an attempt to make the lookalike domains appear legitimate.


In late 2019, researchers noted that more than 100,000 lookalike domains were impersonating legitimate retailers. The retail industry is in the center of the attacker's bull's-eye and experiences numerous attacks as cybercriminals attempt to steal shoppers' credit card data. Hundreds of lookalike domains used with phishing attacks have also been recently discovered in the Canadian banking industry.⁴

Lookalike domain attacks feature three basic layers of social engineering. These layers often include:

- **Site Content:** A site's content may be a modified copy of an existing legitimate website. Cybercriminals will frequently update this content over time to make the attack more effective.
- **URL Path:** Attackers need to present a credible path to support the deception. It can look like the real URL or obscure the real URL in some way.
- **Domain Name:** Typically cybercriminals use a domain name designed to appear legitimate under cursory inspection. In some instances, extra words or characters are added. In other cases, different characters are substituted, from other languages or fonts, that may closely match the correct character and when quickly read are hard to discern.

3. Info Security. “Boom in Lookalike Retail Domains.” November 14, 2019. <https://www.infosecurity-magazine.com/news/boom-in-lookalike-retail-domains/>

4. Bank Info Security. “Phishing Scams Target Canadian Bank Customers.” December 24, 2019. <https://www.bankinfosecurity.com/phishing-scams-target-canadian-bank-customers-a-13551>



BloxOne Threat Defense Custom Lookalike Domain Monitoring enables you to proactively stop lookalike socially engineered attacks. You can submit your own domain, or domains frequently used by your organization, to the Infoblox Cyber Intelligence Unit (CIU). The CIU will analyze and identify likely lookalike domains that will require monitoring. If these lookalike domains generate any suspicious activity, your organization will promptly receive an alert to potential brand-damaging activity.

Teleworkers will likely be active on a mix of mobile devices, home networks and public Wi-Fi networks and have a high probability of facing lookalike threats. Without a security control like Custom Lookalike Domain Monitoring, these teleworkers will be more easily targeted and vulnerable to these attacks.

Domain Generation Algorithms

Various types of malware use domain generation algorithms (DGAs) 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. DGAs allow attackers to rapidly switch the domains that are supporting their malware attacks. As defenders identify and block malicious domains, DGAs enable cybercriminals to move quickly to counter these actions.

Machine learning provides a new capability to identify and block DGA-based communications that present risks to your organization. Infoblox Threat Insight uses behavior analysis to classify DGA domains and separate them from normal domains. Using such techniques as analysis of entropy, n-gram, lexical and size, Threat Insight helps identify and block DGAs. Because DGAs usually do not resolve to Internet Protocol (IP) addresses, that behavior is also used to train the machine-learning mathematical models.

Fast Flux

Fast flux is a DNS technique that cybercriminals use to camouflage phishing and malware sites behind a shape-shifting network of compromised hosts acting as proxies. Using this technique, botnets can shift between IP addresses, which enables cybercriminals to evade detection.

Security solutions relying solely on threat intelligence are vulnerable to missing this type of technique deployed by sophisticated attackers. Infoblox Threat Insight combines machine learning and behavior analysis, finely tuned to DNS to distinguish fast flux domains from normal domains, to protect end users and remote employees from these attacks. Threat Insight is embedded within the BloxOne Threat Defense solution.

DNS Tunneling

DNS tunneling is an attacker technique that uses malware to gather sensitive data from the infected system. It packages data into small portions embedded within a string of DNS queries. These queries follow the DNS standard and bypass all security solutions. The DNS queries carrying the packages are delivered to a DNS server hosted by the attacker, stripping the incoming queries of DNS and reassembling the stolen data. 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 usage of DNS tunnels.

DNS tunneling can be detected with two major methods—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 teleworkers.

Content Filtering

When you need to protect a large-scale remote workforce, scale and cost-effectiveness become huge 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 the corporate 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 has to be funneled through these systems.

Integral to every connection, DNS is an architectural core component of infrastructure that lets you filter the most significant number of requests in the most efficient way. It can block access to non-compliant content. It also keeps the workload off more expensive security solutions while requiring substantially fewer resources and time to manage.

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 company policy. The solution also enables administrators to review content activity.

DoH

DNS over HTTPS (DoH) is a new feature that is 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. As a result, threats like data exfiltration and C&C callbacks go undetected.

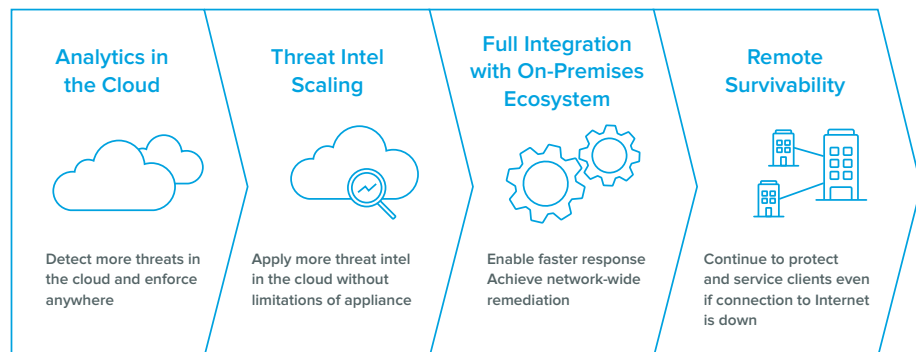
To mitigate these risks, organizations should use internal DNS infrastructure and enforce security policies through DNS by blocking the use of third-party public DoH resolvers. BloxOne Threat Defense and Infoblox threat intelligence services include a special feed called “DoH Public IPs and Hostnames” to help detect attempts to access unmanaged, DNS over HTTPS resolvers and block them, forcing browsers to gracefully failover back to the organization’s managed DNS without interruption to 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.



Hybrid Architecture

Most organizations need analytics and threat intelligence combined with the scalability of the cloud to provide policy enforcement and remediation. Cloud-only solutions can furnish the scale but don't offer the means to remediate compromised clients or gain full visibility into internal threats.

Figure 3: Hybrid architecture offers advantages over cloud-only or standalone on-premises architecture.



The Infoblox hybrid architecture offers these advantages:

- **Cloud Scalable Analytics:** The Infoblox hybrid model provides analytics detection of a wide range of threats. They include domain-generation algorithms, fast flux attacks, fileless malware and dictionary DGA. A threat detected on a roaming remote teleworker can be automatically enforced universally for all other users, devices, assets and applications.
- **Threat Intelligence Scale:** The Infoblox hybrid model enables highly scalable intelligence supported by the cloud. Infoblox shares only active threats to support the scale limitations of your on-premises appliances.
- **Security Ecosystem Integration:** The Infoblox hybrid model allows complete integration with your on-premises technology sets. This integration enables your team to gather important network context and deliver faster, more accurately prioritized incident response and network-wide remediation.

- **Survivability and Resiliency:** Internet disruption still allows your on-premises Infoblox solutions to continue to secure your network.
- **Simplified Single Point of Administration for the Enterprise:** Now you have a single point for most of your administration, control and visibility for both on-premises and your clouds. This simplifies and reduces the cost of administration and reduces error.

Recommendations

Given the current state of the coronavirus pandemic, federal, state and local government policies are requiring enterprise employees to work from home and to collaborate with clients remotely. These organizations have announced new policies to allow employees to work from home or are in the process of doing so.

Deploying a best-practice strategy that supports both your on-premises infrastructure and your remote workforce is essential. Comprehensive visibility to your remote activity is also critical. Using BloxOne Threat Defense and our DNS, DHCP and IP address management (DDI) services enables you to better secure remote workers, protect your critical infrastructure and secure your intellectual property.