SOLUTION BRIEF

BloxOne™ Threat Defense for Healthcare

The Healthcare Challenge

Healthcare remains one of the biggest targets for cyberattacks globally. Healthcare data is comprehensive and provides all of the materials cyber criminals need to falsify financial applications and these attacks have increased substantially over the past 18 months. According to the U.S. Health and Human Services Office of Civil Rights (HHS/OCR),by HIPAA regulation, if a data breach has impacted over 500 individuals in the U.S. then it must be reported to HHS/OCR. That's essentially only major healthcare breaches. The HHS OCR database portal is available here.

When reviewing the 2018 and 2019 breaches to identify those caused by "it/hacking", it was found that these major reported healthcare data breaches in the United States have grown from 2018 to 2019 at a rate of what appears to be well over 90% to a total of 325+ breaches in 2019. If you total the record counts, and assume no overlap in unique patient records, these breaches indicated the theft of 35+ million patient records in total in 2019, up from 10 million patient records stolen in 2018. For additional context, consider that the population of the United States in 2019 is approximately 329.45 million, which means that potentially over 10% of all U.S. residents had their healthcare records breached in 2019.

Important Healthcare Cybersecurity Use Cases

Ransomware Laden Phishing Emails

Ransomware remains a major threat to health care institutions. During our review of the HHS/OCR data we found that a majority of "it/hacking" events were in fact ransomware driven. The majority of ransomware was propagated through phishing email which tricked users into clicking malicious URL links, downloading malicious materials, or clicking on malicious email attachments. The detection of ransomware within healthcare networks is to be considered a data breach and reportable under HIPAA regulation so this increases both risk and liability for healthcare institutions.

DNS Targeted Attacks

The frequency and cost of DNS attacks continues to grow. Attackers can target healthcare as a direct target with DNS denial-of-service (DDos) attacks. DNS also can be used for surreptitious communications with command and control servers, the theft and exfiltration of data, establishing malware laden domains, and more. Domain Name System changer malware is another potential threat. DNS changer malware modifies the DNS settings of a

system and can allow cyber attackers to modify your router to misdirect your users to cyber attacker controlled websites. This attack is usually transparent to your users and seems to work as a standard DNS resolver. Even with the best cyber defenses, this mix of attacks using DNS can be impossible to identify and remediate without foundational security.

Medical Device Hijack and IoT Based Threats

Medical device hijack, otherwise known as Medjack, remains a constant risk for healthcare cyber defense teams. Medical devices generally cannot support any endpoint security or other software agents as they are FDA approved and essentially closed to modification or the installation of any other software. This means they don't have the inherent ability to identify and block malicious activity. This leaves the attack surfaces exposed within medical devices as virtually unprotected.Once malware circulates within the hospital networks, it can easily infect medical devices. Close visibility and inspection of the traffic emanating from these devices can help identify and shut down medical device based threats before they can result in a reportable data breach.

Ambulatory Physicians and Unprotected Mobile Devices

Physicians move between their practices, hospital networks, skilled nursing facilities, and diagnostic laboratories on a regular basis. Their mobile devices are always moving between these networks, and are always a potential source of malware introduction.

DNS Tunneling

DNS tunneling allows attackers that have successfully compromised banks to gather data and then exfiltrate it within a string of DNS queries. This appears to follow the DNS standard and hence bypasses all of the healthcare institutions other DNS solutions. This attack vector can also be mitigated by the use of a foundational security solution.

Healthcare Compliance Challenges

Threat intelligence and the enhanced capabilities delivered by foundational security can help healthcare institutions potentially find new ways to reduce the risk of data exfiltration. This, in turn, may assist with efforts to meet health care compliance, which is regulated by the Health Insurance Portability and Accountability Act of 1996.

Healthcare Institutions Reduce Risk with Foundational Security

One U.S. hospital chose the BloxOne Threat Defense architecture to help protect both cloud-based and on-premise services and applications. This hospital includes a main campus with over 500 hospital beds and admits over 25,000 patients per year in the main hospital facility alone. Primary care practices, specialty care and ambulatory surgery centers, urgent care centers, newborn and pediatric inpatient units, and other specialized care support the over 1 million patients seen on an outpatient basis.

This hospital wanted to strengthen its DNS infrastructure and selected BloxOne Threat Defense as part of a new and robust cybersecurity strategy to prevent DNS based data exfiltration. It can now leverage the full set of BloxOne foundational security capabilities for expanded protection on-premises, within the cloud, and across networks utilizing SD-WAN and IoT. This is critical to the future, as it continues to add many IoT connected medical devices to its internal networks.

Another U.S. based hospital network chose foundational security to strengthen their DNS infrastructure and DHCP to a more stable enterprise network grade as well as to add additional protection for their vulnerable medical devices. This leading hospital includes several facilities with multiple hospital campuses, over 1,500 physicians and over 25 regional health centers and clinics. They brought in Infoblox DDI and

BloxOne Threat Defense and Threat Essentials. Their goal was to safeguard patient data and minimize the potential for DNS data exfiltration. BloxOne Threat Essentials threat intelligence also offered protection for internet of things (IoT) devices, helping secure many of the medical devices used for treatment, against malware.

Protecting Healthcare Institutions 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. Its hybrid architecture extends protection across your on-premises, remote locations, and teleworking environment. It detects and blocks phishing, exploits, ransomware, and other modern malware, and it prevents workers 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.

Infoblox controls enforce your policies and protect all of the employees and devices in a healthcare institution, both on-premises and remote. Using DNS as an essential control point ensures that every Internet request, either from a medical worker's laptop or from a connected healthcare device, 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.

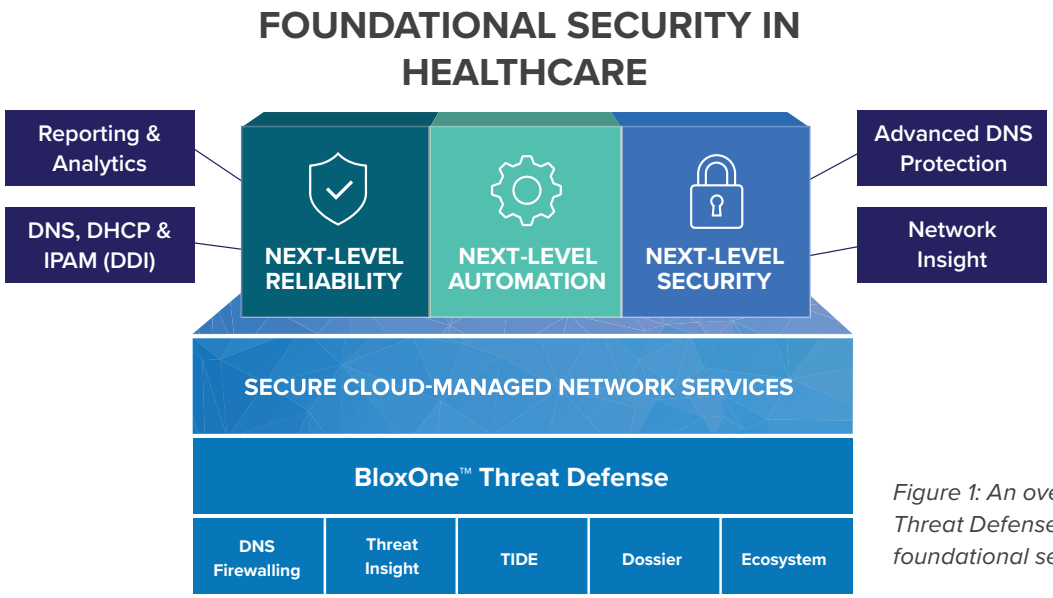

Figure 1: An overview of BloxOne Threat Defense and its key foundational security components

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com