Cybercrime is on the rise -- breaches in 2019 increased 17% over 2018, the SANS Institute reports -- and healthcare is especially at risk. Annual health data breaches have risen 70% over the past 7 years, with more than 130 million records targeted by a “hacking or IT incident,” according to a study in the Journal of the American Medical Association. And the threat landscape in 2021 promises to be even worse.

Healthcare organizations must protect vast swaths of personally identifiable information -- but there’s more than just data on the table.

“When you look at ransomware through the lens of healthcare, you start talking about lives,” said Allen McNaughton, director of pre-sales engineering at Infoblox Public Sector. “Somebody is on the operating table and all of a sudden the connected devices that are around there aren’t working anymore.” In fact, a woman in Germany died September 10 when a hospital that had been hit by a ransomware attack had to turn her away. She died before she could be treated at a second hospital.

And the attacks are now hitting the U.S. On one day in late October 2020, six hospitals were attacked by the Ryuk ransomware, which the Federal Bureau of Investigation believes came from a Russian gang of cybercriminals. The FBI, the Cybersecurity and Infrastructure Security Agency, and the Department of Health and Human Services issued a joint advisory warning of the danger, citing ‘credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.’

Given the high stakes, healthcare organizations need a new approach to secure not just their networks, but an increasingly sprawling ecosystem of medical devices and Internet of Things (IoT) appliances.

The rise of IoT
Connected medical devices are a special area of concern. In 2018, the FDA released a medical device security playbook to help identify security vulnerabilities, but only 61% of healthcare IT professionals are confident that this is an effective security policy for the healthcare industry. Almost a quarter (23%) of these professionals are unfamiliar with or do not know about the policy.

The increasing use of networked medical equipment and IoT devices has added an extraordinary layer of complication to the business of securing healthcare organizations.

“Every single one of those devices -- from tablets that the medical staff are carrying, to access control systems for buildings, to MRI machines and million-dollar systems -- are all networked in some capacity,” said Chris Usserman, principal security architect, Infoblox Public Sector.

There are deep interconnections. Digital prints from an MRI machine may be transferred electronically to some other part of the network for processing and storage. When that MRI machine reaches out to its vendor for updates and upgrades, that’s a potential security gap.
“An attacker can get into that device and use the trust in the device to connect to other parts of the network,” Usserman said.

The wide array of IoT devices expands the attack surface. All the traffic coming in and out of those endpoints can be compromised, and the interconnections can potentially be leveraged to give attackers access across multiple, indirectly related systems.

A new vision
In order to secure this vast and heterogeneous landscape, healthcare organizations need to organize their networks in such a way as to protect components not just from outside intruders, but from each other.

“It should not be just a hard outer shell, where once you penetrate that, you’ve now got unfettered access to everything else,” McNaughton said.

Instead, IT leaders need a broad and deep approach to security, one that starts at the top and spans their entire connected ecosystem. Within this architecture, a next key step is to leverage automation across the security infrastructure to the greatest extent possible.

Especially in the COVID era, when many organizations are operating short-handed and decentralized, it’s important to minimize the manual labor associated with security tasks.

“Security tools should work together in order to automate responses,” McNaughton said. “That requires the ability to categorize and contextualize data, so that when an alert gets to an analyst, they can be confident that it’s a real threat.”

The Infoblox approach
Infoblox takes a multi-pronged approach providing security augmented by automation and contextualization.

It starts with DDI: A holistic approach that addresses Domain Name System (DNS) security; Dynamic Host Control Protocol (DHCP) address assignment; and IP address management.

Typically, a device connects to a network via Dynamic Host Control Protocol (DHCP) and is assigned an IP address. When Infoblox issues IP addresses, it creates accountability and visibility. Administrators know that a given person is connected via a particular device, and what devices are active across the enterprise at any given time.

“We actually fingerprint what that device is,” McNaughton said. “You can keep an authoritative database, knowing what device you’ve given an IP address to, and even its location within a building. I can say: Allen is on a MacBook Pro running Catalina in the lobby.”

A solid defense then adds specific controls around DNS – effectively patrolling the entry/exit gate. “A computer or a device or an application will reach out via DNS to figure out where it’s going. That’s the first communication from a device once its connection is established on the network, and you need to be able to look at that, to manage and monitor it, and act upon it accordingly,” McNaughton said.

With Infoblox, if a computer is sending malicious DNS traffic, or attempting to connect with a malicious internet destination, both knowingly and unknowingly, security teams can see where that’s happening and immediately dig into the problem.

By putting in place DNS security controls, “you can control or limit the ability of malware to connect with its command and control servers 92% of the time,” Usserman said.

DNS actually plays a critical role in execution of most malware campaigns, including the recent Ryuk ransomware campaign targeted at healthcare companies. The campaign leveraged a tool called anchor_dns that used DNS as the control plane to execute PowerShell command scripts. It also used DNS as the data exfiltration channel.

“Because we’re handling security at the network layer, we can also institute a DNS-based firewall,” he said. “Utilizing the millions of verified indicators that we bring to the table, as well as customer defined threats, we can stop those at that initial callout point and then alert the security teams that there’s something on my network attempting to reach out to somewhere bad.”

At the same time, Infoblox delivers threat contextualization as part of its Security Orchestration and Automated Response (SOAR). This approach enables security teams to prioritize threats depending on their severity, and to automate responses, especially to low-priority threats that can be remediated by AI and other defensive tools.

“If I have an alert that comes in, and it’s mixed in with 1,000 other alerts, how do I choose which ones go to the top of my list for immediate response?” Usserman said. Contextualization and automation helped ensure high-value security experts are devoting their time and skills toward the highest-risk/highest-threat incursions.

Going forward
Government healthcare organizations can take steps now to pivot toward a more proactive approach to security. The first step is to take a thorough inventory. Given the wide array of medical devices, IoT endpoints, BYOD connections and traditional PCs deployed across a healthcare organization, it’s important to have a full and clear picture of what’s actually on the network.

“Knowing what’s on your network is vital,” Usserman said. “What are the doctors and the other staff connecting to -- not just the large devices but everything else that runs on the network? You want to look for the east and west, the north and south, to understanding what’s happening, what is permissible, what is regular, and what is authorized.”

It makes sense to investigate whether and to what extent you’re already applying early-stage security controls. “Are you managing and monitoring from a DNS perspective on those devices?” McNaughton said. From there, organizations should utilize security ecosystem integrations to automate and orchestrate the security response playbooks.

With support from a vendor like Infoblox, healthcare organizations can apply DNS-level defenses that secure network connections and apply automated management controls to the entire spectrum of connected devices, from desktops to medical equipment to IoT. This top-level approach to security ensures organizations can meet their regulatory obligations, while powerful visibility and contextual data can drive greater levels of automated response to free skilled security personnel to focus on the most pressing threats.