Internal Segmentation Firewalls for the Healthcare Industry

Introducing a New Approach to Securing Healthcare IT
Internal Segmentation Firewalls for the Healthcare Industry
Introducing a New Approach to Securing Healthcare IT

Table of Contents

Introduction 3
Not Just a Cold—a Syndrome 4
New Diseases Require New Medications 4
Beyond Quarantine 5
Aligning Your Security Technology 6
Fortinet ISFW Solutions for Healthcare 7
Conclusion 8
Introduction

Compliance, Risk and Responsibility

Security in the healthcare industry is more than just a matter of compliance. Obviously, the regulatory environment is a significant consideration, but healthcare providers, insurers, and others have a real responsibility to protect patient data, the value of which has been estimated at ten times that of credit card data on the black market. Why is it so valuable? Because Protected Health Information (PHI) can be used to build exceptionally rich personal profiles, enabling identity theft, cyber espionage, and even extortion.

The sheer value of PHI to cyber criminals, nation states, and other bad actors paints a large target on healthcare, increasing the risk to both patients and providers. At the same time, researchers, pharmaceutical companies, and device manufacturers are finding their intellectual property increasingly at risk, not just from competitors but from attackers in a variety of nations where drug counterfeiting is rampant.

Data breaches, then, can, for example,

- Cost a pharmaceutical company billions in lost revenue
- Permanently damage the reputation of an insurer and, again, cost billions in patient compensation
- Carry significant costs for patients, both financially and in terms of safety and privacy
- Result in substantial penalties under HIPAA and the HITECH Act.

Healthcare, however, has typically not invested in security in the same way as other regulated industries and recent headline-grabbing breaches bear this out. The only solution is for healthcare to play catch up and begin implementing innovative approaches to protect patients and their most valuable data.

42.5% of the data breaches reported in 2014 were in the healthcare industry. Nearly 100 million patient records have already been exposed in the first half of 2015.

—Identity Theft Resource Center
Not Just a Cold—a Syndrome

Medical professionals define a syndrome as a collection of symptoms and conditions that, taken together, often constitute a much more serious illness. The common cold is inconvenient but rarely of concern. SARS and MERS, on the other hand, are more concerning public health problems.

The healthcare security landscape is much more akin to a syndrome, with multiple problems and challenges creating a perfect storm of vulnerabilities that place patients, providers, researchers, and payers at risk. Whether it’s stolen intellectual property leading to counterfeit medication or patient data breaches exposing patients to fraud and identity theft, lapses in healthcare security can be expensive, damaging, and even dangerous.

Security professionals often refer to an attack surface – all of the different points or vectors through which attackers can compromise a system. In healthcare, the attack surface is especially large:

- Traditional cyber attacks use desktop and mobile malware, phishing schemes, Trojans, ransomware, and more to target users, mobile devices networks, servers, and databases, allowing attackers to gather protected health information (PHI) and other critical data from healthcare enterprises. What separates healthcare from other enterprises, though, is the very high value of the data. Patient records can fetch up to 10 times more on the black market than credit card numbers.

- Connected medical devices are proliferating rapidly in hospitals and clinics and not only transmit sensitive information to electronic health record (EHR) systems but are often used to automate patient care. While the potential to compromise patient data in motion from these devices is a real concern, the FDA recently issued its first warning about the physical danger to patients from a compromised device (in this case, an infusion pump that could be taken over by attackers and used to deliver a fatal dose of medication).

- Home healthcare devices are a relatively new phenomenon that can be as simple as a fitness-tracking wearable or as complicated as remote monitoring or telemedicine equipment. Whatever the implementation or use case, these heterogeneous devices provide a growing number of potential points of entry to sensitive information systems.

The combination of an unprecedented attack surface with high financial stakes, network and data center architectures optimized for performance rather than security, and sophisticated attackers employing advanced threats and social engineering techniques makes healthcare IT particularly vulnerable. More importantly, the nature of the devices and data flows involved means that healthcare networks are vulnerable both to external attacks and internal threats.

New Diseases Require New Medications

When bacteria develop drug resistance, we use more powerful, novel antibiotics. When surgeons encounter new challenges, they develop new operating techniques or seek out innovative devices. The same is true of network security.

Just as amoxicillin remains a first line of defense for many bacterial infections, perimeter firewalls and endpoint protection are still essential elements in a security ecosystem. But the nature of threats to healthcare networks is such that we now need to introduce new tools and layers of protection that operate much closer to our critical data as seen from the threat life cycle in Figure 1. Enter the Internal Segmentation Firewall (ISFW).

The ISFW was developed in response to a growing awareness that network threats are no longer just coming from attackers outside a network attempting to breach defenses like next generation firewalls. Now, sophisticated spear phishing attacks fool even savvy users into providing access credentials that let cybercriminals through the proverbial front door. Some of the largest recent breaches in healthcare appear to be the result of such attacks.
In the same way, the pervasive use of mobile devices by healthcare professionals, both on and off protected networks, means that potentially infected devices are regularly being brought inside healthcare networks. Guests come and go at hospitals and clinics, accessing open networks or even having physical access to potential attack vectors like connected medical devices.

Vendors and device manufacturers are also introducing new hardware and software with far less visibility and control than IT normally enjoys in other enterprise settings. Partners, affiliates, and other outside agencies leverage healthcare networks while IT administrators must focus first on enabling patient care and research amidst a complex threat landscape.

The bottom line is that healthcare networks are subject to an extraordinary number of internal threats. And once attackers are inside the network, they will too often find it very flat, making it easy for criminals to move among resources and increase their footprints, all while hiding from defenses focused on the perimeter rather than the servers, devices, and data that have their own share of vulnerabilities.

Quarantine is also a term from the early days of computer antivirus applications. Known viruses and infected files would be logically quarantined for inspection or deletion. Now, however, technology has advanced to such a point where we can be far more intelligent about how we protect our networks infection just as we can generally do a much better job of protecting populations from illness with modern approaches to public health, infection control, etc.

Internal segmentation firewalls are a critical component of this evolving approach to network security. Because they operate inside our networks instead of at the edge (Figure 2), they allow us to prioritize assets that need the highest degrees of protection and monitoring, all without impacting performance. As their name suggests, ISFWs have moved far beyond the notion of quarantines and instead segment networks, dramatically improving visibility into possible attacks and providing complete internal segregation of data and resources to both comply with regulatory requirements and to better meet the complex security needs of healthcare organizations.

**So How Does An ISFW Work?**

ISFWs are specially designed firewalls that are deployed at strategic network locations in so-called “transparent” or bridged mode. This turns off the routing functions built into most next generation firewalls (NGFWs) and allows for rapid inspection of traffic as it moves across a network. Fundamentally, this translates into faster time to detection of a threat on the network instead of waiting for an attacker to attempt to exfiltrate data or contact a command and control server that perimeter defenses are best equipped to detect.

For ISFWs to be effective and avoid becoming bottlenecks on a network, they must have

- Extremely high throughput with custom processors designed for line-speed traffic inspection
- High port densities to accommodate top-of-rack and other internal network functions
- The ability to be deployed in-line rather than at normal points of data ingress and egress.

**Beyond Quarantine**

To control serious communicable diseases, healthcare providers often rely on quarantine to prevent the spread of infection. It isn’t realistic to quarantine every patient with an illness, of course. The practice is disruptive, expensive, and rarely necessary; it’s certainly ineffective for patients who don’t even know they are sick or that they might have been exposed to a serious illness.
Does An ISFW Replace NGFWs?

As we know, an increasing number of security threats now come from inside a network. Many attacks also originate outside a network and attempt to breach perimeter defenses directly. ISFWs and NGFWs are complementary technologies that prevent, detect, and mitigate internal and external threats, respectively.

When an attack gets past perimeter defenses through user error (e.g., a successful phishing attack), the introduction of infected endpoints directly into a network (e.g., a physician’s tablet), or a direct attack on an internal endpoint (e.g., a connected medical device), an ISFW protects internal resources in ways that NGFWs weren’t designed to do.

NGFWs, by virtue of their deployment locations, largely inspect “North-South traffic”, or traffic entering and exiting a network. ISFWs, on the other hand, inspect “East-West traffic”, or traffic moving between locations inside a network. Taken together, these related technologies provide near total control and visibility into the data and applications running into, out of, or on a network. This level of control is of particular interest in healthcare because regulatory requirements dictate wellplanned segmentation and segregation of protected health information and health information systems.

Aligning Your Security Technology

As healthcare organizations spend increasingly larger percentages of their IT budgets on security, aligning those investments with the specific needs of providers, payers, and researchers becomes critical. ISFW fills a significant gap in network security that allows IT to securely deliver platforms that enhance patient care, make providers more efficient, and better comply with regulatory mandates.

With Clinical Workflows

Both the FDA and the Department of Health and Human Services frequently talk about patient data in motion and data at rest. Healthcare organizations must grapple with data in motion from a wide variety of sources:

- From mobile devices, laptops, and terminals used by doctors and nurses to EHR systems
- From connected devices to workstations and EHR systems
- To and from payer systems

Unfortunately, many of these systems aren’t under direct IT control. For example, many mobile devices are used under BYOD scenarios or frequently leave the network, while connected medical devices like imaging equipment are installed and managed by vendors instead of IT. Vendors may even install servers and workstations directly into hospital racks with little oversight from IT who are expected to strictly plan an enablement role for such patient care systems.

ISFWs then give IT the ability to provide physical demarcation with clinical hardware and increase visibility into traffic to and from these systems.

With Regulatory Requirements

This same issue of demarcation and segmentation is fundamental to satisfying regulatory requirements related to protection of patient data. Healthcare organizations have been working for years to move to a single common architecture that also maintains the demarcation between patient data and other systems required by HIPAA and the HITECH act.
ISFWs are a natural extension of regulatory security efforts. Because they can be deployed inline, network administrators gain unprecedented control and visibility to improve compliance with no appreciable impact on performance or usability issues for clinicians. In this setting, Fortinet ISFW protects from internal threats but, more importantly, creates intelligent network segregation.

With the Realities Of Healthcare Networks

Many healthcare settings maintain parallel networks, essentially a split domain infrastructure. One is tightly controlled as would be expected in a regulated enterprise environment. The other is more open, intended to meet the needs of physicians, researchers and academics, device vendors, patients, and even the hospital gift shop.

Maintaining parallel networks in this way is expensive, time-consuming, and an easy way to introduce network vulnerabilities. Again, ISFW provides the tools to build a common architecture for healthcare networks.

Fortinet ISFW Solutions For Healthcare

ISFW is a new class of firewall, characterized by high performance, high port densities and transparent deployments enabled by default. Figure 3 shows where ISFWs fit into the overall picture of network security appliances. For healthcare in particular, there are several key use cases for internal segmentation firewalls.

In the Data Center

EHR systems have increased efficiency, improved patient care options, and made it easier to coordinate care. Yet the move to centralize protected health information has increased security pressures on healthcare data centers. Cloud-based EHR providers also bear considerable burdens securing their own data centers to provide reliable, safe services to their customers.

Whereas next generation firewalls sit at a network’s perimeter and data center firewalls sit at the edge of a data center, ISFWs can be brought very close to the data they need to protect. They can be deployed around private clouds, physical servers running EHR systems, and vendor systems installed in healthcare data centers. ISFWs can lock down these data stores and detect intrusions and attempts to exfiltrate data long before attackers attempt to move data off the network, even if the attacks were launched from within the network itself.

Around Legacy Systems

Healthcare settings are breeding grounds for legacy systems that may no longer be able to receive security patches. Researchers may run protocols for years at a time, relying on legacy workstations and databases while expensive imaging hardware may long outlive installed software. Forklift upgrades of embedded systems and other workstations may impractical, too disruptive, or too expensive to undertake.

ISFWs can protect these systems by keeping them in their own network segments while still allowing unfettered access by clinicians and the health information systems into which they feed data.

In the Clinic

The FDA recently issued its first warning about a medical device that was vulnerable to attack and that could be used to deliver fatal doses of medications to patients. Researchers have demonstrated dangerous vulnerabilities in other connected medical devices as well that could be exploited either to harm patients or to access patient data.

Here too, placing an ISFW inline with the connected devices can provide levels of security that often aren’t built into machines designed to improve patient care rather than secure patient data or ensure patient safety. As these devices proliferate and age, securing them at the device level instead of the network level will become quite challenging for IT departments.

For the Payer

Insurance companies have been making headlines with the largest healthcare breaches to date. Many have come under fire for inadequately securing their most critical assets—patient data. ISFWs allow payers to isolate patient data stores without interfering with existing transactional systems. Again, the inline, transparent nature of ISFWs makes them ideal choices for rapid, non-disruptive deployment.

For the Outside Entity

Hospitals often outsource pharmacy services, gift shops, cafeterias, etc. Each of these entities often brings their own information systems with them, expecting Internet access but not providing control to hospital IT. ISFWs allow IT to monitor and segregate networks and information systems for these entities without needing to control or manage their individual systems.
Conclusion

The stakes are incredibly high when it comes to healthcare security. Financial penalties for data breaches are high and patient data is more valuable than ever to both cybercriminals and nation-states interested in espionage. Recent evidence suggests that cyber spies are, in fact, building large databases from healthcare data breaches for future use against citizens.

At the same time, the threat landscape only gets more complex for healthcare with the Internet of Medical Things, EHR, and clinician demands for intelligent tools placing further strain on already stretched IT resources.

Fortinet offers a complete ecosystem of security tools that provides the required protection, segregation, and segmentation for patient data and critical healthcare systems. New internal segmentation firewalls fill the gap in securing networks against internal threats and offering flexible architectures uniquely suited to healthcare environments.

About

Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company’s fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pureplay network security providers, Fortinet can solve organizations’ most important security challenges, whether in networked, application or mobile environments—be it virtualized/cloud or physical. More than 200,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands.

Learn more at http://www.fortinet.com/healthcare and Twitter: @FortinetHealth.