The Fortinet Secure Health Architecture

Providing Next Generation Secure Healthcare for The Healthcare Industry

Authored by: Mark Hanson – U.S. Director – Fortinet, Inc. - Healthcare

Introduction

Healthcare providers are migrating from large, independent stand alone organizations to complex new ecosystems with provider organizations, affiliated physician groups, labs and business associates involved in both the provisioning of care, and the collection of vast amounts of information from patients. Health Information Exchanges (HIEs) are evolving and providing a conduit to transfer and store Patient Health Information (PHI). Healthcare as we know it is continuing rapid change.

Along with our changes in coverage and insurance via US legislation, a variety of technology initiatives are mandated by new regulations and are subject to new compliance parameters as well. Healthcare providers will soon be required to provide communication and collaboration platforms that allow seamless integration among the various stakeholders. These changes in information flows, along with an explosion of digital records content that needs to be stored and shared, are driving the need for a secure, flexible and scalable IT platform through which Providers, Payers, Pharmaceutical and Health Sciences can support collaboration and secure information exchange.

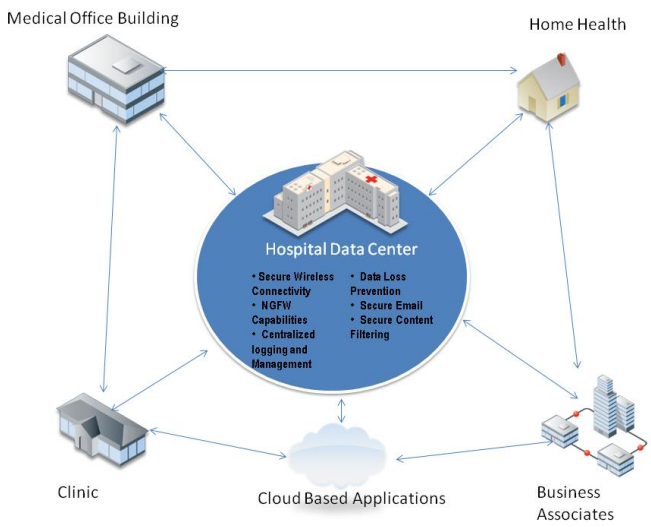
The transition towards more patient-centric care and decentralized monitoring means providers, patients and payers need to access information that originates outside the hospital setting. The trends toward personalized medicine, prevention and wellness mean stakeholders need to connect information from various points within the healthcare value chain. The more that private information is opened to outside entities, the greater the chance that these systems can be compromised and data is lost either accidentally through poor processes or intentionally through nefarious activity.

Upcoming Changes to the Healthcare Industry

In order to address these challenges, healthcare providers have to evaluate the security needs for different functions in the network. Securing the hospital or clinic is only one component in the modern distributed healthcare architecture (see Figure 1). As healthcare providers expand more services to customers and collect more data internally, they will find that the elements required to secure and manage those services extend beyond a single product and will require an ecosystem of products designed to work seamlessly to provide security while not interfering with the patient experience. Fortinet recommends customers evaluate their security needs at each of the following levels:

- Management Level
- Aggregation Level
- Business Associates Access Level
- Direct Access Level

Figure 1 - The Modern Distributed Healthcare Architecture



Here are several initiatives taking place as part of next generation healthcare along with the security implications of these initiatives. Each of the following challenges can be solved by providing security at one of the levels above.

Allowing Patient and Provider Access to the Network

As contradictory to security as it sounds, healthcare providers are now looking for ways to increase the access doctors, vendors, and patients have to healthcare industry, applications and systems. With new guarantees for patients regarding access to information and a focus on lowering costs through new initiatives like Health Information Exchanges, the entire healthcare center is driving towards a more collaborative environment where all parties have access to the information they need.

The most obvious security concern with this approach is ensuring that sensitive information like PHI and payment information is kept separate and secure from general Internet and network traffic. This requires encryption and wireless management technology coupled with traffic shaping technology to ensure that the appropriate treatment information is accessible and is always the top priority.

Increased Use of Clinical Informatics to Improve Workflow

Along with the increased collection and flow of data, healthcare organizations are constantly striving to improve workflow, both physical and informational. Improved workflows equal lowered costs, productive caregivers and an environment that allows improved patient safety and quality care. The key challenge from a security perspective is ensuring that only the required pieces of data are transferred and nothing more.

Constant Contact through Social Media

It should come as no surprise that healthcare organizations are looking for new ways to communicate with patients via mobile devices. According to new estimates by research firm eMarketer, time spent using mobile devices for activities has more than doubled in the past two years among US consumers, up to an average 82 minutes per day, up from just 34 minutes in 2010[1]. With more patients getting their information and media through mobile devices, healthcare organizations understand that patients are managing their care through these mobile devices and social media. Patients in the hospital and visitors are likely to be using social media to share updates with friends and family.

For the healthcare provider, the challenges with social media revolve around maintaining compliance with regulatory mandates – ensuring that no sensitive information is compromised. A very large challenge around social media includes keeping the network free from advanced threats and malware. As nurses, doctors, patients, and visitors all bring mobile devices on the network, the chance of infection from one of those devices increases.

Increasingly Stringent Compliance Mandates

As a result of the increasingly sensitive data handled by the healthcare industry, regulatory requirements have been implemented to help increase the security of healthcare providers and associates as well as the data they protect. HIPAA and HITECH set up standards around protecting PHI and more recently set up fines and

[1]http://www.emarketer.com/newsroom/index.php/consumers-spending-time-mobile-growth-time-online-slows/

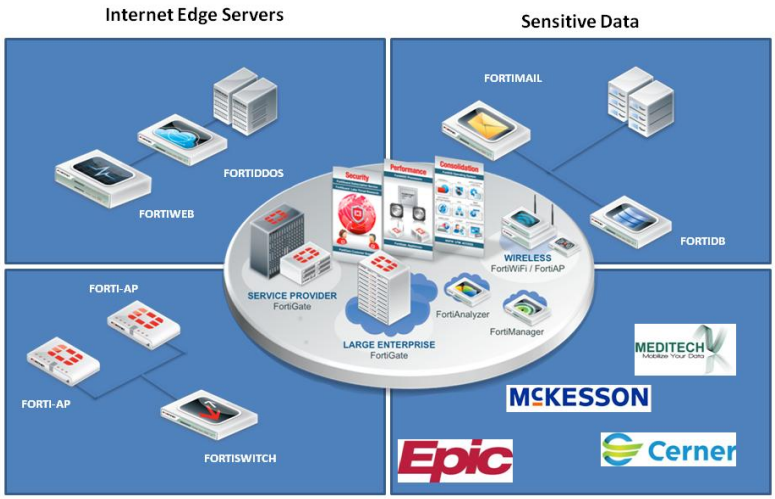
penalties for non-compliance through recent Omnibus rulings. The Stage 2 rules of Meaningful Use also mandate encryption as a core component of protecting PHI. Compliance mandates are becoming more prescriptive and including more security standards in their recommendations.

Healthcare organizations also find themselves responsible for complying with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS, the security standards set by the world's largest credit card providers, sets broad requirements for securing personal nonpublic information used on digital platforms in retail and now in the healthcare industry.

Fortinet Provides End-to-End Security for Next Generation Healthcare

All the challenges mentioned above require disparate functionality. This is where Fortinet's broad range of integrated security functionality and specialized product lines can provide solutions for healthcare environments that is unmatched by any other security vendor. Figure 2 illustrates how Fortinet solves many of the challenges facing healthcare today.

Figure 2- Fortinet Secures Next Generation Healthcare



Management Level

Given the widely distributed nature of modern healthcare establishments, the ability to quickly modify and manage security appliances is essential. Fortinet provides FortiManager and FortiAnalyzer products to help the Healthcare industry manage their distributed environments.

FortiManager ™

"Single pane of glass" management console for configuring and managing any number of Fortinet devices, from several to thousands, including FortiGate®, FortiWiFi™, FortiMail™ and FortiAnalyzer™ appliances and virtual appliances, as well as FortiClient™ endpoint security agents. You can further simplify control and management of large deployments by grouping devices and agents into administrative domains (ADOMs).

FortiAnalyzer ™

Centralized logging, analyzing, and reporting appliances securely aggregates log data from Fortinet devices and other syslog-compatible devices. A comprehensive suite of easily customized reports enables you to analyze, report, and archive security event, network traffic, Web content, and messaging data to aid measurement of overall policy compliance.

Aggregation Level

The aggregation level is the destination for all data. Typically this is the hospital datacenter. Core security functions such as firewalling, Intrusion Prevention, DLP, application control and VPN termination take place at this level. Fortinet's enterprise fixed rack and modular chassis based FortiGate appliances are the industry leading and best suited for this level.

FortiGate®

Fortinet's flagship network security solution that delivers the broadest range of consolidated network security and network services on the market, including: firewall, VPN, traffic shaping, IPS, antimalware, application control, Data Loss Prevention, vulnerability management and many

more security functions. Below is a couple models of FortiGate appliances that are found in our healthcare customers' data centers.

FortiGate-3600C

FortiGate-3600C network security appliance combine next generation firewall (NGFW) protection with unified threat management (UTM) security that provides an intrusion prevention system (IPS), application security, on-board sandboxing, antivirus and antimalware protection along with other security features. They offer unmatched performance, flexibility, and security for any large healthcare provider.

FortiGate 1000 Series

The FortiGate-1000 series integrates network and security functions into a single device to help identify and thwart multiple threats for mid-sized organizations and large branch offices of large enterprises. With numerous accelerated multi-threat security interfaces, healthcare organizations can create multiple security zones for various departments, users, access methods, and even devices to enforce network security at accelerated speeds.

FortiMail

The FortiMail family of appliances is a proven, powerful messaging security platform for any size organization, from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, the FortiMail appliances utilize Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats.

You can prevent your messaging system from becoming a threat delivery system with FortiMail. Its inbound filtering engine blocks spam and malware before it can clog your network and affect users. Its outbound inspection technology prevents outbound spam or malware (including 3G mobile traffic) from causing other Antispam gateways to blacklist your users.

Three deployment modes offer maximum versatility while minimizing infrastructure changes or service disruptions: transparent mode for seamless integration into existing networks with no changes to your existing mail server, gateway mode as a proxy MTA for existing messaging gateways, or full messaging server functionality for remote locations. FortiMail provides Identity-Based Encryption (IBE), in addition to S/MIME and TLS, as email encryption option to enforce policy-based encryption for secure content delivery. Furthermore, the FortiMail customizable and predefined dictionaries prevent accidental or intentional loss of confidential and regulated data.

Business Associate Level

The individual clinic, lab, doctor's office, or any business associate requires security and connectivity for a wide variety of functions including WiFi, voice, and traditional network connectivity. With the addition of consumer connectivity, each associate much also be able to provide security functions such as antimalware and application control. Fortinet products including FortiGate, FortiWifi, FortiSwitch, FortiVoice and FortiAP wireless access points provide all the components needed for a next generation healthcare organizations to operate in a secure manner while still offering an enhanced consumer experience.

FortiGate/FortiWifi 90 Series

The FortiGate/FortiWiFi-90 series security appliances deliver comprehensive enterprise-class protection for smaller locations, branch offices, customer premise equipment (CPE) and clinic networks. An integrated set of essential security technologies protects all of your applications and data. Through our range of clinical office solution we provide per-device pricing, with an integrated management console, a range of interface options (including modem, wireless broadband, SFP, 3G/4G, POE, and ADSL-A), as well as remote management capabilities significantly reduce procurement deployment and administrative costs.

Access Level

As healthcare organizations extend access to providers using tablets and to patients using mobile devices, ensuring secure access is critical. Fortinet has several products that can ensure secure access control through rogue AP detection, authentication, guest Wi-Fi, web filtering, rate limiting and load balancing to assist with your BYOD initiatives.

Wireless and BYOD

Wireless access point FortiAP solutions provide increased visibility and policy enforcement capabilities while simplifying your overall network environment. They employ the latest 802.11n-based wireless chip technology, offering high-performance wireless access point with integrated wireless monitoring and support for multiple virtual APs on each radio.

FortiAPs work in conjunction with the feature-rich family of FortiGate controllers to provide a fortified wireless space that delivers complete content protection. FortiGate controllers centrally manage radio operation, channel assignment, and transmit power, which further simplifies your deployment and management requirements by bring LAN WAN Security management together.

FortiSwitch with POE

The FortiSwitch platforms are purpose-built to meet the Ethernet infrastructure and provisioning needs of today's network edge. You can scale up/out your operations performance needs with ease of use and low cost of ownership to meet the demands of bandwidth-intensive applications from small clinics to large hospital datacenters.

Conclusion

The entire healthcare industry is undergoing a dramatic shift designed to enhance the level of care provided to patients. The sensitivity of patient information has created the need for end-to-end security solutions throughout the entire healthcare network – from doctor's offices all the way to the hospital datacenter. Policies and regulations such as Meaningful Use, HIPAA, and HITECH continue to drive the need for security of our patient health information.

Fortinet is the only information security vendor that can address the widest variety of security needs in the healthcare vertical. By providing solutions to address security in hospital, Medical Office Buildings (MOBs), clinics, business associates and satellite offices, Fortinet is in the best position of any vendor to create a secure infrastructure for all aspects of patient care. Fortinet provides an infrastructure with security as the foundation, not an afterthought. With security as the foundation, healthcare organizations can build IT services and applications that meet the requirements of the business and healthcare mandates.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480