"Riverside's doctors and colleagues are continually impressed with our ability to quickly address the latest security challenges using Fortinet."

– Erik Devine
Chief Security Officer
Riverside Healthcare

Riverside Healthcare

RIVERSIDE HEALTHCARE

Introduction

Healthcare providers are migrating from large, independent stand-alone organizations to complex new ecosystems with Provider Organizations, affiliated physician groups, labs, and others involved in both the provisioning of care, and the collection of vast amounts of information from patients. Health Information Exchanges (HIEs) are evolving and more affordable transfer of clinical information and other types of data are increasing. Healthcare, as we know it, is changing quickly.

Besides the changes in coverage and insurance, a variety of technology initiatives are mandated by new regulations. 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 content that needs to be stored and shared, are driving the need for a secure IT platform through which hospitals can support collaboration and information exchange. The network and IT security are now the core components of any healthcare organization.

The move toward 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 – from providers, laboratories, payers, and patients. At some point in the not too distant future, this will include information on diet, purchases and training regimens, as well as results. The more this private

Details

Customer Name: Riverside Healthcare
Industry: Healthcare
Location: Illinois

Business Impact

- Unified protection across 17 facilities
- Centralized administration and monitoring
- Removed throughput and bandwidth constraints
- Facilitated secure, remote access for VPN-SSL users

Deployment

- FortiGates
- FortiAnalyzer
- FortiManager
- FortiMail
- FortiDDOS
- FortiAuthenticator

information is opened to outside entities, the greater the opportunity for malicious content to infiltrate these systems or for pertinent data to be leaked, intentionally or accidentally.

There are healthcare systems that have embraced these new changes. These organizations understand the importance of security and have taken significant steps to ensure that existing systems and campuses can communicate securely while keeping the patient and payee data secure. Riverside Healthcare is one of the organizations ahead of the curve. This paper will show how Riverside Healthcare is using Fortinet technologies to effectively defend the network, and the information residing on networked devices, from a wide variety of threats.

Riverside Healthcare

Riverside Healthcare is a fully integrated healthcare system serving the needs of patients throughout the counties of Kankakee, Iroquois, Will, Grundy, and beyond. Riverside Healthcare is composed of four separate entities:

Riverside Medical Center is located in Kankakee, Illinois, and is part of Riverside HealthCare, a fully integrated healthcare system. Riverside Medical Center is a 312-bed hospital that provides a full scope of inpatient and outpatient care. Riverside is a nationally recognized, award-winning hospital with leading programs in heart care, cancer care, neurosurgery, and orthopedics. It is the area's only Magnet® Recognized hospital and has been named a 100 Top Hospital seven times. Riverside also operates and supports 16 community, primary, and specialty health centers throughout the region.

Riverside Senior Life Communities offer many options for the area's senior population. These include independent living communities, assisted living and state-of-the-art memory care/Alzheimer's communities, skilled and intermediate care nursing, as well as rehabilitation services for short and long-term needs.

Oakside Corporation operates the Riverside Health Fitness Center and also coordinates community counseling programs, pharmacy, health equipment sales and leasing, and home health care.

Riverside Healthcare Foundation raises funds for the health system for use in facility construction and repair, new equipment acquisition, community health care education initiatives, and clinical research.

Riverside Health Fitness Center is a 70,000-square-foot, medically based fitness center owned and operated by Riverside Healthcare. This is a world-class center that reflects Riverside's commitment to improving the health and fitness of the community.

Challenges Faced by Riverside Healthcare

There was a time where disruption was the key goal of hackers, and hospitals were not seen as valuable targets. Cyber criminals in 2016 are no longer interested in causing a nuisance, but use attacks for financial gain. Today a complete medical profile of a individual is worth 10 times that of just a credit card number, making hospitals' data a highly coveted target. Ransomwear has become a rising threat to health care. The threats to healthcare organizations are more complex, and cyber criminals continue to improve their techniques. As threats become more malicious, IT administrators must address the challenges that come from malware entering the network. Unfortunately, there are numerous challenges today that make securing the network a daunting task.

The Requirement to Have More Open Networks

The original model of network security was focused on protecting the network from the outside using firewalls and other traditional security devices. With the popularity of social media applications like Facebook and Twitter and the requirement to provide easy access to data to partners and patients, the potential for an accidental malware incident increases significantly. All it takes is a single click and malware can then exploit vulnerabilities in applications and download malicious programs, such as key loggers, to steal user names and passwords and private data. Unfortunately, the most common applications and file formats are the ones with the greatest chance of exploit.

Increasing Interest in BYOD

Changes in the devices used by employees in the healthcare industry places the endpoint at greater risk. The use of mobile devices – tablets, laptops, and smartphones – is commonplace in the modern hospital, and the need to secure data from the Internet all the way to the endpoint is the key concern today. Mobile employees can increase their productivity and improve patient care by allowing data entry remotely. Mobile connectivity is also a key strategy for many CIOs. CIOs are increasingly interested in implementing mobile applications and wireless connections within

hospitals. Security is a significant concern as these mobile devices connect to the network. The need to protect patient data residing on and being transmitted by these devices will increase in importance.

Maintaining Compliance and Regulations

Embracing new technologies to improve the quality, flow, and safety of patient information is a critical issue for hospitals. Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are helping to guide hospitals in the proper implementation of new technologies. HIPAA was created to guarantee patient protection and privacy. HITECH contains incentives related to healthcare technology and how information is flowed through an infrastructure. It contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers. The adoption of electronic health records is expected to increase the amount of security required under HIPAA and increases the potential legal liability and fees for not remaining within compliance.

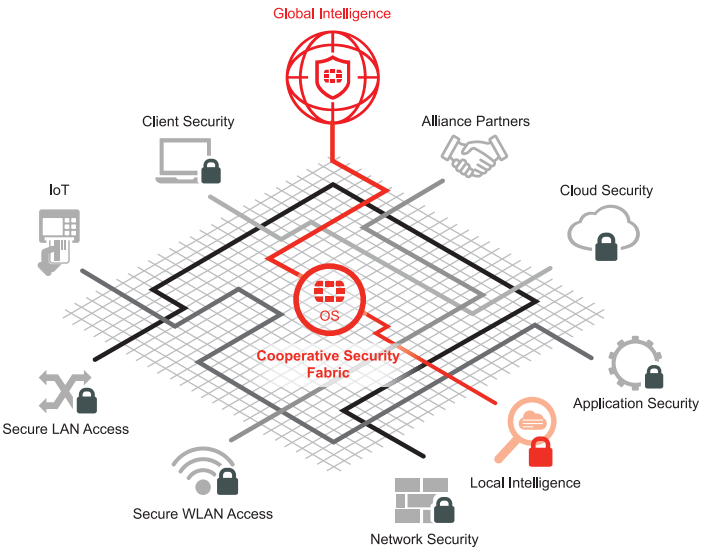
Healthcare organizations are increasingly also subject to other regulatory requirements typically associated with other verticals – requirements such as the Payment Card Industry Data Security Standard (PCI DSS), various National Institute of Standards and Technology (NIST) guidelines, and guidelines from the Food and Drug Administration (FDA).

Increasing Collaboration between Patients, Employees, and Outside Networks

Another challenge within the healthcare industry results from the increased expectation of collaboration from patients, employees, and outside networks. Recent trends in healthcare have led to a proliferation of healthcare content, and modern healthcare depends upon the reliable, rapid, and secure exchange of this information throughout a large healthcare organization. The criticality of this information, and the fact that it needs to be available to different stakeholders throughout the hospital as well as to others in the healthcare value chain outside the hospital, make a shared platform essential to effective hospital operations.

To adhere to evidence-based medicine, information needs to be consolidated from diverse sources such as third-party databases, standard protocols, physician visits, medical imaging data, clinical trials, literature references, transcriptions, prescriptions written, etc. In addition, the information needs to be viewed and vetted by various individuals, including primary care physicians, specialty clinicians, administrative personnel, employers, financial services, and claims processors to collaborate to determine appropriate care protocols, medication administration, and standard operating procedures. There is a need for a collaborative workspace that can enable distributed individuals and teams to work together more efficiently and effectively toward enhancing their existing systems.

In addition to increased information exchange between healthcare providers, there is also an increase in information exchange between hospitals and their patients. The shift toward more preventative care means ongoing monitoring and outreach to push information and treatment out to patients, and to bring information in from patients. Hospitals are using web-based platforms for these interactions, as well as expanding the content they are providing to patients prior to arrival at the hospital, during treatment, and as follow-ups to various procedures or medications that have been provided.



Security Without Compromise at Riverside Healthcare

The role of the network in your business strategy is more important than ever, and ensuring it's both fast and secure is critical to your success. Having the right security woven throughout your network can make the difference between running a smooth, safe network or being the latest security breach news headline.

Fortinet is the only company with security solutions for network, endpoint, application, data center, cloud, and access designed to work together as an integrated and collaborative security fabric. This also means we are the only company that can truly provide you with a powerful, integrated end-to-end security solution across the entire attack surface along any point along the kill chain.

Simply deploying security end to end is not enough. These solutions must work together to form a cooperative fabric, spanning the entire network, linking different security sensors and tools together to collect, coordinate, and respond to any potential threat. And it must do this wherever it occurs, in real time, with no network slowdowns

An Industry-Leading, Next-Generation Firewall

Fortinet firewall technology combines ASIC-accelerated stateful inspection with an arsenal of integrated application security engines to quickly identify and block complex threats.

Intrusion Prevention

Fortinet IPS offers a wide range of features that can be used to monitor and block malicious network activity, including predefined and custom signatures, protocol decoders, out-of-band mode (or one-arm IPS mode), packet logging, and IPS sensors.

Anti-malware/Antivirus

Fortinet antivirus technology combines advanced signature and heuristic detection engines to provide multi-layered, real-time protection against both new and evolving virus, spyware, and other types of malware attacks in web, email, and file transfer traffic. FortiASIC Content Processors, integrated into FortiGate and FortiWiFi products, accelerate both signature scanning and heuristics/anomaly detection for protection against viruses, while delivering performance that scales from entry-level appliances to multi-gigabit core network or data center platforms.

Fortinet's Security Fabric Includes All of the Key Capabilities Your Organization Needs for a Truly Complete Solution:

Scalable: Protects the enterprise from IoT to the cloud

Secure: Global and local threat intelligence and mitigation information is shared between products for faster protection

Aware: The fabric behaves as a single entity regarding policy and logging, enabling end-to-end segmentation for better protection against advanced threats

Actionable: Big data cloud systems correlate threat and network data to deliver real-time, actionable threat intelligence

Open: Well-defined, open APIs allow leading technology partners to become part of the fabric

The Power to Secure Applications

Next to the availability of services, data is the next critical component for healthcare organizations. A loss of data can mean a violation of compliance mandates, the loss of sensitive patient data, and most importantly, the loss of patient trust. Fortinet provides granular protection of an organization's most sensitive data through a variety of controls including:

Application Control

Web 2.0 applications, such as Facebook, Twitter, and Skype are increasing the volume and complexity of network traffic, and expose organizations to a new generation of web-based threats and malware. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard Application Control Database. This allows for the control of more than 2,200 different web-based applications, software programs, network services, and network traffic protocols. FortiGuard Services deliver regularly scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available.

Fortinet provides extremely granular control around these applications. For any recognized application, Fortinet can control access to that application or behavior within the application (for example, chatting within Facebook) and can provide this granular control by user, group, time of day, and numerous other criteria.

Data Loss Prevention

Data loss events continue to increase every year, resulting in fines, penalties, and loss of revenue for companies worldwide. Many data loss events are caused by trusted employees who frequently send sensitive data into untrusted zones, either intentionally or by accident. Fortinet DLP uses sophisticated pattern-matching techniques and user identity to detect and prevent unauthorized communication of sensitive information and files through the network perimeter. Fortinet DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching, and data archiving.

The Power to BYOD

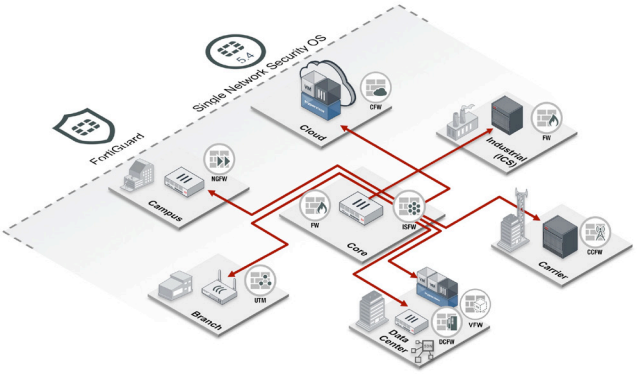
Finally, the mobile client itself is at risk from attack when off the home network. Fortinet secures mobile clients – laptops, smartphones, and tablets – protecting end users while they are travelling or simply working from outside the office. Fortinet has solutions aimed at the endpoint itself that allow for protection of mobile devices and encrypted communications from any location.

Web Content Filtering

Integrated into all FortiGate and FortiWiFi appliances and FortiClient endpoint security agents, Fortinet Web Filtering technology gives the option to explicitly allow websites, or to pass web traffic uninspected both to and from known-good websites in order to accelerate traffic flows. Users can receive real-time updates from FortiGuard Web Filtering Services to determine the category and rating of a specific URL. You can also easily add websites or URLs to the local URL filtering list using both text and regular expressions.

SSL and IPSEC VPN

With the number of threats accelerating, secure communications between enterprise networks, businesses and partners, and corporations and mobile workers is now more important than ever. Data breaches, information leaks, and infected networks and systems are costing corporations and government agencies billions of dollars every year.



"Fortinet has allowed me to address the latest compliance requirements and implement new IT services while lowering costs through consolidation."

– Eric Devine
CSO, Riverside Health

Endpoint Protection

The Fortinet FortiClient endpoint security solutions provide anytime, anywhere endpoint security for network endpoints. When used in connection with FortiGate appliances, FortiClient provides a range of security features to protect the network and ensure policy compliance. Fortinet also has mobile One-Time Password applications available for both Android and iOS to provide strong authentication.

Conclusion

Modern healthcare organizations like Riverside HealthCare are contending with a brave new world of requirements around regulatory compliance and openness. Providing security is not enough to enable these new complex environments. The security vendor must support an ever-changing set of requirements while providing continuous, user-level access controls.

Fortinet's breadth of products, constant security updates, and overall lowered TCO has allowed Riverside HealthCare to securely deliver cutting-edge IT services to its caregivers and patients while ensuring that all information stays secure. Fortinet's ability to provide an end-to-end solution allows Riverside to focus on delivering new and innovative services instead of worrying about its vulnerability to new attacks.

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

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

June 10, 2016