FORTINET

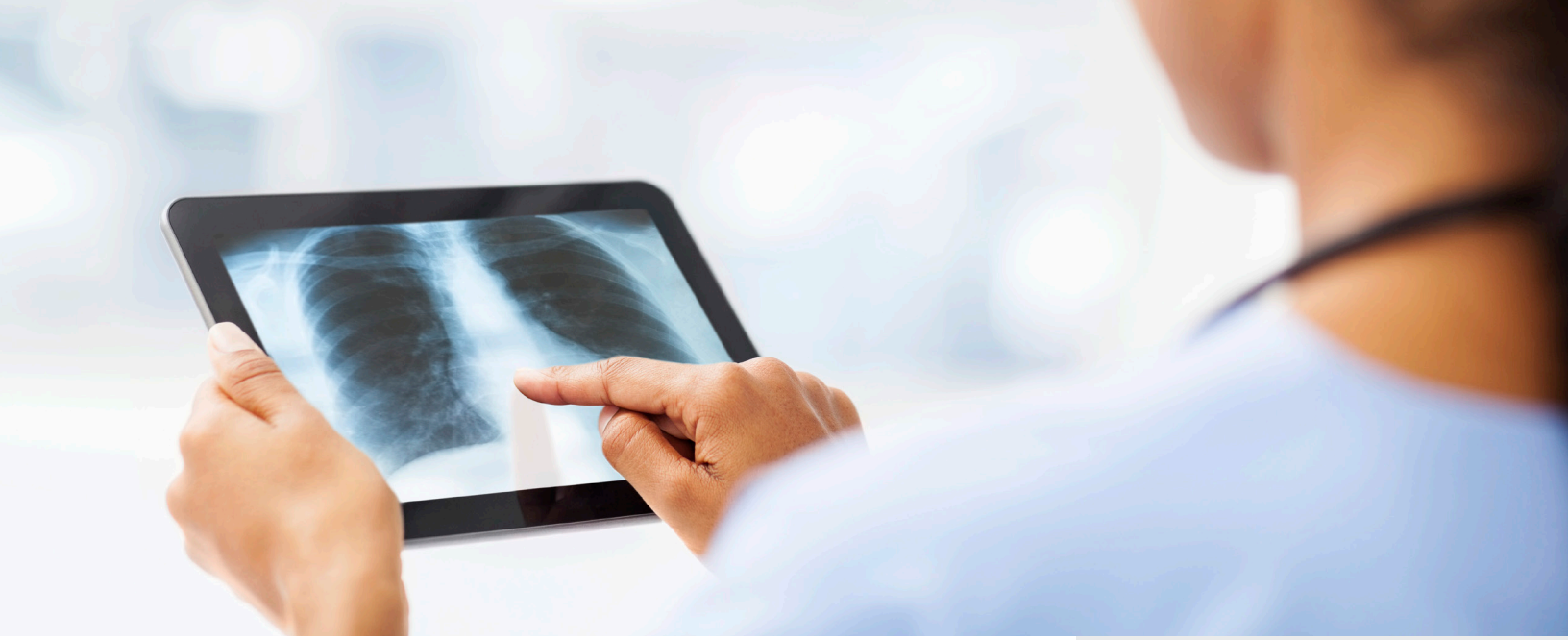
WHITE PAPER

Fortinet Secures Next-Generation Healthcare Enterprise

Get Better Security, More Control, Universal Access, and the Best Performance Available

Fortinet Secures Next-Generation Healthcare Enterprise

Table of Contents



Fortinet Secures Next-Generation Healthcare Enterprise

Introduction

Healthcare is moving to a more distributed model, connecting hospitals with clinics, physician practices, labs, home health, and urgent care centers like never before. With this new distributed model, it is imperative that nurses, doctors, clinicians, and caregivers have seamless, secure access to patient data no matter where they are or what device they use. At the same time, the risk to electronic protected health information (ePHI) has never been greater.

With the many large-scale data breaches in the last few years, it is clear that healthcare is being targeted by cyber criminals. An August 2014 report by the FBI revealed that healthcare records are going for a premium of up to 10 times more than credit card information and a Ponemon study in 2013 found healthcare breaches cost more than in any other industry.

In order to address the new distributed healthcare model and the intensifying threat landscape, hospitals need to change the way they secure systems and networks. With the high risk of storing ePHI and the remote nature of evolving healthcare, the ability to secure a diverse and distributed network is essential. A coordinated approach to security is necessary to close the gaps between systems and better prevent the loss of ePHI.

Protect Sensitive Data, Applications, and Systems While Enabling Secure, Universal Access

In this highly regulated, highly competitive landscape, healthcare organizations constantly face the challenge of maintaining an omnipresent, consistent network across all their locations while also maintaining strong security measures necessary to protect ePHI. To further complicate matters, clinicians need secure, universal access to all of their resources, including clinical and support systems, even from their homes. So it is critical that healthcare organizations have strong security solutions as well as fast, reliable, and accessible networks.

"An August 2014 report by the FBI revealed that healthcare records are going for a premium of up to 10 times more than credit card information."

Safely Allow Patients and Visitors Access to the Hospital's Network

As contradictory as it sounds, healthcare organizations are looking for ways to increase the access patients and visitors have to research information and the Internet on a wide variety of devices. The most obvious security concern with this approach is ensuring that ePHI is kept separate and secured from patient and visitor Internet traffic. It is also critical that patient and visitor traffic does not interfere with critical organizational traffic. This combination of factors requires next-generation security, network segmentation, and wireless management technology, coupled with traffic shaping, to ensure that the ePHI network is secure and always accessible.

Increasingly Stringent Compliance Requirements and Consequences

With the Health Insurance Portability and Accountability Act of 1996 (HIPAA), healthcare organizations are being held to higher standards to secure ePHI more than ever before. The HIPAA Privacy Rules are in place to protect the privacy of individually identifiable health information while the HIPAA Security Rules set the national standards for the security of ePHI. The HIPAA Breach Notification Rule requires covered entities and business associates to provide notification following a breach of unsecured, protected health information.

The 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act expanded breach notification requirements and established the concept of "minimum necessary" access rights. Acceptable security technologies and penalties for failure to comply were also more clearly defined. HITECH gave HIPAA much stronger teeth in both fines and notification requirements, including a description of the incident, when it occurred, what was discovered, the type of information involved, and a description of the investigation and plans to prevent future incidents. When breaches occur, they can permanently scar a healthcare organization's reputation.

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

All the challenges mentioned above require disparate functionality. Fortinet's broad range of integrated security and specialized product lines provide solutions for healthcare environments that are unmatched by any other security vendor. **Figure 1** illustrates how Fortinet solves many of the challenges facing the next-generation healthcare organization.

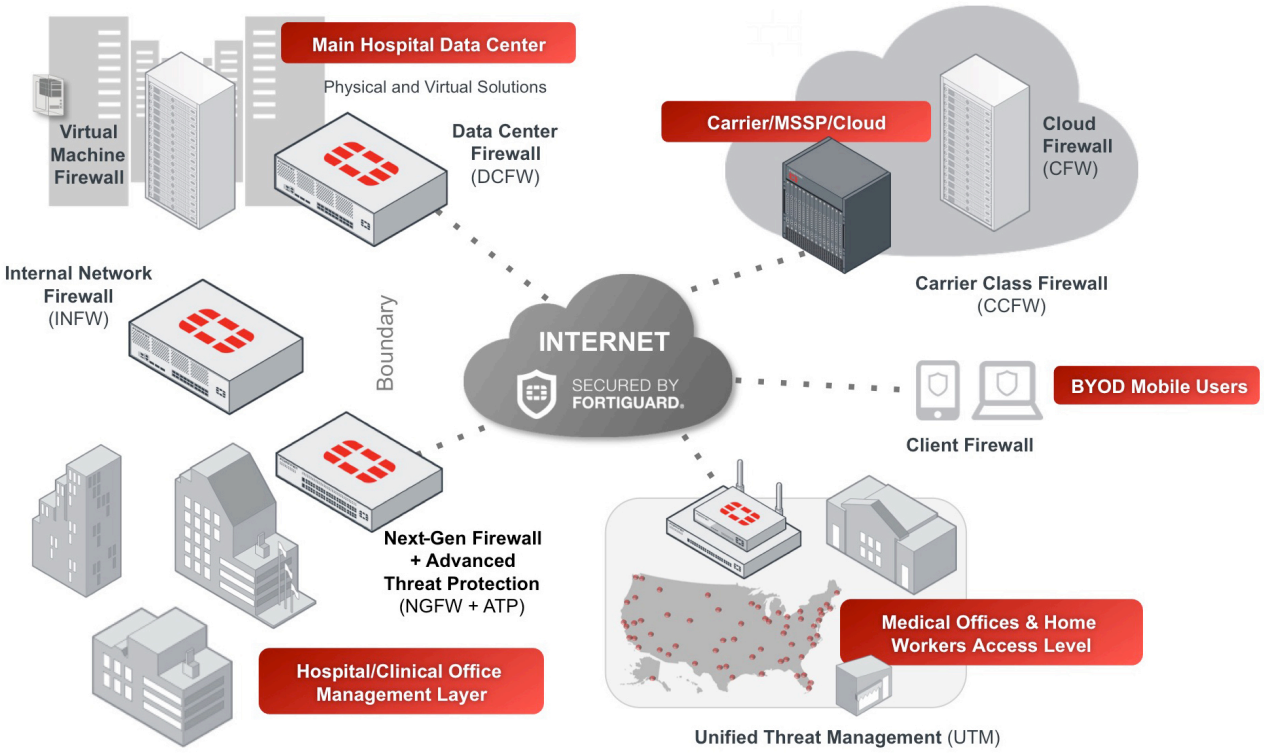


FIGURE 1: FORTINET SECURES ALL LEVELS OF NEXT-GENERATION DISTRIBUTED HEALTHCARE

Main Hospital and Data Center

FortiGate Delivers Unparalleled Security Effectiveness and Control

Fortinet's flagship network security platform delivers industry-leading, integrated next-generation Firewall security capabilities, including: firewall, VPN, IPS, application control, vulnerability management, advanced threat protection, WAN optimization, and many more functions.

Intelligence from FortiGuard Labs delivers unmatched security effectiveness as well as extensive control and visibility of network traffic to the FortiGate firewall. As a result Fortinet IPS, web filtering, antivirus, IP reputation, and advanced threat protection receive top ranking in third-party industry tests – consistently identifying and blocking more threats than security solutions from other vendors. Fortinet data center firewalls, next-generation firewalls, web application firewalls, and breach detection systems (sandboxing) are all NSS Labs Recommended. The Fortinet antivirus engine consistently ranks among the most highly effective in threat blocking in Virus Bulletin and AV Comparatives industry test results.

Control and visibility are core to an effective next-generation security solution. A Fortinet solution enables organizations to identify and enforce security policies on more applications and more types of users than other NGFW solutions on the market. It is the only NGFW able to identify and apply policies based on the type of end-user device being used. Organizations also get unprecedented visibility into how popular cloud-based applications are being used, such as details on the files being transferred to and from cloud file storage services or what videos are being watched and by whom.

FortiGate Delivers Unparalleled Performance

Hospital data centers handle very large volumes of traffic, and core resource-intensive security functions are often implemented here. These data centers must have a security solution that can protect as well as deliver high throughput speeds. Fortinet's high-performance appliances and chassis-based FortiGate hardware platforms are based on the Optimum Path Processing architecture of the FortiOS operating system and leverage custom high-speed ASICs to deliver industry-leading performance. With multiple 10 Gbps, 40 Gbps, or even 100 Gbps interfaces and speeds up 1 Tbps, FortiGate provides high performance security without introducing latency into the network.

Below are several models of FortiGate platforms often used in healthcare customers' data centers.

FortiGate 5000 Series

The FortiGate 5000 series chassis platforms deliver very high performance and connectivity options optimized for service providers and large data centers. Their native 10 GbE support and highly flexible AdvancedTCA™ (ATCA)-compliant architecture protect large, complex networks, including multitenant, cloud-based security-as-a-service and infrastructure-as-a-service environments.

FortiGate 3000 Series

The FortiGate 3000 series of network security appliances brings security to the 40 GbE and 100 GbE backbone. High port density 40 GbE ports and 10 GbE ports provide security and connectivity for all but the largest data centers. The FortiGate 3810D even supplies four 100 GbE ports suitable for Internet2 and the largest network backbones, while the 3200D comes with forty-eight 10 GbE ports, making it perfect for internal network segmentation at high speed and minimal latency. The 3000 series offers unmatched performance, flexibility, and security for your large enterprise or service provider networks.

FortiGate 1000 Series

The very popular FortiGate 1000 series integrates network and security functions into 2RU appliances to help identify and thwart multiple threats for mid-sized organizations and large branch offices or clinics. With numerous accelerated multithread security interfaces, organizations can create multiple security zones for various departments, users, access methods, and even devices to enforce network security at accelerated speeds.

FortiGate 100-500 Series

These 1RU rack-mountable FortiGate appliances come in a variety of ports, speeds, options, and configurations to fit any size clinic, hospital, or small data center. With high port density, available Power Over Ethernet (PoE), available internal hardware switch, and advanced network processor and content processor ASICs, these small appliances provide enterprise-level security and functionality at the clinic level.

Next-Generation Firewall Management

Given the widely distributed nature of modern healthcare organizations, the ability to quickly modify and manage security appliances is essential. In addition to the extensive, easy-to-use management that comes with every FortiGate, Fortinet offers centralized control and visibility with FortiManager and FortiAnalyzer appliances to help healthcare systems manage their distributed environments and provide centralized logging and reporting.

FortiManager

Organizations can centrally manage all their FortiGate, FortiWiFi, FortiMail, and FortiAnalyzer appliances and virtual appliances, as well as FortiClient endpoint security agents, in this "Single-pane-of-glass" management console. FortiManager is highly scalable and able to manage up to several thousand devices. You can further simplify control and management of large deployments by grouping devices and agents into administrative domains (ADOMs). Scripting and API modules allow for advanced management options.

FortiAnalyzer

Organizations get extensive visibility into the state of their network security with FortiAnalyzer centralized logging, analysis, and reporting capabilities. A comprehensive suite of easily customized reports enables you to analyze, report, and archive security event, network traffic, web content, and messaging data to measure policy compliance from Fortinet devices and other syslog-compatible devices.

Distributed Medical Offices & Home Workers

The individual hospital/clinic level requires security and connectivity for a wide variety of functions including WiFi, voice, and traditional network connectivity. With the ever-dropping costs of bandwidth and the explosion of web-based applications, security needs to be pushed beyond the core. By providing full Unified Threat Management (UTM) security, wireless access, voice systems, and networking at every location, application and web performance is improved, for employees as well as patients/visitors, and only critical clinical functions are pushed over the VPN or WAN circuits to the central data centers. Fortinet products including FortiGate, FortiWiFi, FortiSwitch, FortiVoice, and FortiAP wireless access points provide all the components needed for a next-generation hospital/clinic to operate in a secure manner while still offering an enhanced patient/visitor experience.

FortiGate/FortiWiFi 60-90 Series

The FortiGate/FortiWiFi 60 series security appliances deliver comprehensive enterprise-class protection for smaller locations, medical offices, customer premise equipment (CPE), and hospital networks. An integrated set of essential NGFW and UTM security technologies protects all of your ePHI. Simple per-device pricing, 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.

FortiVoice

FortiVoice products give you complete control of your telephone communications. Easy to use, affordable and reliable, FortiVoice phone systems and phones deliver everything you need to handle calls professionally, control communication costs, and stay connected everywhere. VOIP PBX functionality can operate independently or tie back to the central data center PBX.

BYOD Mobile Users

As your locations extend access to employees 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 WiFi, web filtering, rate limiting, and load balancing.

FortiAP

Wireless access point FortiAP solutions provide increased visibility and policy enforcement capabilities while simplifying your overall network environment. They employ the latest 802.11ac-based wireless chip technology, offering a high-performance wireless access point with integrated wireless monitoring and support for multiple SSIDs on each radio. FortiAP solutions work in conjunction with the feature-rich family of FortiGate controllers to provide a fortified wireless space that delivers complete content protection. FortiGate or FortiCloud controllers centrally manage radio operation, channel assignment, and transmit power, which further simplifies your deployment and management requirements.

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 data centers.

Advanced Threat Protection

With healthcare as a primary target for cyber criminals, advanced threat protection is key. Effectively and efficiently protecting your organization against advanced threats requires multiple types of security technologies working together in an integrated system to prevent, detect, and mitigate attacks.

Prevent Attacks from Ever Penetrating Your Organization

Prevent the attack by reducing the attack surface while inspecting and blocking known threats with VPN, user authentication, network access control, SSL inspection, application controls, IPS, antivirus, anti-spam, IP reputation, and web filtering. These technologies, powered by security intelligence from FortiGuard Labs, are available through the FortiGate, FortiMail, FortiClient, and other Fortinet platforms.

Detect Zero Day and Unknown Threats Fast with FortiSandbox

Detect unknown threats, assess behavior, and identify trends with FortiSandbox. By using a sandbox that integrates with FortiGate, FortiMail, and FortiGuard Labs, organizations get more efficient, faster, and more effective advanced threat protection. FortiSandbox gets suspicious and malicious threats to expose themselves by examining their behavior in a secure environment and shares newly gained threat intelligence with the extended Fortinet ecosystem. FortiSandbox is available as an on-premise or cloud solution for very flexible deployment options.

Mitigate Attacks

Integrated FortiSandbox results quickly inform FortiGate and FortiMail making it easy to quickly quarantine potentially infected networked devices and block emails containing advanced threats. FortiGuard Labs powers a continually improving ecosystem of protection by investigating and analyzing new sandbox findings and creating security updates to protect against the latest advanced threats.

Conclusion

The next-generation distributed healthcare organization will depend on a seamless environment that encourages patient interaction through mobile devices and applications while maintaining and protecting ePHI. Providing this environment will require a solution that operates from the perspective of security first, while still delivering high-speed performance and universal access. Any misstep in providing a secure environment will have a direct effect on public trust and patient satisfaction.

With our expansive product line and security foundation, Fortinet products can deliver the capabilities needed by healthcare organizations as they advance past traditional closed network architecture to provide the flexibility, reliability, performance, and security that a modern distributed healthcare organization needs today.

About Fortinet

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 pure-play 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 fortinet.com/healthcare and Twitter: @FortinetHealth.

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

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

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 11, 2015