FORTINET

SECURE PATIENT CARE STARTS WITH FORTINET

WHITE PAPER

"Fortinet really understood the Halifax Health mission. In addition to performance and protection we needed to have a product that met our financial needs, and Fortinet did that."

- Tom Stafford, Chief Information Officer, Halifax Health

80% **PROVIDERS ADMITTED A "SIGNIFICANT SECURITY INCIDENT"**

2016 HIMSS CYBERSECURITY SURVEY

MOST WORRISOME CYBER-ATTACKS FOR HEALTHCARE ADMINISTRATORS:

- Denial of Service
- Malware
- Ransomware
- Phishing

PONEMON INSTITUTE, MAY 2016

INTRODUCTION

Recent high-profile attacks on healthcare organizations ranging from large hospitals to major insurance providers have highlighted the need for security that goes far beyond ticking boxes for HIPAA compliance. Patient health records have much higher value on the black market than credit cards and other financial data, making health providers a prime target for cybercriminals, while our growing reliance on electronic health records and connected medical devices provides a nearly unparalleled attack surface.

Unfortunately, too many healthcare organizations have chronically underinvested in IT security measures to protect critical systems and data, leaving them far more vulnerable than their peers in other industries like finance where security has been a top business and regulatory priority for years.

It's time to change the way we approach security in healthcare. Read on to find out more about both immediate and emerging vulnerabilities and why secure healthcare begins with Fortinet.

WHY IS HEALTHCARE A TARGET?

PHI – HIGH VALUE, HIGH STAKES

For years, cybercriminals focused their efforts on retail and financial targets. Yet as credit card companies and banks implemented increasingly sophisticated systems for detecting fraud and dealing with data breaches, hackers have begun to turn their attention to healthcare and Protected Health Information (PHI). Consider this scenario: If a credit card number is stolen, algorithms quickly identify fraudulent charges and automatically close the account. The credit card holder is issued a new card and, after some brief inconvenience, goes on about his or her life.

Medical records, however, are a rich source of more complete personal profiles, providing cybercriminals with a wealth of information that can be used for identity theft and fraud for far longer before its use is discovered. As we have seen with recent breaches, medical records can include social security numbers, addresses, medical claims data, and more. This is why medical records are worth ten times more than credit card numbers on the black market.

The payoff for those who can breach healthcare databases is very high. At the same time, the stakes are quite high for healthcare organizations, with substantial penalties for violations of HIPAA regulations and Omnibus rules and the potential for devastating brand damage with customers and patients.

THE THREE VECTORS OF A HEALTHCARE CYBER ATTACK

Would-be cybercriminals are also finding that healthcare is a fairly easy target. Not only do many organizations lack proper security capabilities, but three major vectors have emerged that provide a very large attack surface.

1. Traditional malware and cyberattacks like those experienced by businesses in every industry provide the first inroad for hackers. Sophisticated phishing schemes, DDoS, ransomware, and many other types of attacks have all hit healthcare organizations. The big difference, though, is that many of these organizations lack the security to effectively mitigate these threats.

2. Connected medical devices represent the second vector. The number of possible targets is growing rapidly as hospitals

move to connect increasing numbers of devices to their networks for monitoring and automation. Unfortunately, these devices are generally not designed for security and researchers have already demonstrated how they can be exploited to either gain access to health information systems or even physically harm patients.

3. Personal and home health devices, also known as transformed care, are a new frontier in medicine. They promise increased access to care using mobile devices, wearables, and purpose-built devices for telemedicine and remote health monitoring. But many of these devices and applications are being built for function and convenience rather than security and can provide hackers with largely unfettered access to the centralized health systems to which they are connected.

A PERFECT STORM FOR HEALTHCARE SECURITY

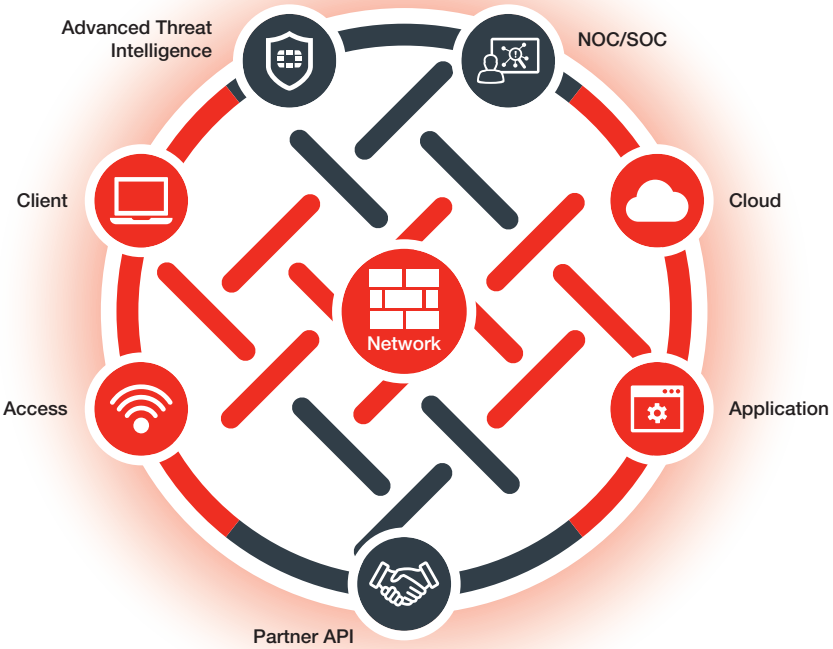
All of this represents a perfect storm for healthcare security. The presence of high-value information, a large and varied attack surface, and vulnerable applications and systems all come together to make healthcare an ideal target.

WHY FORTINET?

Fortinet offers a complete ecosystem of security products that can meet the needs of the smallest doctor's office or the largest health insurer's data center. Our solutions span today's most data-intensive industries, including government, healthcare, financial services, and education. Seven of the top ten US healthcare systems have chosen Fortinet, as have seven of the top ten Big Pharma companies. And as these fields continue to evolve at a feverish pace, companies are increasingly looking to Fortinet as an experienced, leading-edge security partner.

SECURITY FABRIC

Many healthcare organizations have cobbled together point security solutions to meet their growing security needs – but this increases network and management complexity, and creates additional security vulnerabilities. To combat this, Fortinet offers a simplified, integrated security stack with a single management interface – a security fabric. In many cases, security functions can be handled by a single device. As healthcare organizations scale, they can add specialized hardware and additional appliances, but maintain their single-pane visibility into their network security. With Fortinet Security Fabric, healthcare organizations gain consolidated, ubiquitous protection across the enterprise.



NEXT-GENERATION DISTRIBUTED HEALTHCARE

In healthcare, the stakes have never been so high – or the vulnerabilities so numerous. Fortinet's next-generation firewalls (NGFWs) are sophisticated evolutions of time-tested technologies, and they are ideally suited for hospital data center and clinical deployments. In addition, easy-to-use unified threat management (UTM) appliances and secure wireless access points can safely connect distributed offices to hospitals, insurers, and other providers simply and cost-effectively.

INTELLIGENT NETWORK SEGMENTATION

Once attackers breach healthcare networks, they often find them very flat and ripe for lateral movement among servers and applications. Internal segmentation firewalls (ISFWs) are specially adapted for the performance needs inside a network and closer to data center cores, providing intelligent segmentation and additional layers of security. In healthcare settings, critical medical devices and patient data can be placed behind ISFWs to ensure that even if breaches do occur or are staged by actors with network access, threats can be detected, quarantined, and mitigated far faster than with edge protection alone.

ADVANCED THREAT PROTECTION

Fortinet also offers a complete advanced threat protection (ATP) framework that includes sophisticated sandboxing technologies. Sandboxes allow new and previously undetected threats to be tested in a safe environment and then immediately rejected if they are found to be malicious. The resulting threat intelligence is fed back into the framework, providing high performance balanced with outstanding detection capabilities, even for zero days, regardless of the vector or type of attack.

UNMATCHED PERFORMANCE

No matter what their security needs, healthcare providers don't need to compromise security in the name of application and network performance. Fortinet appliances, from next-generation firewalls to sandboxes for advanced threat protection use state-of-the-art ASICs (application-specific integrated circuits) to deliver unmatched performance. Even when a single appliance is delivering a wide range of security functions, healthcare organizations can be assured that clinical workflow will not be disrupted.

FORTIGUARD THREAT RESEARCH AND RESPONSE

Healthcare organizations usually don't have the time or resources to stay on top of every evolving threat. That's why Fortinet employs a large team of researchers that make up FortiGuard Labs – a trusted third-party organization that has the capacity to provide near real-time protection against advanced threats. Our award-winning team combs through a constant stream of data from sensors and hardware worldwide, tracking the latest threat intelligence and conducting original research every day. All of this information is fed back into every Fortinet appliance to provide up-to-the-minute protection from zero days, botnets, viruses, and exploits.

TOP-RANKED RESULTS IN THIRD-PARTY INDUSTRY TESTS

Independent, third-party tests are a critical measure of the quality of a solution. Fortinet Firewall, Next Generation Firewall, Breach Detection System (sandbox), and Web Application Firewall solutions are "Recommended" for security effectiveness and performance value by NSS Labs, the only information security research analyst firm backed by a testing laboratory. Core security technologies from FortiGuard Labs including anti-malware, antiphishing, and antispam consistently receive very high effectiveness scores in Virus Bulletin and AV Comparatives testing. Fortinet solutions are certified by the largest number of third-party independent tests including NSS Labs, ICSA, Virus Bulletin, AV Comparatives, Common Criteria, FIPS, and more.

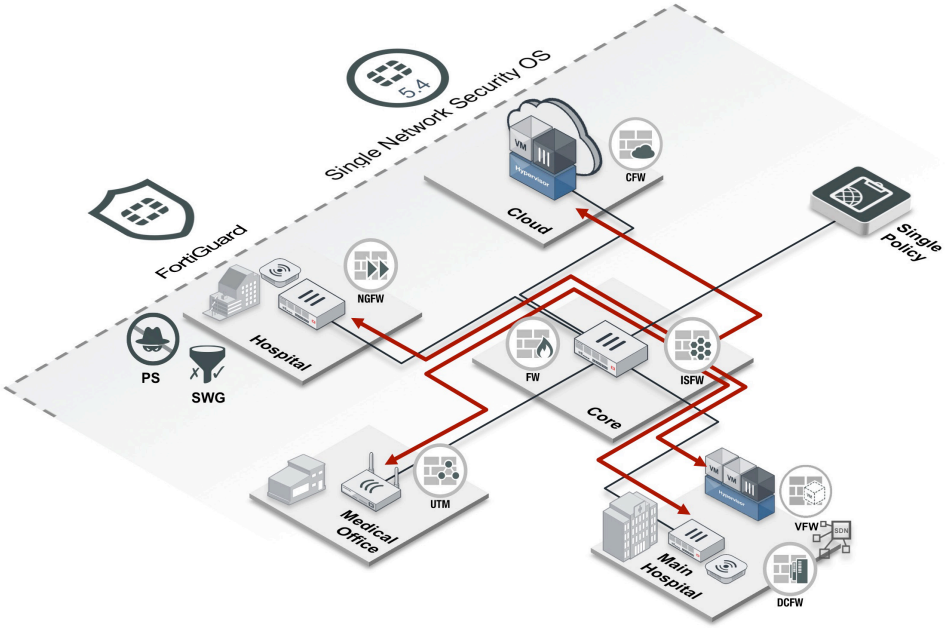
FORTINET – THE PRESCRIPTION FOR SECURE PATIENT CARE

FORTINET HEALTHCARE REFERENCE ARCHITECTURE

So what does all of this look like in the real world? Fortinet partners can design security systems to meet the needs of any healthcare organization, but the diagram below demonstrates how the Fortinet ecosystem can connect and secure the many moving parts in a healthcare setting.

CONCLUSION

Fortinet is well positioned to meet the varied and critical security needs of healthcare organizations worldwide. With products that offer industry-leading security effectiveness, scale to any size, and deliver third-party validated, unmatched performance, Fortinet network security solutions ensure that healthcare institutions never have to choose between patient care and security. Contact your Fortinet partner today to learn how you can not only meet regulatory requirements but also ensure the safety of every patient's medical record, all while embracing new approaches to healthcare delivery and management. For more information visit www.fortinet.com/healthcare or join the conversation on 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
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

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

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Dec 27, 2016