FORTINET

INTELLIGENT SEGMENTATION FOR THE HEALTHCARE INDUSTRY

WHITE PAPER

INTELLIGENT SEGMENTATION FOR THE HEALTHCARE INDUSTRY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Healthcare CISOs face a complex set of challenges as they seek to support digital transformation while protecting critical patient information and proprietary medical research and complying with shifting regulations and standards. As the healthcare network attack surface expands and the sophistication of cyber threats increases, the security skills needed to deal with threats remain in short supply. Intelligent segmentation technologies that share and apply real-time threat information across an integrated security architecture can address these problems. The Fortinet Security Fabric includes internal segmentation firewalls (ISFWs) and network access controls (NACs) to keep sensitive data safe while enabling dynamic access for supporting agile medical services and optimal network productivity.

INTRODUCTION

As guardians of the most highly sought-after data asset on the black market, healthcare providers, insurers, and other supporting entities have a critical responsibility to protect patient data. Protected health information (PHI) can be used to build exceptionally rich personal profiles, enabling identity theft, cyber espionage, and even extortion. On the black market, the going rate for a credit card number is worth 25 cents; however, an electronic health record (EHR) can be worth hundreds or even thousands of dollars.[1]

The value of private medical data that is stored and communicated places patients and providers at risk. At the same time, researchers, pharmaceutical companies, and device manufacturers are finding their intellectual property increasingly at risk, not just from competitors but also from attackers in a variety of nation-states, where drug counterfeiting is rampant.

Within the healthcare industry, a successful cyberattack can:

- Disrupt operations and critical services that impact patient care
- Cost organizations millions in lost revenue and patient compensation[3]
- Permanently damage brand reputation and consumer trust
- Carry significant costs for patients—financially and in terms of safety and privacy
- Result in substantial penalties under Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act regulations[4]

As if the weight of these consequences weren't enough, the current evolution of healthcare business models and associated technologies has exposed new vulnerabilities for cyber criminals to exploit. As organizations apply new technologies to facilitate better patient care, the constant influx of new medical mobile applications, medical devices, and increased dependency on cloud-based computing is demanding a more vigilant assessment of a constantly changing network security posture.

Healthcare organizations have the highest costs associated with data breaches at **$408 per lost or stolen record**—nearly three times higher than the cross-industry average ($148). The associated costs of a major healthcare breach can be as high as **$350 million.**[2]

WHAT'S HAPPENING IN HEALTHCARE

Digital transformation is making healthcare organizations increasingly distributed through adoption of next-generation technologies. Providers are accommodating their patients' busy schedules through off-site services such as minute clinics, telemedicine events, or secure text consultations. Cloud-connected wearables and implanted medical devices deliver better care to patients and help them avoid unnecessary office visits through remote monitoring capabilities. In this new era, nurses, doctors, and caregivers require seamless and secure access to patient data—no matter where they are or what device they're using.

And while these organizational and operational changes offer many benefits in terms of quality of care to patients, they simultaneously impact the healthcare attack surface. Distributed networks that lack a well-defined network boundary are harder to defend. New security vulnerabilities have been exposed by a number of intersecting factors, such as:

M&A ACTIVITY

Driven by financial pressures to reduce operational costs and the need to expand clinical service portfolios, mergers and acquisitions (M&A) activity in the healthcare sector is gaining momentum. For the next-generation distributed healthcare enterprise that heavily relies on collaboration across disparate users and departments, this makes it increasingly difficult to protect data, applications, users, and the network. Integration of IT and medical technologies and the need to share information between newly merged organizations creates new vulnerabilities. These extend from rapid system interoperability demands and diluted visibility due to a multitude of point solutions—a dynamic that has not gone unnoticed by cyber criminals.

45% of ransomware attacks last year targeted healthcare organizations[5]

56% of healthcare breaches come from internal threat actors[6]

78% of healthcare employees showed some lack of preparedness with common privacy and security threat scenarios[7]

It takes an average of **308 days** for a healthcare organization to discover a breach[8]

ADOPTION OF SMART DEVICES

Connected medical devices not only transmit sensitive information to EHR systems but are often used to automate patient care. The Internet of Things (IoT) now comprises two of the top 10 application vulnerability exploits in healthcare.[9] As healthcare organizations add more IoT and Internet of Medical Things (IoMT) devices to their environments, this expanded attack surface adds more complexity while increasing the threat posture. With compromised IoT devices now capable of exploiting multiple vulnerabilities at the same time, this upward trend is likely to spread to IoMT devices as well,[10] especially considering the explosive growth of IoMT (26.2% compound annual rate through 2021[11]).

ENCRYPTION AND INSPECTION

While encryption protects sensitive data moving across the network, it also increases the need to inspect both inbound and outbound traffic. Cyber criminals use encryption to hide malware and exploits as well as to mask stolen data being exfiltrated from the network. Constant inspection of encrypted traffic carries a high processing cost, and many firewalls suffer degraded performance as a result.

EXPANDING THREAT LANDSCAPE

Traditional cybersecurity attacks use malware, phishing schemes, Trojans, ransomware, and embedded email links to exploit PHI and other critical data from healthcare enterprises. This proliferation of polymorphic attack vectors is impacting healthcare at higher rates than other verticals. On average, healthcare organizations experience more than double the attacks that businesses in other vertical market categories experience.[12]

Rising attack volumes are partially driven by increasing threat velocity and variety. The number of malware families increased by an alarming 25% in Q4 2017, and unique malware variants are growing at an annual rate of 19%.[13] This combination of rapid development and the increased propagation of new variants is successfully catching organizations unprepared.

To meet the challenges of digitally transformed healthcare networks, security leaders need a next-generation security strategy. This means deploying an integrated security architecture that shares intelligence across the distributed organization. And it means using best-of-breed controls like segmentation within that architecture to protect sensitive healthcare data and IP.

WHY SEGMENTATION

Agile network technologies can help control access within healthcare environments through dynamic network segmentation and potential quarantine of affected systems.

Healthcare organizations must be able to perform macro-segmentation to separate both physical domains (e.g., laboratories, clinics, pharmacies) and functional domains (e.g., facilities management, billing, radiology).

But this alone is not enough. There is also a wide variety of different users with numerous unsecured and often personal devices within each domain. In U.S. hospitals, there may be as many as 15 connected devices per bed.[14] To securely support the use of such devices requires enforcing access policies for all users and connected devices.

ISFWs were developed in response to a growing awareness that network threats are no longer just coming from outside attackers attempting to breach perimeter defenses like next-generation firewalls (NGFWs). Healthcare networks are subject to an extraordinary number of internal threats as well. Traditionally flat and open network topologies make it easy for threats to move laterally (east to west), seeking out resources to plunder once they're inside.

Without proper segmentation, ransomware attacks (e.g., WannaCry) can easily propagate across the network, making recovery much more difficult to implement. Segmentation enables proactive and dynamic isolation of an attack, which limits its ability to spread.

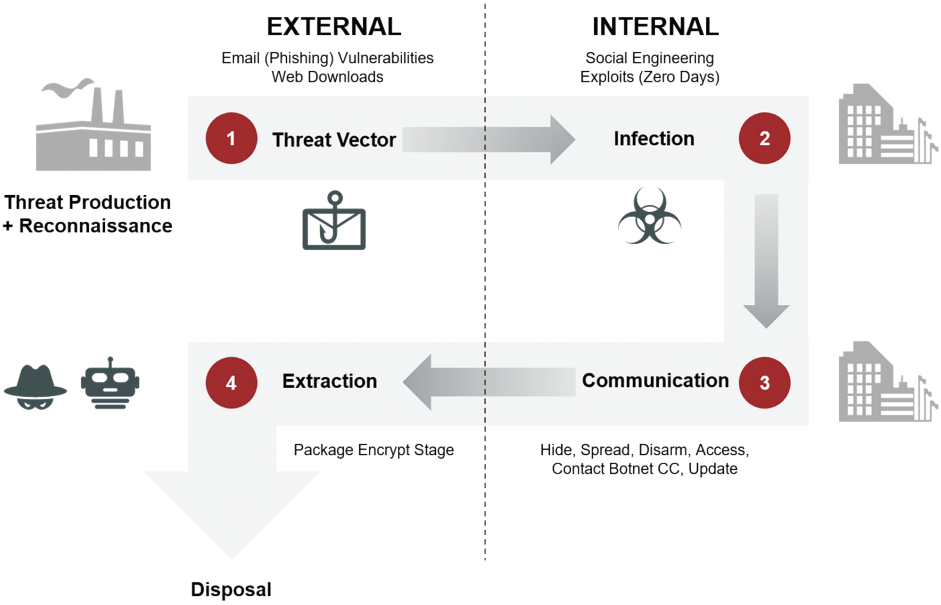

FIGURE 1: ADVANCED THREAT LIFE CYCLE.

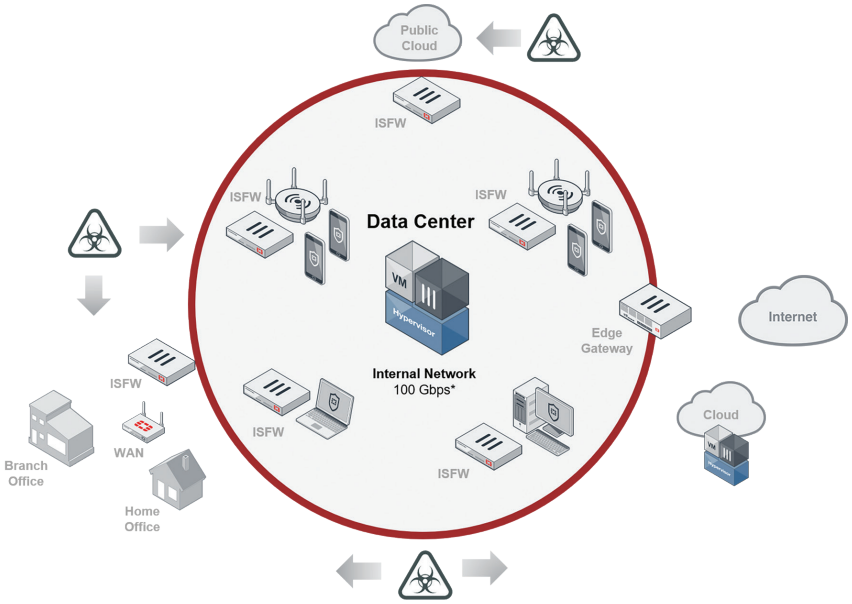

FIGURE 2: ISFWS CAN BE FLEXIBLY DEPLOYED TO PROTECT A VARIETY OF RESOURCES INTEGRAL TO A NETWORK INSTEAD OF RELYING EXCLUSIVELY ON PROTECTION AT THE GATEWAY.

Because they operate inside networks instead of at the edge (Figure 2), ISFWs can prioritize assets that need the highest degrees of protection and monitoring without impacting performance. By enabling segmentation controls from end to end across the security architecture, ISFWs dramatically improve visibility into possible attacks. They can provide complete internal segregation of data and resources to comply with regulatory requirements and to better meet the complex security needs of healthcare organizations. Most importantly, shared intelligence enabled across security environments leads to better efficiencies in identifying, and in some cases, auto-remediating threats.

HOW AN ISFW WORKS

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 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

MANAGING UNSECURED IoMT DEVICES

Many IoMT devices are headless and cannot be updated to protect against new vulnerabilities—including multivector attacks. Traditional security approaches cannot protect them. However, segmentation enables organizations to institute checks and policies at various points of the network to control users, applications, and data flow. It also gives organizations the ability to identify and isolate a potentially compromised device before it can do damage or spread to additional segments of the network. This is particularly important in healthcare, where it takes an average of 308 days for an organization to discover it experienced a breach.[15]

NETWORK ACCESS CONTROL (NAC)

To increase visibility of potential risk, healthcare organizations must implement even more granular access control across the integrated security solutions in the architecture. NAC settings can be based on roles, device type, time of day, location, and other device attributes. It is important that both macro- and micro-level segmentation can be adjusted dynamically to support reorganization, expansion, and changes in policies when devices on the network have high risk or unknown security postures.

WHY FORTINET

Part of the integrated Fortinet Security Fabric, FortiGate ISFWs are specially adapted for the performance needs of the internal network, providing intelligent segmentation and additional layers of security. Critical data, such as medical devices or EMRs, can be placed behind ISFWs to ensure threats are detected and mitigated faster than with edge protection alone, even when breaches occur or are staged by actors with network access.

SECURING IoMT DEVICES

To stop IoMT-targeted threats, the Fortinet Security Fabric shares threat intelligence across an integrated architecture of security solutions capable of providing visibility, segmentation, and synchronized protection throughout the entire infrastructure—on-premises, in the cloud, and on and through IoMT devices. FortiGate ISFWs provide visibility of everything connected to the network due to the ability to learn and profile all devices attaching and communicating via the network. IoMT devices can be authenticated and classified to build a risk profile, then sorted into policy-driven groups based on their risk profiles.

FortiGate ISFWs apply security policies based on device type and network access requirements. Policy-driven device groups and internal network segmentation enable monitoring, inspection, and policy enforcement based on the activity at various points within the infrastructure. To contain threats, compromised devices can be quarantined and remediated at multiple points within the network, ensuring the malicious traffic does not reach critical systems or data.

CLOUD SEGMENTATION

Agility is one of the main reasons healthcare customers choose cloud-based solutions. With agility, however, comes a state of constant change in terms of the services, applications, and resources they need. Fortinet dynamic network segmentation protects application traffic within and across vendors, cloud platforms, and applications—even as workloads and environments shift.

Fortinet segments application and data migration between clouds in multi-cloud environments. Using microsegmentation, FortiGate security nodes protect east-west migration of threats while still being able to keep up with modern performance demands. FortiGate ISFWs also inspect persistent traffic between cloud segments to protect against data loss and to make sure that data is routed based on risk and policy. Additionally, FortiGate ISFWs provide out-of-the-box automation and orchestration of intelligent segmentation for all of the leading public cloud platforms.

DYNAMIC NETWORK ACCESS CONTROL

The Fortinet FortiNAC network access control solution extends segmentation even further by configuring third-party network devices to implement segmentation policies. Security Fabric integration allows FortiNAC to assign segmentation policies and change configurations on switches and wireless products, including solutions from more than 70 different vendors. These dynamic controls extend the reach of the Security Fabric in heterogeneous environments.

COMPLIANCE

Network demarcation and segmentation are 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. FortiGate ISFWs are a natural extension of regulatory security efforts. Because they can be deployed in-line, network administrators gain unprecedented control and visibility to improve compliance with no appreciable impact on performance or usability issues.

USE CASES

For healthcare in particular, there are several key use cases for the intelligent segmentation capabilities provided by the Fortinet Security Fabric and FortiGate ISFWs:

IN THE DATA CENTER

Cloud-based EHR providers bear considerable burdens securing their data centers to provide reliable, safe services to their customers. FortiGate 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. FortiGate ISFWs 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 be impractical, too disruptive, or too expensive to undertake. Fortinet Security Fabric segmentation capabilities can protect these systems, keeping them in their own secured network zone. Yet, at the same time, they still allow unfettered access by clinicians and the health information systems into which they feed data.

IN THE CLINIC

Connected medical devices have dangerous vulnerabilities that bad actors can exploit in a number of ways—from ransomware attacks, to the theft of confidential patient records, to operational or device outages that put patient lives at risk. As IoMT products proliferate and age, it is critical that organizations secure them at the device level and not to the network level. Placing a FortiGate ISFW in-line with IoMT devices provides levels of security that often are not built into those devices.

At the same time, FortiNAC enforces granular policy-based controls that extend segmentation for any and all smart devices across the extended organization. In addition, FortiGate NGFWs include Fortinet SD-WAN, which extends both networking and security functionality to distributed healthcare organizations with multiple branch offices and/or remote sites.

FOR THE PAYER

Many insurance companies have come under fire for inadequately securing patient data. FortiGate NGFWs allow payers to isolate patient data stores without interfering with existing transactional systems. Again, the in-line, transparent nature of ISFWs make them ideal choices for rapid, nondisruptive deployment.

FOR THE OUTSIDE ENTITY

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

INTELLIGENT SEGMENTATION HELPS SECURE DISTRIBUTED HEALTHCARE

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. At the same time, the threat landscape is only getting more complex for medical organizations—with IoMT devices, EHR, and clinician demands for intelligent tools placing greater strain on already stretched IT security resources.

The Fortinet Security Fabric integrates a complete ecosystem of security tools that provide the required protection, segregation, and segmentation for patient data and critical healthcare systems. New ISFWs fill the gap, securing networks against internal threats and offering flexible architectures uniquely suited to healthcare environments.

[1] Mariya Yao, "Your Electronic Medical Records Could Be Worth $1000 To Hackers," Forbes, April 14, 2017.
[2] Heather Landi, "Healthcare Data Breach Costs Remain Highest at $408 Per Record," Healthcare Informatics, July 13, 2018.
[3] Heather Landi, "Healthcare Data Breach Costs Remain Highest at $408 Per Record," Healthcare Informatics, July 13, 2018.
[4] "Healthcare Data Breach Statistics," HIPAA Journal, March 20, 2018.
[5] Mike Duffy, "The 3 most important security statistics healthcare organizations need to know," Becker's Hospital Review, March 7, 2018.
[6] "2018 Breach Data Investigations Report," Verizon, April 10, 2018.
[7] Elizabeth Snell, "78% of Healthcare Workers Lack Data Privacy, Security Preparedness," Health IT Security, February 6, 2018.
[8] Heather Landi, "2017 Breach Report: 477 Breaches, 5.6M Patient Records Affected," Healthcare Informatics, January 23, 2018.
[9] Ladi Adefala, "Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries," Fortinet, March 6, 2018.
[10] "Q4 2017 Threat Landscape Report," Fortinet, February 2018.
[11] "Is IoMT the Magic Bullet to Reshape Coordinated and Proactive Care Delivery?" Frost & Sullivan, June 27, 2017.
[12] Ladi Adefala, "Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries," Fortinet, March 6, 2018.
[13] Ladi Adefala, "Healthcare Experiences Twice the Number of Cyber Attacks As Other Industries," Fortinet, March 6, 2018.
[14] Lily Hay Newman, "Medical Devices Are the Next Security Nightmare," WIRED, March 2, 2017
[15] Heather Landi, "2017 Breach Report: 477 Breaches, 5.6M Patient Records Affected," Healthcare Informatics, January 23, 2018.

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

253402-0-0-EN
November 28, 2018 1:52 PM
wp-intelligent-segmentation-healthcare-industry