TRANSFORMING HEALTHCARE SECURITY IN THE DIGITAL ERA

EXECUTIVE SUMMARY

Hospitals and other medical organizations around the world remain among the most aggressively pursued targets of cyber criminals. Aging infrastructure, rapid merger landscapes, and high resource turnover pose a continuous challenge to healthcare information security leadership. At the same time, modern clinical care offerings are broadening adoption of new digital technologies, such as smart medical devices and multi-cloud services, to provide better care and customized services to patients. Unfortunately, these new technologies can expand the attack surface and bring new vulnerabilities to the network.

With increased information security risk and heightened awareness to ensure patient privacy, healthcare organizations need comprehensive network security that doesn't compromise performance or capabilities enabled by digital transformation (DX), and that is able to correlate security events in multiple environments. The Fortinet Security Fabric offers an integrated security architecture that can address the specific needs of modern healthcare—including high-performance protection, internal network segmentation, advanced threat protection, and end-to-end shared intelligence.

INNOVATION BRINGS RISK

Modern healthcare organizations are striving to deliver a more personalized customer experience and improve patient engagement through distributed and collaborative care. Providing these services to a broader patient population has driven rapid network technology distribution, resulting in challenges with visibility and remediation of threats.

Adoption of faster, cloud-based edge computing and digital technologies has helped health organizations get closer to consumers and improve the overall patient experience. This includes four major objectives related to DX:

1. Cloud adoption
2. Internet of Medical Things (IoMT): smart, connected devices
3. Ubiquitous broadband
4. Big data analytics

Currently, there are 7.1 million patients using connected medical devices and remote monitoring.[1] In addition, healthcare providers are expected to spend $9.5 billion on cloud services by 2020, with most organizations using a multi-cloud environment.[2] These advances simplify communication between patients and physicians, provide instantaneous health status, and encourage patients to take a more active role in their care.

However, these innovations also bring with them new and expanding risks. As healthcare organizations adopt more connected DX technologies, their environments become more complex and the healthcare network attack surface expands. With the sophistication of cyberattacks increasing, along with the known deficiencies in the current security resource marketplace, it's a perfect storm of vulnerability.

REWARDS OUTWEIGH GREATER RISKS—UNTIL THEY DON'T

Hospitals are putting more trust in distributed systems to store and analyze medical data, without the needed reassessment of security measures and controls. The U.K.'s National Health Service (NHS) recently gave healthcare providers the go-ahead to store confidential patient information in the public cloud. This is a notable shift in the level of trust healthcare providers are affording to the cloud, especially given the WannaCry ransomware attack that shut down the NHS in May 2017.[3] A 2017 study revealed that more than 25% of all data breaches last year were related to the healthcare space.[4] Despite the cyber risks associated with these sorts of adoptions, health organizations are moving forward due to the benefits they can provide in reducing cost.

At the same time, the potential liabilities under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act can reach into millions of dollars. The HITECH Act also dramatically expanded the number of vendors that can be held liable for data breaches. Similar to HIPAA protection for protected health information (PHI), the European Union's General Data Protection Regulation (GDPR) expands on the notion by regulating the entire life cycle of personal information, including how it's gathered, processed, stored, and ultimately destroyed.[5]

Regulatory penalties are only the beginning of the financial costs associated with healthcare data breaches. A study by the Ponemon Institute found that the average annual cost of cyber crime to healthcare institutions worldwide rose to $11.7 million per business in 2017. That figure represents a 23% increase from the $9.5 million per business reported in 2016 and 62% growth in spending over the last five years.[6]

Most health IT departments are challenged with constant prioritization of efforts, and during rapid integration that they have to choose between productivity and security—with productivity often winning in order to support the organization's broader business objectives. In reality, these trade-offs need not exist. The right security can enable the increased productivity that DX brings.

SPECIFIC CYBER RISKS OF IoMT DEVICES

Traditional network strategies primarily supported the deployment of firewalls along the perimeters of the network, but as evidenced in many cases, once a threat is successfully inside, there are usually few security measures in place to detect it or slow it down. This lateral movement is one reason connected IoT medical devices are popular attack vectors for cyber criminals. These internal endpoints have been authorized to access the network as authenticated users. Once through the perimeter defenses, IoMT devices have largely unquestioned access to much of the data stored on the network, making them ideal targets for cyber criminals.

Aside from their network access, many IoMT devices are also not designed with security as a core focus. Many devices in use have been built to perform clinical functions with little focus on securing the device or the data they collect. This means that IoMT devices often stay in use and continue to circulate on the network even with known vulnerabilities that can be targeted by cyber criminals to enter the network. The lack of applied encryption and the inability to apply security patches increase the risk of exposure of patient data.

EVOLVING HEALTHCARE SECURITY

Fortinet is dedicated to meeting the varied and critical security needs of today's healthcare organizations without sacrificing performance. We do this with integrated and scalable solutions that offer third-party validated security effectiveness and performance.

Fortinet and Partner-Ready Fabric Products integrate to form the Fortinet Security Fabric. This integration enables expanding organizations to dynamically adapt to the evolving IT infrastructure that results from

DX initiatives. Each security in the Fabric is aware, allowing consistent application of security controls, coordinated threat intelligence, and single-pane-of-glass management.

This integrated, collaborative approach detects threats more quickly and initiates and synchronizes a coordinated response no matter what part of the network or what endpoint is in jeopardy.

FORTINET INTEGRATES SECURITY FOR HEALTHCARE

Unlike isolated point security products, the Fortinet Security Fabric provides end-to-end control of the entire fluid network, not just at predefined perimeters. It also integrates with external solutions and shares information, further enhancing the healthcare organization's security capabilities and allowing it to leverage existing technology investments.

END-TO-END VISIBILITY AND CONTROL:

From any point on the continuum, a variety of users, including patients, staff, and healthcare partners, may access applications and data inside the healthcare network. These fluid network boundaries and geographically dispersed users and devices greatly expand the attack surface, making it exceedingly difficult to implement effective access control, centralized threat detection, and proactive mitigation.

SEGMENTATION:

In U.S. hospitals, there may be as many as 15 connected devices per bed.[7] Securing them requires enforcement of access policies for all users and connected devices, while assuring that latency does not affect clinical workflow and data availability. By applying microsegmentation using internal segmentation firewalls (ISFWs), segmentation can be adjusted dynamically to support reorganization, expansion, changes in policies, and so on. The Fortinet Security Fabric provides this agility, as well as complete visibility of all network segments.

SECURE CLOUD APPLICATIONS:

When migrating to the cloud, healthcare organizations should look for providers that can offer end-to-end visibility—from the IoMT at the edge, through the cloud, to the data-center core. This support structure ensures that health IT departments maintain visibility on security standards, even those outside their domains, so they can more confidently leverage the advantages of a multi-cloud environment.

SPEED AND PERFORMANCE:

The quality of patient care depends on the immediate and continuous availability of information and applications. To address this, the Fortinet Security Fabric uses security-specific processors in components such as firewalls and access points. Compared to off-the-shelf processors, security processors deliver faster packet processing, content inspection, and policy management processing. This enables security staff to implement strict security measures with minimal impact on application response times.

AUTOMATION AND INTEGRATION:

Automated security processes overcome human limitations to mitigate threats at the pace at which they occur. Automated systems are faster and less error-prone than humans at performing routine monitoring and response tasks (while considering all existing industry regulations). Armed with artificial intelligence (AI) and machine-learning (ML) capabilities, they are also better at prioritizing threats, allowing organizations to respond prudently, rather than trying to tackle every apparent threat.

ADVANCED THREAT PROTECTION:

No single technology can stop every threat. As a critical part of the Fortinet Security Fabric, sandboxing is a highly effective means of detection and mitigation. Operating at key locations in the Security Fabric, a sandbox provides an isolated, secure environment to validate incoming threats. It automatically propagates the threat information throughout the Fabric, immunizing the entire network against further damage. Through integration with external security technologies, applications, and services, the sandbox also shares threat information with the rest of the security community to help disrupt zero-day threats.

KEY PRODUCTS FOR SECURING HEALTHCARE

Fortinet delivers comprehensive security products that make up the Security Fabric. The following are key to healthcare environments:

- **FortiGate:** next-generation firewalls featuring the industry's best threat protection and performance, plus segmentation and simplified management
- **FortiSandbox:** sandboxing with top-rated, proactive advanced threat detection
- **FortiMail:** secure email gateways with high performance, top-rated effectiveness, and comprehensive coverage
- **FortiWeb:** web application firewalls (WAFs) that use AI to defend web apps from known and zero-day threats with nearly no false positives
- **FortiClient:** easy-to-manage, automated, fully customizable endpoint security
- **FortiADC:** application delivery controllers that optimize availability, user experience, and scalability of healthcare applications
- **Secure Wi-Fi:** a full suite of WLAN products designed to address the unique requirements of healthcare (e.g., mobile devices, IoMT, remote monitoring)

DIGITAL TRANSFORMATION REQUIRES SECURITY TRANSFORMATION

The growing threat of cyberattacks looms over every industry, but healthcare remains among the most highly targeted segments. As organizations adopt distributed patient-centric care models using connected medical devices that enable greater business capabilities, they also must be aware of the increased risks that can come with these innovations.

To continue to innovate, and to comply with the multitude of regulatory standards, healthcare providers must also transform how they approach network security. The Fortinet Security Fabric enables DX through integrated solutions that cover the network's entire attack surface. This leveraged shared intelligence ensures comprehensive protection and fast response to even the newest and most sophisticated threats.

[1] Thomas Beaton, "7.1M Patients Use Remote Monitoring, Connected Medical Devices," mHealthIntelligence, February 13, 2017.

[2] Karin Ratchinsky, "Cloud today and tomorrow: Why hospitals are tripling the use of cloud services," Healthcare IT News, January 8, 2016.

[3] Lily Hay Newman, "The Ransomware Meltdown Experts Warned About Is Here," Wired, May 12, 2017.

[4] Rebecca Weintraub and Joram Borenstein, "11 Things the Health Care Sector Must Do to Improve Cybersecurity," Harvard Business Review, June 1, 2017.

[5] Jonathan Nguyen-Duy, "How the General Data Protection Regulation Will Specifically Affect Healthcare," Fortinet, April 30, 2018.

[6] Jessica Kim Cohen, "Cybercrime costs healthcare companies $12.5M per year, report finds," Becker's Hospital Review, October 2, 2017.

[7] Lily Hay Newman, "Medical Devices Are the Next Security Nightmare," WIRED, March 2, 2017.

FORTINET®

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