FORTINET

ADVANCED THREAT PROTECTION FOR THE HEALTHCARE INDUSTRY

Advancing Medicine Needs Advanced Security

WHITE PAPER

ADVANCED THREAT PROTECTION FOR THE HEALTHCARE INDUSTRY

Advancing Medicine Needs Advanced Security

TABLE OF CONTENTS

Motivated Actors, Emerging Threats 3

High-Stakes Security 3,4

Breaking the Kill Chain of Advanced Attacks. 4

Advanced Threat Protection 5

Fortinet's ATP Solution for Healthcare. 5,6

Security Without Compromise 6

MOTIVATED ACTORS, EMERGING THREATS

The healthcare industry is in a unique and particularly vulnerable position when it comes to cybersecurity. Providers face substantial regulation around privacy and data security, while hackers have much to gain from patient data. Recent statistics put the black market value of healthcare records at ten times that of credit card information.

Attackers aren't just motivated by potential financial rewards either. Several large data breaches have been attributed to state actors collecting data for suspected espionage purposes. Protected health information (PHI) can be used to build rich personal profiles in the wrong hands.

Further complicating matters is the heterogeneity of the healthcare industry.

- Healthcare providers are expanding their care models, bringing more care and more data closer to patients with remote care, remote clinics, and online services, as well as sharing big data across provider networks.
- Pharmaceutical companies need to secure intellectual property (IP) worth potentially billions of dollars.
- Insurance providers must accommodate data exchange with countless providers, agencies, and brokers.
- Connected medical devices and remote monitoring are introducing new attack vectors and pushing even more data into vulnerable systems.

Unfortunately, healthcare has not traditionally focused on security in the same way as financial institutions or government agencies, for example, have. Now, though, as cyber criminals turn their attention to healthcare and threats become increasingly advanced, there is a sense of urgency industrywide.

More than **25% of all data breaches** last year were related to the **healthcare space,** resulting in an estimated **$5.6 billion lost** to cyber crime per year.[1]

HIGH-STAKES SECURITY

When a consumer credit card number is compromised, the credit card company issues a new card and will often refund fraudulent charges. In many cases, algorithms detect fraud before the consumer even knows their card number has been stolen.

When healthcare data is stolen, though, there are no such automatic protections. It can take months or years to see the effects of the full-blown identity theft that PHI can enable. Perhaps more importantly, new credit cards are easily issued; not so for one's identity. At the same time, the potential liabilities to healthcare organizations 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 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.[2]

Regulatory penalties are only the beginning of the financial costs associated with healthcare data breaches. Recent high-profile data breaches at major insurers have resulted in multiple class action lawsuits and substantial damage to brands and corporate images. 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.[3]

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

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

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

For pharmaceutical and biotechnology companies, corporate espionage is a very real concern, with several documented incidents of foreign hackers stealing IP. The $75 billion counterfeit drug market, among many other factors, is driving pharmaceutical IP theft to new levels. These organizations also often have HIPAA regulations with which to comply surrounding clinical trial data.

No matter which segment of the healthcare market we look at, potentially millions of dollars are at stake for every breach.

TRADITIONAL CYBERATTACKS

Traditional malware and cyberattacks provide the first inroad for hackers. Unfortunately, many healthcare organizations lack the security to effectively mitigate even these basic and well-known threats. Desktop and mobile malware, phishing schemes, DDoS, and ransomware have all hit healthcare organizations and continue to cause serious problems. Malicious software can be deployed through targeted attacks, compromised websites, spam, infected mobile devices, and any number of other avenues.

Ransomware continues to be a particular menace. According to one 2017 year-end report, the majority of healthcare providers were impacted by a ransomware attack in the past 12 months; almost all of the largest data breaches reported came from ransomware attacks, unauthorized server access, and computer viruses.[4]

CONNECTED MEDICAL DEVICES

Savvy hackers are learning to look beyond mobile devices or more commonplace network penetrations. Instead, the vast numbers of network-connected monitoring, diagnostic, imaging, and patient-care devices offer new opportunities to attack healthcare networks.

Currently, there are 7.1 million patients using connected medical devices and remote monitoring solutions. Many of these devices are running COTS operating systems that are well-understood by hackers, or simple embedded operating systems that were designed for function rather than security. Further, given the lengthy government certification process for many such devices, changes to address vulnerabilities are few and far between—leaving organizations exposed for extended periods of time.

Hackers who successfully compromise one of these devices are often greeted by very flat networks that are vulnerable to lateral movement of threats and the long-term survival that characterizes advanced attacks.

HOME HEALTHCARE DEVICES

Increasingly, patients are looking for ways to manage their health from home. Devices ranging from wearable fitness monitors to full-blown telemedicine interfaces are transmitting potentially sensitive data to cloud services, electronic health record databases, and other data stores. The devices themselves, while incredibly convenient, expand the attack surface hackers can use to access PHI.

BREAKING THE KILL CHAIN OF ADVANCED ATTACKS

The "kill chain" hardly sounds like a topic fit for healthcare, but it's an important construct as organizations consider how best to protect their critical data and PHI from attackers. The kill chain essentially describes how an attacker penetrates a network, establishes a foothold within the network, and then prepares to remove data, resulting in a breach.

Where the notion of the kill chain really becomes useful is in illustrating the many opportunities organizations have to prevent an attack from becoming a successful breach. The most common vector for advanced attacks, for example, remains email. Phishing attacks have been behind some of the most costly recent healthcare breaches and can provide ongoing sources of information for attackers to mount advanced, long-term campaigns. Antispam technologies then provide the first chance to break the kill chain and fend off an attack.

The second chance comes in the form of web filtering, designed to prevent a user from following a known malicious link or being connected to a compromised website via an attachment. Intrusion prevention systems (IPS) are the third line of defense, preventing malicious sites from launching attacks or downloading malware. Client and gateway antivirus may then catch malware that slips past IPS. Finally, if malware does become established within a network, application control and IP reputation services can prevent communication between the malware and command and control servers run by the attackers. These communications can guide lateral movement, instruction and staging data, and ultimately, exfiltration of data. Each layer of protection stands between an attacker and successful exfiltration of patient records, giving security infrastructure multiple, redundant opportunities to break the kill chain. Even with all of these layers, zero days, advanced obfuscation techniques, and novel approaches can open new avenues for attacks. This is where advanced threat protection (ATP) comes in.

[4] Elizabeth Snell, "Healthcare Ransomware Attacks Contribute to 2017 Top Data Breaches," HealthITSecurity, December 13, 2017.

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

ADVANCED THREAT PROTECTION

No single technology can stop every threat. Nor can a single organization see the entire threat landscape. It is important to establish a continuous and collaborative threat protection strategy that can prevent threats from penetrating the organization, detect those that do, and mitigate their impact.

Components in a security fabric that aid in prevention may include next-generation firewalls, secure email gateways, web application firewalls, and endpoint security clients. These may be deployed as physical (hardware-based) or virtual (software-based) devices. The latter are particularly appropriate for serving and managing geographically disparate clinics, offices, and other facilities.

Sandboxing is a highly effective means of detecting previously unknown threats. Operating at key locations in the security fabric, a sandbox provides an isolated, secure environment to examine unrecognized code. If it determines it's a threat, it automatically propagates the threat information throughout the fabric, immunizing the entire network against further damage.

COMPONENT 1: STOP KNOWN THREATS

Recognizable malware. Known phishing campaigns. Popular exploit techniques. Common evasion tactics. Compromised websites. These can be detected and blocked immediately with a combination of endpoint protection, next-generation firewalls, email gateways, and more. An important goal of ATP is to block as many threats as possible in this stage because it is fast and efficient.

COMPONENT 2: ANALYZE UNKNOWN THREATS

New vulnerabilities, new malware variants, and new attack techniques appear with alarming frequency. Some can be recognized as "variations on a theme," but many others require further analysis to determine their potential for harm. Suspicious (or even apparently benign) payloads need to be observed in a "sandbox" environment.

COMPONENT 3: RESPOND TO THREATS IMMEDIATELY

When new threats are identified, a fast, automated response is required to stop them. In addition, threat intelligence needs to be pushed back out to the ATP solution so that previously unknown threats can become known and mitigated immediately.

FORTINET'S ATP SOLUTION FOR HEALTHCARE

Healthcare encompasses a wide range of organizations and IT environments. Fortunately, ATP is quite flexible and provides comprehensive defenses in heterogeneous deployments. While ATP may look different for an insurance company than for a remote clinic, the idea is the same: block known threats immediately, detect unknown threats with sandboxing, and share intelligence on new threats.

Fortinet ATP delivers multilayered security controls including:

NETWORK PROTECTION

FortiGate Next-Generation Firewalls should be deployed at the perimeter and between key "zones" (as internal segmentation firewalls). They inspect incoming, outgoing, and internal traffic at key points controlled by IT. FortiGates also include IPS, web filtering, and application control. Medical devices that cannot be individually secured can be deployed behind a FortiGate for protection.

ENDPOINT PROTECTION

Clinicians are increasingly relying on mobile devices and laptops to access patient data, enter notes, and otherwise interact with electronic health records. FortiClient delivers comprehensive endpoint security and secure VPN for remote access.

EMAIL SECURITY

Several high-profile healthcare data breaches began with targeted phishing attacks. Email is also a popular method of disseminating confidential information. The FortiMail Secure Email Gateway delivers top-rated email security as well as data loss prevention (DLP).

WEB APPLICATION SECURITY

Web applications are extremely vulnerable and are often susceptible to numerous attack types. A web application firewall, such as FortiWeb, is required to provide another critical layer of protection.

SECURE WIRELESS

Hospitals, clinics, and research institutions all need to support wireless access. Wi-Fi can be an obvious point of entry for hackers and must be secured. Fortinet's Secure Access solution enables secure access points and switches, along with identity and access management.

SANDBOXING

FortiSandbox detects advanced threats that evade traditional security controls. Available as a physical appliance, virtual machine, or cloud-based solution, FortiSandbox observes the runtime behavior of suspicious files, payloads, and URLs. If a staff member at an insurance provider receives a suspicious email attachment, for example, the file can be automatically handed off to the FortiSandbox for testing to ensure that it doesn't contain malicious code.

When sandboxes and ongoing threat research can effectively hand off threat intelligence to the frontline layers of protection—whether to anti-malware software on a nurse's laptop or to next-generation firewalls protecting a data center at a pharmaceutical company—healthcare organizations can achieve extraordinary levels of protection. A shift away from point solutions and toward an integrated security architecture featuring ATP capabilities can move the needle on healthcare security in remarkable ways.

The limited breadth or quality of vendor portfolios often forces healthcare organizations to rely on a patchwork of point solutions. Hospital mergers, emerging health information systems, complicated payment environments, and many other factors unique to healthcare compound the problem. As an integrated part of the Fortinet Security Fabric architecture, our Advanced Threat Protection solution offers health IT a powerful, unified ecosystem to secure health information and valuable IP.

SECURITY WITHOUT COMPROMISE

Healthcare organizations have found themselves in the cross hairs of attackers from around the world. Nation-states are building detailed profiles on patients for espionage, while hackers are looking for big payoffs from high-value PHI. Attacks and the tools used to conduct them are getting more sophisticated every day and the stakes are incredibly high, both from a financial perspective for healthcare providers and from the perspective of patients looking to protect their privacy.

Implementing an effective ATP solution can secure patient data and IP while ensuring high-performance networking. Healthcare organizations no longer need to compromise performance for the sake of security (or security for the sake of access to information) now that scalable and manageable solutions exist to meet a wide range of needs across diverse healthcare systems.

HANDOFFS IN ADVANCED THREAT PROTECTION

The notion of the handoff is critical in advanced threat protection. Unknown or suspicious payloads are handed off from the first prevention stage to a sandbox for deeper automated analysis of all at-risk traffic. Risk ratings are returned to the prevention products to improve protection the next time traffic is seen. At the same time, threat information from the sandbox gets handed off to researchers who can work to better understand the source and behavior of the threats. Finally, researchers can use this new threat intelligence to update first-line protection measures.

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

July 5, 2018 7:35 AM

Macintosh HD:Users:US:Documents:FORTINET_ck:ATP_for_healthcare_WP:ATP_for_Healthcare_WP_ck