Advanced Threat Protection
For the Healthcare Industry

Advancing Medicine Needs Advanced Security
Advanced Threat Protection For Healthcare

Table of Contents

Introduction 3

High Stakes Security 4

No, Not That Kind of Vector 4

Breaking the Kill Chain of Advanced Attacks 5

The Advanced Threat Protection Framework 6

What Does ATP Look Like In Healthcare Settings? 6

Fortinet Solutions For Healthcare ATP 7

Conclusion 8
Introduction

Motivated Actors, Emerging Threats

The healthcare industry is in a unique and particularly vulnerable position when it comes to cyber security. 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. A number of recent 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 itself.

- Healthcare providers are expanding their care model, 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 worth potentially billions of dollars.
- Insurance providers must accommodate data exchange with countless providers, agencies, and brokers.
- The “Internet of Medical Things” is introducing new vectors and pushing even more data into vulnerable systems.

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

42.5% of the data breaches reported in 2014 were in the healthcare industry. Nearly 100 million patient records have already been exposed in the first half of 2015.

-Identity Theft Resource Center
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 HIPAA and the HITECH Act can reach into millions of dollars. The HITECH Act also dramatically expanded the number of vendors who can be held liable for data breaches.

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 2014 study by the Ponemon Institute found that the average annual cost of cyber crime to healthcare institutions is estimated to be more than 2.1 million USD. Costs, however can go much higher – A large insurer that suffered a massive breach in 2015 will likely deplete its $100 million cyber crime insurance policy just on contacting and providing credit monitoring to affected customers.

For pharmaceutical and biotechnology companies, corporate espionage is a very real concern with several documented incidents of foreign hackers stealing intellectual property (IP). The 75 billion USD 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.

No, Not That Kind of Vector

Healthcare professionals often refer to vectors when talking about disease transmission. Mosquitoes, for example, are vectors for malaria. Security researchers also talk about vectors – means by which malware can be transported onto a network and through which hackers can carry out an attack. In healthcare, the number of potential vectors for a cyber attack is alarming and increasing rapidly.

“Traditional” Cyber Attacks

Even “traditional” cyber attacks – desktop and mobile malware, phishing schemes, Trojans, ransomware, and the like – have potentially very serious consequences for the healthcare industry. As Fortinet’s vice president for healthcare, Ryan Witt, wrote recently,

“…they’re all out there, but the healthcare industry is particularly vulnerable because it lacks the built-in protections and underlying security mindset of other industries.”

These types of malicious software can be deployed through targeted attacks, compromised websites, spam, infected mobile devices, and any number of other avenues.

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. 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 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 (EHR) databases, and other data stores. The devices themselves, while incredibly convenient, further expand the attack surface hackers can use to access protected health information.

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 protected health information 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. Anti-spam 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, however, zero days, advanced obfuscation techniques, and novel approaches can open new avenues for attacks on protected health information and critical IP. This is where the Advanced Threat Protection Framework comes in.
The Advanced Threat Protection Framework

As with all things in cyber security, there is no silver bullet that can protect an organization from advanced threats. No single point solution can protect patient data or the intellectual property of research institutions. Instead, truly robust protection requires an interconnected framework of technologies and services designed to protect data and devices wherever they reside and whatever the nature of the attack.

This type of framework needs to be flexible, highly automated, and easy to deploy, protecting small clinics, remote users, large hospitals, insurance providers, and the largest pharmaceutical companies. Regardless of the scale and exact components, though, the advanced threat protection (ATP) framework can be broken down into three major components.

Component 1: Deal With Known Threats

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

Component 2: Analyze Unknown Threats

In the world of advanced threats, researchers frequently say that every day now is a “zero day”. New vulnerabilities, new malware variants and new attack techniques appear with alarming frequency and while some can be recognized as “variations on a theme”, many others require further analysis to determine their potential for harm. Suspicious (or even apparently benign) payloads need to be observed in a so-called “sandbox” environment.

Component 3: Respond To New Threats

When new threats are identified, they require to be investigated by trained security professionals to determine scope and impact. More importantly, threat intelligence needs to be pushed back out to the framework so that previously unknown threats can become known and mitigated immediately.

What Does ATP Look Like In Healthcare Settings?

Healthcare encompasses a wide range of organizations and IT environments. The advanced threat protection framework, though, is quite flexible and provides comprehensive protection in heterogeneous deployments. While advanced threat protection 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 feed back intelligence on new threats.

ATP begins with multilayered prevention, including

- Network protection: At the edge and segmenting between key “zones” inspecting incoming, outgoing and internal traffic at key points controlled by healthcare IT. Technologies applied here are firewalling for segmentation and next generation firewalls (NGFW) for deeper inspection. In many cases, gateway AV and URL filtering is deployed as stand-alone secure web gateway or consolidated NGFW.

- Endpoint protection: Clinicians are increasingly relying on mobile devices and laptops to access patient data, enter notes, and otherwise interact with electronic health records. Wherever possible, these will have anti-malware clients—ideally a full endpoint protection platform (EPP) stack—installed and, if operating remotely, access sensitive information via a VPN.

- Internet of Medical Things: In many cases, clinical and patient devices won’t be able to accommodate specific endpoint protection. Instead, these should be protected behind next generation firewalls that include intrusion prevention systems, specific application control and two-factor (or “strong”) authentication to prevent unauthorized access and to block malware.

- Email security: A number of high-profile healthcare data breaches recently have begun with targeted phishing attacks. Securing email with dedicated gateways in enterprise settings or unified threat management (UTM) in smaller settings can weed out many of these attacks.
Secure wireless: Hospitals, clinics, research institutions, etc., all need to support wireless access; WiFi can be an obvious point of entry for hackers and should be secured at the access point. And the more security at this edge the better.

Securing applications: Increasing reliance on cloud-based EHR and other healthcare web applications like insurance portals means that specific web application firewalls will provide another critical layer of protection. Additional inspection and detection often comes from the deployment of sandboxes- in one of a number of forms depending on the scale of the healthcare organization. Insurance providers, for example, will likely have one or more sandbox appliances in their data centers to achieve the necessary throughput for evaluating the high volume of data entering their systems. A hospital may centralize sandboxing for distributed clinics and offices, with handoffs occurring over WAN and/or VPN connections. It may also choose a cloud-based sandbox for small or remote facilities to avoid the backhaul.

When these sandboxes and ongoing threat research can effectively hand off threat intelligence back to the front line 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 towards an ATP framework can move the needle on healthcare security in remarkable ways.

Fortinet Solutions For Healthcare ATP

The limited breadth or quality of vendor portfolios often force health care organizations to rely on a patchwork of point solutions. Hospital mergers, emerging health information systems, complicated payment environments, and many other factors particular to healthcare compound the problem. Fortinet's Advanced Threat Protection Framework, however, gives health IT a powerful, unified ecosystem to prevent, detect, and mitigate threats to protected health information and valuable intellectual property.

Handoffs In Advanced Threat Protection

The notion of the handoff is critical in advanced threat protection. Unknown or suspicious payloads get handed off from the first, prevention, stage of the framework 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.

FortiGate next generation firewalls scale from small units that can be used to immediately protect a new medical device or rapidly secure a community clinic through high-end systems designed for large data centers at large insurance providers. In one case, a hospital was able to cut months off the setup time for an urgent care center by deploying wireless-enabled firewalls directly on portable carts to secure the clinic and connect to the affiliated hospital data center securely.

FortiMail appliances provide highly effective email gateways to shield users from spam and phishing attacks.

FortiClient software secures mobile and desktop endpoints, enforces FortiGate policies when devices are off-network and provides convenient VPN support, with easy centralized management, whether or not clinicians and staff are on the network.
Additional Fortinet software and appliances support two-factor authentication, web application firewalls, secure wireless, and more, all key components of a secure healthcare enterprise.

Detect
The FortiSandbox appliances provide contained environments to observe 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 that might be used to compromise patient records.

When FortiSandbox identifies malicious or high-risk payloads, integrated products and security staff are immediately alerted for mitigating action. Full threat lifecycle intelligence is optionally sent on to FortiGuard Labs for further research.

Mitigate
Based on the risk ratings returned, as well as indicators of the compromise uncovered, organizations are able to swiftly (and in certain cases proactively) respond to validate and contain attacks. Further, when information is shared with FortiGuard Labs- Fortinet’s dedicated research arm- expert researchers turn threat data into protection updates that are quickly fed back into the Advanced Threat Protection Framework.

If a hospital in San Francisco running a FortiGate and FortiSandbox in its data center encounters a new attack, not only will that hospital have the information they need to respond and mitigate the incident but a doctor in Istanbul running FortiClient on his laptop will also be automatically protected from the attack in the future.

Conclusion
Healthcare organizations have found themselves in the crosshairs 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 protected health information. 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 and identities.

Healthcare IT is faced with a choice: dramatically improve security or suffer damaging, expensive breaches of the sort that make headlines, impact the bottom line and compromise the identities of those in their care. Implementing an advanced threat protection solution, based on the right ecosystem of hardware, software and threat intelligence can secure patient data and intellectual property, all 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 the wide range of needs across their diverse health care systems.

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 http://www.fortinet.com/healthcare and Twitter: @FortinetHealth.