FORTINET

WHITE PAPER

Fortinet Healthcare Cybersecurity Solutions

Enabling the Latest Advances in Patient Care While Protecting Against Cyberattacks

Executive Summary

Medical advancements are saving and improving thousands of lives, and the healthcare industry is in many ways at the epicenter of digital innovation. However, these improvements in care, coupled with consolidation and merging partnerships, have made networks—and cybersecurity—much more complex. Data integrity and protection of confidential information are critical priorities in the industry, but cost containment is another necessity. Fortinet cybersecurity solutions for healthcare organizations enable a broad, integrated, and automated approach to protecting patients and their data. The Fortinet Security Fabric delivers comprehensive visibility and control across the data center, hybrid cloud environment, and the proliferating number of devices at the network edge. It also enables automated remediation and reporting, critical for compliance in a highly regulated industry.

Hospitals and medical clinics these days are centers of awe-inspiring, lifesaving digital technology. Care providers move from room to room, accessing myriad electronic devices and records to provide the best care possible. Internet-of-Medical-Things (IoMT) devices prolong life, improve its quality, and make the relationship between the patient and the care team less transactional. In addition, digital technology enables providers in different healthcare organizations to coordinate care more seamlessly.

"[W]hen hackers hold health records and sensitive patient data hostage, hospitals have no choice but to pay the ransom. Refusing to pay means patients could ... have lifesaving surgeries postponed."[4]

While providers and innovators in the healthcare sector are dedicated to saving lives and curing disease, their systems are a very attractive target for cyber criminals,[1] and incidents are frequent. One recent 30-day period saw six U.S. hospitals and health systems hit with cyberattacks.[2] Adversaries understand that downtime or other disruptions can threaten human lives. As a result, they aim to cause such disruption in an attempt to sow chaos or extract ransoms from desperate organizations.[3] Personal medical and financial data found on healthcare organizations' systems is also valuable to hackers for resale purposes.

Mergers and acquisitions and increasing partnerships between organizations add complexity to further healthcare organizations' sprawling technology infrastructure. The attack surface broadens as the network expands, and the number of third-party users accessing network resources is growing rapidly. IoMT devices are proliferating to address every conceivable medical condition—many of which were not designed with security in mind. From a compliance standpoint, the healthcare industry is highly regulated, with the Health Insurance Portability and Accountability Act (HIPAA) and state-level privacy laws placing strict guidelines on the sharing of medical information.

Key Healthcare Cybersecurity Challenges

Low Latency

While HIPAA does not require electronic protected health information (ePHI) to be encrypted, healthcare organizations have found that encryption is the only practical way to meet the law's protection requirements.[5] As a result, a large majority of a healthcare organization's network traffic is encrypted with secure sockets layer (SSL) or transport layer security (TLS) encryption.

As a result, medical organizations need to manage large volumes of encrypted network traffic securely without impacting network performance; latency impacts everything from staff productivity to patient care. On-demand data availability to support critical clinical services like telemedicine and remote diagnostics will continue to grow, and supporting technologies must be compatible with current releases of 5G cellular data transmission protocols as well as WAN edge optimization.

Data Integrity

Market forces and federal and state legislation have driven a trend toward interoperability within growing market partnerships of healthcare providers in recent years. As individuals and entities access healthcare information from each other's networks with increasing

frequency, the integrity of patient data throughout its life cycle is critical. For example, loss of life is possible when:

- A drug allergy is not clearly indicated on an electronic medical record (EMR) when time matters
- A medical device transmits or receives incorrect information
- The formulary for this year's flu vaccine is manipulated or compromised

It is also vital to secure research and DevOps environments and segregate them from patient care networks. Organizations must monitor and pass audits to demonstrate their compliance with standards and regulations around data integrity

57% of healthcare organizations surveyed had three or more intrusions in the past year.[6]

Operational Efficiency

As IoMT devices, mobile access to resources, and cloud-based services proliferate in the healthcare industry, organizations tend to fill gaps in an expanding attack surface by purchasing point products or relying on the security tools provided by each public cloud vendor. Since these tools do not integrate with each other, the result is architectural fragmentation. This creates several problems around operational efficiency:

- Increased cybersecurity staff time to correlate log reports
- Delayed response to fast-moving incoming threats
- Back-office inefficiency due to a large number of contracts and licenses from different vendors
- Increased software costs due to duplication of features on more than one product
- The need to maintain expertise with multiple point products on a small cybersecurity staff

Such disaggregation also creates increased "alert noise," making it virtually impossible for healthcare providers to clearly identify indicators of compromise. Being unaware of threats when they infiltrate the environment can be a life-or-death proposition at a healthcare organization.

Physical Distribution of Sites and Partners

As in most industries, the trend in healthcare is toward organizational consolidation and operational cost reduction, making mergers and acquisitions frequent. In addition, organizations and providers participate in an increasingly complex web of affiliated and unaffiliated clinics, hospitals, research sites, and insurance carriers. All these entities use and transfer ePHI data owned by the enterprise health system. Owing to their often-disconnected systems, all players in this process struggle with challenges of visibility, data control, access auditing, and compliance reporting. As a result, providing consistent security controls across organizations is a big challenge.

Cost

As payments by insurance companies remain flat—or even decline—and some government reimbursement programs are discontinued, healthcare organizations face extreme cost-cutting measures, particularly for operational expenses. Every dollar subtracted from overhead makes it less likely that prices to patients will need to increase. This will be an even bigger priority if pending medical services price transparency legislation moves forward in 2020, as consumers will be able to see these price increases. If anything, IT and cybersecurity spending in healthcare will be even more heavily scrutinized in the foreseeable future than it is today.

Compliance Reporting

Jurisdictions around the world continue to enact a patchwork of regulations affecting healthcare, with HIPAA serving as the regulatory centerpiece in the United States. Protection of ePHI is critical for both compliance and patient care reasons. Providers also have personal financial information from nearly every patient and human resources data from their large pool of current and former employees. Healthcare organizations must be able to achieve and demonstrate compliance with multiple regulations and standards without redeploying critical staff from strategic initiatives to preparing audit reports.

Use Cases

There are various use cases when it comes to cybersecurity and healthcare organizations, including:

The Distributed Health Enterprise

Market forces and government policies are causing significant consolidation in the healthcare industry. In addition to mergers and acquisitions, many entities form deep partnerships with other organizations, with the goal of sharing a common IT records system. Both trends tend to result in different entities and locations using different technologies—at least for the time being. This increases the attack surface and impacts everything from visibility to operational efficiency.

To address this fragmentation of systems and applications, healthcare enterprises need to assimilate new branch locations into an integrated cybersecurity architecture. Connections with these locations must deliver performance with minimal latency, and care should be taken that adversaries cannot penetrate a less secure branch location and then move laterally within the enterprise.

As a starting point, Fortinet networking and secure branch solutions enable fast-growing healthcare networks to scale their operations securely and with high performance. Fortinet technology enables quick integration of newly acquired branch locations by providing integrated networking and security within the branch and with headquarters. **Fortinet Secure SD-WAN** uses software-defined wide-area networking technology to enable network traffic to move over the public internet—or even over selected public clouds using a virtual WAN (vWAN). And **Fortinet SD-Branch** solutions allow network access control, wireless access points, and networking hardware to integrate into the larger security architecture.

Digital Innovation and IoMT Security

Connected IoMT devices are a big part of the digital transformation currently underway in the healthcare industry. It is critical that the data coming in and out of these devices be accurate and timely. Securing these devices is a critical priority, and the vast number of distinct device types complicates the task. Many of them do not have robust, built-in security, and most of them transmit data over public cellular and Wi-Fi networks.

Regardless of the security features found in each individual device, these devices must integrate with an organization's overall security architecture to prevent intrusions. Similarly, users of these devices must be verified and access restricted to those who need it. This helps ensure data integrity and timely patient care.

The **Fortinet Security Fabric** enables organizations to evaluate users and devices using intelligent segmentation and several layers of trust verification. **Intent-based segmentation** functionality in **FortiGate NGFWs** enables a flexible, intelligent approach to segmenting the network. For devices, **FortiNAC** network access control (NAC) keeps track of IoMT devices and their compliance with security policies, while advanced endpoint protection tools like **FortiClient** and **FortiEDR** protect those devices from attack. For users, **FortiAuthenticator** and **FortiToken** identity and access management tools provide layers of authentication. And the **FortiManager, FortiAnalyzer,** and **FortiSIEM** management analytics solutions—plus Fortinet security orchestration, automation, and response (SOAR) tools, including **FortiSOAR**, can be seamlessly integrated into the Security Fabric to automate management, reporting, and threat response.

Cyber and Physical Security

Hospitals and health clinics must be prepared for the unexpected when it comes to physical security. Patients who are diagnosed with serious illnesses or suffer critical injuries often experience extreme emotional swings while at a facility—as do patients' friends and family. In addition, criminals enter healthcare facilities to steal controlled substances, cause operational disruptions, and target those who provide controversial types of medical care. In short, physical security is just as critical as cybersecurity in the healthcare industry.

The best way to optimize physical security is to integrate surveillance cameras and recorders with the larger security architecture, enabling cybersecurity protection for these devices. Integrating telephony into the same network provides seamless connections between security personnel, cybersecurity professionals, and law enforcement.

Fortinet provides the opportunity for institutions to integrate cyber and physical security functions—as well as voice communications and public address (PA) systems—onto a

"**Four to seven percent** of a health system's IT budget is in cybersecurity, compared to about 15% for other sectors such as the financial industry."[7]

single console for centralized visibility and management. This enables IP phone systems, security cameras, emerging facial recognition and weapons detection technologies, and recordings of footage to be a part of the organization's overall security architecture. **FortiCamera, FortiRecorder, FortiVoice,** and **FortiFone** provide the hardware and software for this integrated system as a part of the **Fortinet Security Fabric**. This is particularly useful for privacy and security investigations and for keeping all parties informed about incidents in progress.

39% of healthcare organizations surveyed had an intrusion in the past year that put **physical safety at risk**. [9]

Insider Threat Protection

Recent research by Verizon identifies the healthcare vertical as having the highest risk from insider threats among all industries.[8] Two factors are particularly relevant in this trend: the high value of medical information on the black market, and the high turnover in administrative and frontline care positions in the industry. As with other industries, incidents involving insiders can be either accidental or deliberate, and deliberate attacks occur because of a variety of motivations. The stakes are high, as compromised data can result in serious complications or even death, and disclosure of ePHI can incur serious liability on an organization.

Successfully battling insider threats requires a multilayered, coordinated approach at a time when trust is no longer static. The network should be intelligently segmented to restrict access to each piece of information to those who need it. Additionally, every request for network resources should be inspected from the perspective of both the user and the device. Such a zero-trust approach helps detect inappropriate activity by insiders and block it before it causes damage.

The **Fortinet Security Fabric** provides layers of protection against accidental and deliberate insider attacks. **Intent-based segmentation** features in **FortiGate NGFWs** help keep unauthorized users from accessing specific datasets. The **FortiAuthenticator** and **FortiToken** identity and access management tools verify users, while **FortiInsight** user and entity behavior analytics (UEBA) watches for anomalous behavior by trusted user accounts. **FortiPresence** presence analytics technology can also help detect unauthorized access to physical locations by tracking locations of mobile devices. **FortiDeceptor** deception technology lures adversaries into identifying themselves. And **FortiNAC** network access control and **FortiClient** and **FortiEDR** advanced endpoint security tools help with device verification and protection.

Emerging Industry and Regulatory Trends

Change is the name of the game in healthcare privacy and security, and emerging trends like embedded medical devices will continue this trend of constant change for the foreseeable future. Rapid transition in both technology and regulation will run in parallel tracks, with different jurisdictions passing different requirements in an effort to keep up with advancing technology.

There is no way to predict what a healthcare organization will need in the future to protect its systems and comply with new regulations. As a result, organizations must build a robust but resilient security architecture that can absorb and seamlessly integrate new tools and elements—without requiring a full rip and replace of the underlying system every few years.

The **Fortinet Security Fabric** is built on FortiOS, a robust, flexible operating system that enables seamless integration of a broad portfolio of Fortinet tools. In addition, Fortinet works with its Fabric Partners to build **Fabric Connectors** that enable select third-party tools to be deeply integrated into the Security Fabric. And robust **application programming interface (API) tools** enable organizations to integrate other third-party solutions.

Fortinet's deep integration of security solutions deployed on-premises and in the cloud unlocks full automation of security workflows, from detection to response to remediation. Additionally, **FortiManager, FortiAnalyzer,** and **FortiSIEM** help security teams achieve full visibility and centralized control. This enables a proactive rather than a reactive stance toward cybersecurity.

Corporate Hybrid Cloud Infrastructure

Increasingly, healthcare organizations struggle with imparting consistent security controls for the multitude of enterprise environments that they are responsible for managing. Most notably, a majority of healthcare institutions now operate in multiple public and private clouds along with the corporate data center. Such an approach can increase efficiency, address problems with interoperability, and ultimately improve patient care. But if an organization relies on each cloud's built-in security tools, consistent reporting of an enterprise security posture is practically impossible.

Organizations facing a fragmented security architecture across their hybrid cloud environment cannot solve their problem without deliberately moving toward end-to-end integration. While the built-in security tools provided by each public cloud provider are useful for what they are designed to do, institutions need a way to aggregate all these systems with the on-premises infrastructure, enabling a single-pane-of-glass view of the entire infrastructure.

Fortinet **Dynamic Cloud Security** tools, part of the **Fortinet Security Fabric**, unify healthcare organizations' hybrid cloud infrastructure by enabling consistent policy management and centralized visibility of the entire infrastructure. These solutions are designed with *native integration* with all major public cloud providers, *broad protection* to cover the entire attack surface, and *management and automation* functionality that enables a proactive approach to threat detection and response, as well as automated compliance reporting.

"The global healthcare cloud computing market size is expected to reach $27.8 billion by 2026, exhibiting a CAGR of 11.8% over the forecast period."[10]

Fortinet Differentiators

There are a number of different reasons why healthcare organizations should choose Fortinet when tackling the aforementioned use cases. These include:

Integrated Platform

Fortinet's integrated platform *aggregates the security architecture for healthcare organizations*, from the data center to multiple clouds to myriad lifesaving devices. An **open API** and **Fabric Connectors** help them integrate third-party tools for niche coverage and to maximize prior investments.

Cyber-physical Coverage

Fortinet provides the ability to *consolidate secure voice, networking, and surveillance functions* into a single system with centralized visibility and control. This helps fight against coordinated cyber-physical attacks and helps keep facilities, patients, and IT systems safe.

Branch Location Networking and Security

Fortinet offers a *comprehensive SD-WAN and secure networking infrastructure for branch locations* that provides optimal security and improves network performance.

Processing Efficiency

Fortinet application-specific integrated circuit (ASIC) chip processing efficiencies enable high performance—*even with SSL/TLS inspection activated*—a big benefit in an industry with large amounts of encrypted data and zero tolerance for clinical data latency needed to support patient care. Fortinet security processors can accelerate specific parts of the packet processing and content scanning functions. This technology also offers the ability to run multiple security applications without degradation in performance.

High Performance and Low Latency

FortiGate NGFWs provide the industry's best performance during SSL/TLS inspection and experience extremely low latency rates, helping ensure that vital, encrypted medical data is available without delay.[11]

Insider Threat Protection

Fortinet delivers a comprehensive solution to guard against insider threats with robust identity and access management supported by NAC, intent-based segmentation, deception technology, and UEBA.

Robust Threat Intelligence

FortiGuard Labs delivers comprehensive intelligence from a global network of sensors and an artificial intelligence (AI)-powered self-evolving detection system (SEDS) that has been honing its algorithms for nearly eight years. The result is extremely accurate identification of zero-day threats.

Industry Leadership

Fortinet has achieved nine "Recommended" ratings from NSS Labs[12] and achieved the best score in its NGFW Security Value Map. The company is recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls.[13]

Cost-effective Solution

Fortinet delivers industry-leading total cost of ownership (TCO)[14] due to high-performance throughput and latency for NGFWs, Secure SD-WAN, and SD-Branch capabilities. This performance is enabled by purpose-built ASIC security processors. TCO capabilities are also driven by the ability to use SSL/TLS encryption inspection without performance impact—unlike many competitive solutions.

"Substantially addressing cybersecurity in healthcare situations isn't going to be easy, and will take cooperation from everyone from doctors to nurses, to IT professionals and manufacturers."[15]

Conclusion

Given the life-or-death implications of their mission, healthcare organizations should prioritize and invest in a comprehensive cybersecurity strategy. Lives could be lost if operations are disrupted or data is compromised by a cyberattack. In addition, significant fines—and even lawsuits—are possible if patients' ePHI is compromised. As hospitals and clinics face constant organizational transition and technological advancement, Fortinet delivers a flexible, integrated cybersecurity solution that streamlines operations and bolsters protection.

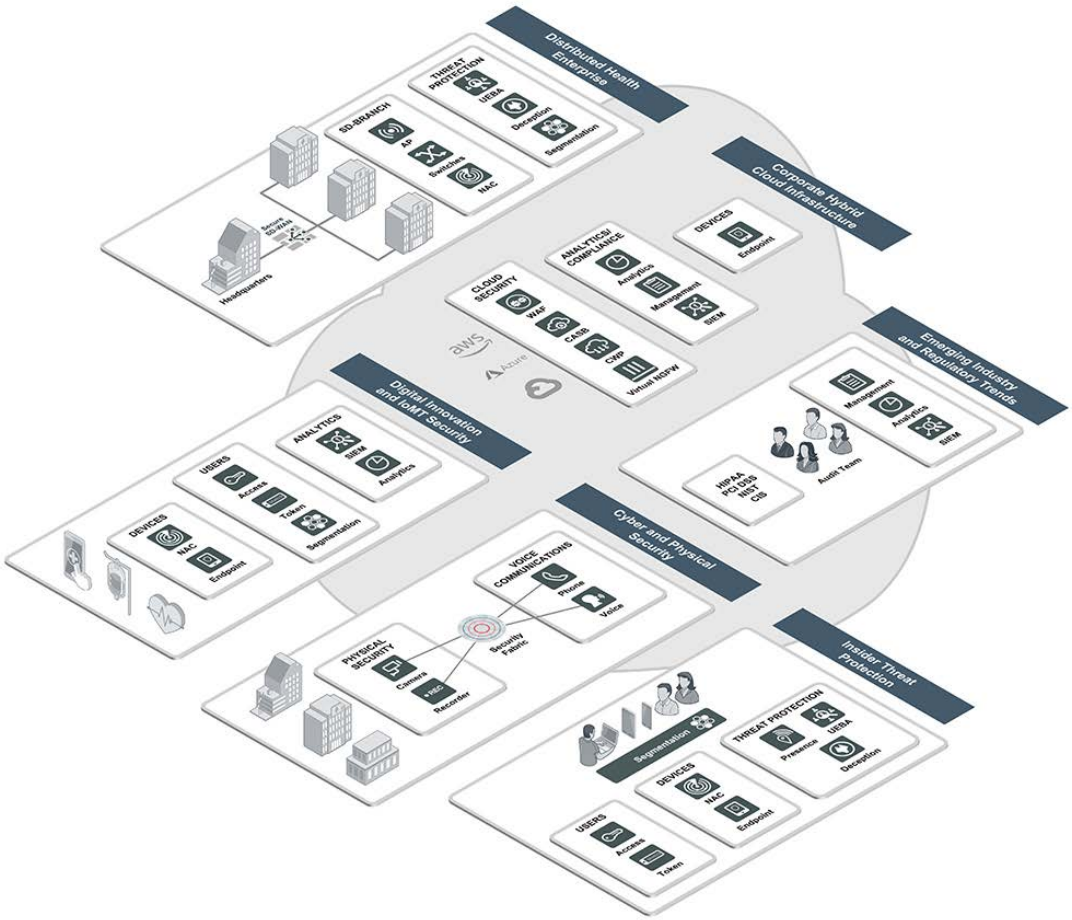

Figure 1: Healthcare cybersecurity use cases.

[1] Kate Patrick, "Hospitals Are Cyber Criminals' Newest, Biggest Target," InsideSources, February 25, 2019.

[2] Laura Dyrda, "6 hospitals, health systems report cyberattacks in the past 30 days," Becker's Hospital Review, July 25, 2019.

[3] Sonia Arista, "3 Trends Plaguing Healthcare Cybersecurity & How to Fight Them," Fortinet, July 3, 2019.

[4] Kate Patrick, "Hospitals Are Cyber Criminals' Newest, Biggest Target," InsideSources, February 25, 2019.

[5] Elizabeth Snell, "Healthcare Data Encryption not 'Required,' but Very Necessary," Health IT Security, June 14, 2017.

[6] Aggregated results of 2019 Fortinet surveys of CIOs, CISOs, CFOs, IT infrastructure leaders, security architects, and network leaders.

[7] Susan Morse, "Healthcare's number one financial issue is cybersecurity," Healthcare Finance, July 30, 2019.

[8] "2018 Data Breach Investigations Report," Verizon, 2018.

[9] Aggregated results of 2019 Fortinet surveys of CIOs, CISOs, CFOs, IT infrastructure leaders, security architects, and network leaders.

[10] "Healthcare Cloud Computing Market Size, Share & Trends Analysis Report By Application, By Deployment Model (Private, Public, Hybrid), By Pricing Model, By Service Model, By End Use (Providers, Payers), And Segment Forecasts, 2019–2026," Research and Markets, July 2019.

[11] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

[12] Ibid.

[13] "Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls," Fortinet, accessed January 15, 2020.

[14] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

[15] Nicole Wetsman, "Health Care's Huge Cybersecurity Problem," The Verge, April 4, 2019.

January 30, 2020 7:27 AM

516902-0-0-EN

D:\Fortinet\White Paper\Healthcare Solution\wp-fortinet-healthcare-cybersecurity-solutions-V2-1302020-727AM