A SECURITY FABRIC FOR DIGITAL-AGE HEALTHCARE
As healthcare organizations increase their quality of services through new digital care delivery and provider collaboration models, they amplify their exposure to all kinds of attacks. Ransomware has been a particular menace. According to one report, 88% of ransomware attacks are directed at the healthcare sector.\(^1\) In 2017, the cost of a healthcare data breach was $380 per record—higher than any other industry and twice the cost of an average breach elsewhere.

CISOs aren’t sitting idly by; no healthcare security professional wants to be the next victim of a high-profile attack. And no healthcare organization can afford the tarnished reputation of a Health Insurance Portability and Protection Act (HIPAA) breach. According to one study, 65% of patients say they would steer away from companies whose records have been compromised.\(^2\)

However, just as flu vaccines for one season become ineffective for the next, network security strategies that protect only against today’s specific threats will leave healthcare organizations exposed to the unimaginable tomorrow, as threats mutate and new threats arise. Point products and platforms leave security gaps and require an unattainable level of security staffing. What healthcare CISOs need is a **security fabric**, an automated, adaptive, and integrative model for organization-wide network security.
GROWING EXPECTATIONS, SHRINKING RESOURCES

Long waits for appointments. Hours spent at clinics. Interminable paper forms. Healthcare consumers in the digital age expect better. Today, preferred healthcare providers accommodate their patients’ busy schedules, through off-site services such as minute clinics, telemedicine events, or secure text consultations. This is being driven by Millennials who prefer to use digital channels to engage with their healthcare providers over in-person or phone interactions. Healthcare providers also deliver better care to patients and help them avoid unnecessary office visits by monitoring them through cloud-connected wearables and implanted medical devices (IoMT).

Healthcare CISOs face a complex set of challenges as they seek to support this digital transformation while protecting critical patient information and proprietary medical research and complying with shifting regulations. Specifically, just as the healthcare network attack surface expands and the sophistication of cyber-attacks increases, the security skills needed to deal with the threats remain in short supply.

The security fabric outlined here can help CISOs meet these challenges in collaboration with their clinical, administrative, and IT staff.
A MULTI-LAYERED APPROACH

The security fabric represents a new architectural approach to enterprise information security. Fabric components include enterprise firewalls, cloud security, advanced threat protection, connected unified threat management (for small sites such as medical offices and clinics), application security, secure access, and services for network operations centers (NOC) and security operations centers (SOC).

The fabric model is unique in several ways:

- Unlike point products and security platforms, a security fabric provides end-to-end control of the entire fluid network, not just at pre-defined perimeters.
- A fabric maximizes security communication throughput, because it utilizes high-performance, security-optimized processors rather than off-the-shelf processors. It also minimizes latency in threat analysis and response by enabling each component to communicate directly with the others, rather than going through a central management system, as is the case with security platforms.
- A security fabric integrates with external solutions and shares information with them, further enhancing the healthcare organization’s security capabilities and allowing it to leverage existing technology.
END-TO-END VISIBILITY AND CONTROL INCREASE CONFIDENCE IN DIGITAL TRANSFORMATION

Healthcare is patient-centric, and the continuum of care may flow through clinics, billing offices, hospitals, pharmacies, laboratories, and to the home (see Figure 1). Electronic health record (EHR) data flows along the continuum of care. In addition, 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. Such fluid network boundaries and geographically dispersed users and devices greatly expand the attack surface, and it becomes exceedingly difficult to implement effective access control, centralized threat detection, and proactive mitigation.

SEGMENTATION BEST PRACTICES

Agile segmentation is a key enabler of access control in every healthcare environment. Thus, it is a central tenet of the security fabric approach. Healthcare organizations must be able to perform macro-segmentation to separate domains, either physical domains such as laboratories, clinics, and pharmacies, or functional domains such as facilities management, billing, and radiology.

This is not enough, however. There is a wide variety of 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.³ Allowing the use of such devices is often essential to the healthcare organization’s digital transformation. To do so securely, however, requires enforcing access policies for all users and connected devices. The easiest way to do that, in these typically flat (level-2) domains, is to apply micro-level segmentation using internal network security firewalls.

Where it makes sense to do so, healthcare organizations can implement even more granular access control within the fabric components themselves. The access control settings can be based on roles, device type, time of day, location, and so on.

It is important that both macro- and micro-level segmentation can be adjusted dynamically, to support reorganization, expansion, changes in policies, and so on. The fabric architecture allows this agility, as well as complete visibility of all network segments.

ENABLING SECURE CLOUD APPLICATIONS

In any discussion of the “complete network,” concerns invariably arise about expansion to the cloud. Healthcare CISOs will certainly agree that migrating to cloud platforms—private, public, and hybrid—lowers cost, improves scalability, and reduces data center footprints. But they are also concerned that exposure to the cloud increases vulnerability and can reduce the organization’s ability to see—and hence control—what goes on there.

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 will enable CISOs to maintain their security standards even outside their domains, so they can more confidently leverage the advantages of a multi-cloud environment.

MICRO-SEGMENTATION PROVIDES EFFECTIVE DAMAGE CONTROL

When attack vectors succeed in penetrating perimeter defenses, internal segmentation firewalls limit the attacker’s further progress. Additionally, when lapses in cyber hygiene lead to the compromise of one device, segmentation can prevent the infected device from contaminating the rest of the network.
SPEED AND PERFORMANCE ENCOURAGE COOPERATION ON SECURITY

The quality of patient care depends on the immediate and continuous availability of information and applications. Security processing must not become a bottleneck. If firewalls and access controls get in the way of patient care, CISOs may find department heads and administrators much less cooperative with security initiatives.

To address this concern, the security fabric architecture 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. Conversely, when asked to enhance performance in support of new care delivery models, they can do so without compromising security, enabling application prioritization, traffic optimization, and device-level security in various components of the security fabric.

AUTOMATION AND INTEGRATION KEEPS CISOS A STEP AHEAD

Today, security threats are so sophisticated and so numerous, it is no longer humanly possible to keep track of them—let alone prioritize and address them. Threat propagation is also accelerating, from hours to minutes or even seconds.

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 and machine learning capabilities, they are also better at prioritizing threats, allowing organizations to respond prudently, rather than trying to tackle every apparent threat.

Automation relieves routine threat management tasks, enabling security staff to have more time to work on minimizing security vulnerabilities. For example, they can devote resources to developing security hygiene training programs for hospital staff, clinics, labs, and other healthcare entities. They can also find more time for impact mitigation. In collaboration with clinical and administrative staff, they can rethink how the organization’s healthcare information is generated, transmitted, and stored to reduce the impact of a cyberattack.

Another way CISOs can empower their existing security staff, minimizing the need for new hires, is to integrate the decision-making interfaces. In an environment of point products, staff must toggle from one dashboard to another, and it is difficult to gain a systemic view. In contrast, the security fabric integrates all network security functions and enables their management through a single pane of glass. Thus, the healthcare organization can scale its services securely, without being impeded by today’s shortage of security skills.

“AUTOMATION” DOES NOT MEAN “AUTO-PILOT”

Automation augments human decision-making rather than replacing it. Security staff can discriminate between low-regret situations—in which they supervise the unimpeded operation of the AI-enhanced security algorithms—and high-regret situations, where they take a more active role in directing the threat response.
ADVANCED THREAT PROTECTION IS CONTINUOUS AND COLLABORATIVE

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 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.

It is important to clearly designate who will bear responsibility for establishing and maintaining organization-wide threat protection. In some healthcare systems, it is considered within the purview of the NOC. However, as most NOCs already bear a heavy burden in fulfilling performance and availability SLAs, a SOC may be more effective.

Creating and staffing an in-house SOC with the right security skill sets is not easy, and for some organizations, it may not be feasible. The good news is that the security fabric model supports the outsourcing of SOC functions to managed service providers, which can deploy and manage the various fabric components mentioned above. Judicious procurement of managed security services makes it easier for CISOs to maintain a strong network security posture despite tight IT budgets and skills shortages.

FABRIC: A KEY ENABLER TO HEALTHCARE

The growing threat of cyberattacks looms over every industry, but healthcare is among the most affected. And because today’s healthcare is delivered everywhere, healthcare IT security must be everywhere, nimbly adapting both to users’ needs and to evolving threats.

The security fabric provides a realistic model for comprehensive IT security that CISOs can start implementing immediately—on their distributed premises and in the cloud, in their own SOCs or through managed security services. As the pioneer of the security fabric approach, Fortinet stands ready to assist healthcare CISOs with technology, services and best-of-breed third-party solutions for threat prevention, detection, and response.
“Hospitals are hit with 88% of all ransomware attacks,” Becker’s Health IT & CIO Review, July, 2016.

“65% of Patients Would Avoid Companies that Suffered a HIPAA Breach,” HIPAA Journal.