ciena
Experience. Outcomes.

APPLICATION NOTE

End-to-End Network Encryption for Secure Healthcare

Despite billions of dollars spent on data security in the healthcare industry, cyber attacks and data breaches continue at epidemic levels. Nearly 90 percent of healthcare providers have been hit by data breaches in the last two years, according to a 2016 Ponemon Institute study. Healthcare CIOs have realized it's no longer a matter of *if* you will be attacked, it's *when* you will be attacked. The cost of these data breaches is also rising, to nearly $4.1 million per incident.[1] In addition, patients are now beginning to include cyber security as a factor when choosing their healthcare providers. These potential business impacts and the continuing onslaught of attacks is an increasingly frequent topic in covered entity and business associate board-level discussions.

Traditionally, healthcare data security strategy has focused on shoring up the perimeter. Over the past couple of years, CIOs began focusing more attention on encrypting patient data at rest, mainly due to HIPAA recommendations. But many CIOs are neglecting to encrypt data as it traverses their networks. In the aforementioned Ponemon study, 40 percent of hospitals indicated that they do not encrypt data in transit. This is an alarming statistic, given the trend toward greater sharing of Patient Health Information (PHI) between non-affiliated covered entities and business associates that need to collaborate along the continuum of a patient's treatment. For example, PHI can travel between primary care physicians, specialists, surgeons, imaging centers, home health agencies, accountants, insurance companies, and family members. In an era of analytics and big data, so much new, unstructured data is generated every day that it can be difficult for IT administrators to know where it all resides and how and by whom it is being used.

Benefits

- Safeguards protected electronic patient information from data breach and keeps critical systems secure
- Protects valued reputations and avoids costly fines, public media exposure, and patient churn by meeting expectations for information protection
- Provides a 'safe harbor' exemption under HIPAA requirements for reporting a data breach; contributes to compliance with regulations such as PIPEDA, EUDPD, JPIPA, UKNHS

[1] Ponemon Institute: "Sixth Annual Benchmark Study on Privacy & Security of Healthcare"; May, 2016; by Dr. Larry Ponemon

Why healthcare CIOs do not encrypt in-flight data

Some healthcare CIOs do not fully appreciate that fact that once patient data leaves the premises, it is basically outside of their control. Given all the efforts to lock down data at rest with firewalls, anti-virus software, and intrusion detection, cyber criminals are increasingly turning their attention to intercepting the data as it travels across the network. Cyber security firms are reporting increasing numbers of cyber incidents focused on corporate and internal networks.

Another reason for the lack of focus on in-flight encryption is that many CIOs believe that their fiber-optic networks are inherently immune to breaches. The reality is that a mid-range hacker armed with low-cost equipment and software can intercept patient data undetected for days, months, or even years. Anyone with Internet access can easily shop online for a fiber coupling tool and, after watching a few videos that guide you through the tapping process, can quickly learn how to steal sensitive data from a fiber optic cable. Numerous videos depicting the ease with which hackers can breach a fiber network can be found on YouTube. A single fiber strand can carry an enormous amount of data and, since fiber-optic cables are surprisingly accessible, they have become valuable targets for attackers.

Hacking an Optical Fiber Line in Minutes
Watch Video

An additional reason CIOs have been reluctant to deploy in-flight data encryption is their concern about decreased network performance and cost. In an industry where margins are thinning and network latency can mean the difference between life and death, their concern is understandable, although unfounded. These concerns may stem from experience with Layer 2 and higher network encryption solutions. For example, Layer 3 encryption devices are designed for IPSec encryption (standard Internet encryption). IPSec uses a process that 'tunnels' the original IP packet to encrypt an IP 'header.' However, tunnels can result in an increase in overhead, complexity, and subsequently, network performance speed and processing. Layer 3 encryption also may not be able to support the increasing number of new medical devices, evolving digital health applications, and protocols being deployed throughout the healthcare industry.

In-flight encryption at the optical layer

Optical layer encryption addresses all these issues and more. While technologies like Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are increasingly used to secure connections to servers, the only way to secure everything on the communications link in and out of a facility is to encrypt at the physical layer. This approach renders patient data undecipherable to any hacker that taps into the fiber strand.

TLS and SSL solutions also generally rely on third-party certificate authorities that may themselves be compromised, allowing for man-in-the middle attacks. In addition, the traditional operational model for deploying and maintaining protocol-specific encryption solutions can quickly become cumbersome, complex, and costly with multiple encrypt/decrypt device pairs required to support a multi-protocol environment. At the transport layer, a wide variety of traffic types—such as Ethernet, Fibre Channel, OTN, SONET, and SDH—can be encrypted simultaneously. Furthermore, optical layer encryption guarantees transparent encryption at wire speed. In other words, the encryption process does not reduce the traffic throughput of the signal being encrypted, nor does it modify user data in any way. Additionally, encrypting all traffic before it enters the fiber ensures the entire data channel is encrypted, no matter what.

One major benefit of encrypting in-flight data is the potential 'safe harbor' exemption from the HIPAA requirement to report a data breach. The caveat is that the optical-layer encryption must comply with Federal Information Processing Standards (FIPS) 140-2 standards.

Healthcare key encryption use cases and applications:

1. **Data center Interconnect (DCI)**
    a. Disaster avoidance/recovery
    b. Data center consolidation/optimization
    c. Workload mobility
    d. Cloud services
2. **Video transport**
    a. Remote diagnosis
    b. Telesurgery
    c. Medical distance learning

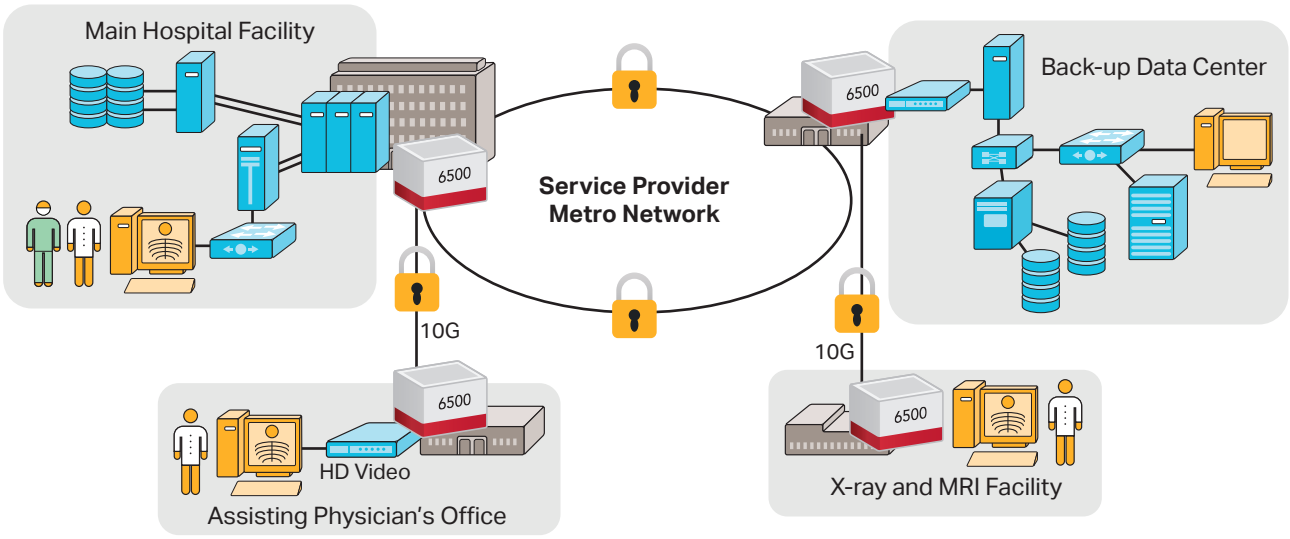

Figure 1. Metropolitan healthcare network

3. Connectivity services-related applications

a. Health Information Exchanges (HIEs)

b. Data analytics and mining/Big Data

c. Patient portals

d. Image storage backup and archiving, lifecycle management

e. Computerized Physician Order Entry (CPOE)

f. Clinical workgroup collaboration

g. Billing, claims, asset/patient tracking

h. Email and ERP systems

Ciena's WaveLogic Encryption solution

WaveLogic Encryption combines the proven encryption technology deployed on platforms that have a large global installed base with the proven reliability of the market-leading 6500 Packet-Optical Platform, deployed by more than 500 operators around the globe. The 6500 underpins much of today's critical communications infrastructure, addressing the requirements of service provider, Internet Content Provider, enterprise, government, finance, healthcare, utility, media and entertainment, and research and education networks.

WaveLogic Encryption delivers a simple-to-implement, ultra-low-latency, wire-speed optical encryption solution that integrates directly into the transport network. With the flexibility of the 6500, providers can select the optimal shelf size to cost-effectively meet their site-specific capacity, space, and power requirements. With its set-and-forget approach, encryption is always on, ensuring the highest level of security and eliminating human error that can result in sensitive patient data being sent over the network unencrypted. As is demonstrated in Figure 1, WaveLogic Encryption ensures all critical patient data traveling across the healthcare network is always secure.

The solution is validated externally, and independently certified by a third party to ensure it is implemented using industry-standard algorithms and advanced security features. It provides a FIPS-certified AES-256 encryption engine with standards-based authentication mechanisms (such as X.509 certificates), enabling seamless integration into existing enterprise PKIs, as well as support for the latest public key cryptography algorithms including Elliptic Curve Cryptography (ECC). Additionally, the hardware and software components of the cryptographic modules are compliant with FIPS 140-2, offering the assurance that the encryption solution complies with all aspects covered by this comprehensive evaluation, including encryption algorithms, key exchange mechanisms, and user authentication. For enhanced data protection, two distinct and independent sets of keys are used for authentication and data encryption functions, with a fast encryption key rotation interval of seconds instead of minutes. The AES-256 data encryption session keys are autonomously negotiated and rotated every second, independently, without impacting traffic or throughput, and without user intervention.

WaveLogic Encryption Solution
Download application note

WaveLogic Encryption enables deterministic, ultra-low-latency in-flight data encryption that supports the full range of critical healthcare applications, allowing healthcare providers to:

- Seamlessly access critical patient data, interconnect resources, transfer massive imaging files, and meet compliance requirements over one highly secure network
- Comply with HIPAA requirements for protecting patient health information through FIPS-certified encryption of all in-flight data 24/7
- Leverage flexible bandwidth offerings at wire speed with no impact on healthcare application performance, from patient portals to EMRs and PACS networks
- Benefit from a simple, integrated encryption management approach that partitions encryption management from transport management to allow the service provider or healthcare organization networking team to manage the network while the security team maintains full control of the encryption security parameters associated with their critical patient data, issuing new keys or certificates as required by their security policies

Encryption of data at rest and in flight is not mutually exclusive. Both are typically implemented in conjunction and complement each other as part of a holistic security strategy. When deploying an in-depth, multi-tier data security strategy, healthcare organizations must understand the use case, application, and compliance requirements. They should also ensure their chosen software or technology adheres to the highest level of encryption standards and algorithms, such as ECC algorithms. Ciena's WaveLogic Encryption solution combines a high degree of flexibility and security, with ease of operation and administration, to enable a cost-effective, ultra-low-latency wire-speed encryption solution for efficient and secure collaboration between healthcare stakeholders.

Visit the Ciena Community
Get answers to your questions