Trusted Cyber Technologies

THALES

High Assurance Encryption for Healthcare Network Data

White Paper

A Connected Healthcare Industry

The healthcare industry has adopted a range of new technologies, as the government and private healthcare providers alike seek to realize operational efficiencies. The need to provide an improved standard of patient care sits alongside stated objectives to improve workforce productivity, reduce management costs and better leverage the opportunities presented by technology in an increasingly connected environment.

In an industry typified by geographic, stakeholder and systems diversity, technology can present as many challenges as it does solutions. However, the ubiquitous availability of connectivity, device proliferation and a concerted effort to centralize patient records has finally put the healthcare industry in a position to exploit technology to the advantage of patients and clinicians alike. Information sharing, mobile access to patient records, remote diagnostics and collaborative case management are all helping to create better patient outcomes.

Healthcare IT infrastructure has become borderless; with clinicians, government agencies, advisory boards, independent consultants, office managers, patients and service providers connected via a wide range of devices. As healthcare stakeholders and systems become better connected, the volume of healthcare data created, processed, analyzed and stored is greater than ever. The increased use of HD video – either for collaboration or patient monitoring – is also changing the nature and format of healthcare data.

Big data requires big data networks, so there has been a corresponding increase in the adoption of Cloud and data center services; all leveraging high-speed Ethernet and Fiber Optic networks to exchange huge volumes of potentially sensitive information. However, the benefits of connectivity are overshadowed by the increased risk to patient and stakeholder privacy and data security.

It has emerged that the healthcare industry has become heavily reliant upon data security. Organizations are constantly challenged to address patient privacy, data theft, loss of intellectual property, systems disruption, financial penalties and loss of trust; all amidst an evolving landscape of cyber-crime.

Healthcare Data is a Valuable Commodity

The sensitive nature of healthcare data, which not only includes financial details, but medical histories, dates of birth, addresses etc. makes it a valuable proposition for potential cyber criminals. The loss of healthcare data comes at a cost.

The breach landscape has changed dramatically. The majority of data breaches used to be down to human error, system's glitches and lost or stolen devices. By 2016, this had changed and the majority were now a result of malicious, large-scale hacking events. Healthcare data is often used for the purposes of identity theft, but the depth and detail of the information available also enables criminals to participate in large scale fraud or extortion.

Targeting Healthcare Data

The high-speed networks used by modern healthcare organizations are becoming increasingly complex. Multiple devices and links feature across a variety of network technologies, protocols and topologies. With this complexity comes risk. Cyber-criminals exploit areas of weakness, either within the healthcare organization itself or at the point it connects with third party networks. While the sharing of patient records and management information has become a part of day to day communications, healthcare providers often have little or no understanding of external organizations' data security.

As the health industry evolves, the security of legacy infrastructure is not always given due consideration during the integration phase. At the same time, the adoption of high-speed Ethernet networking devices that are running older versions of software introduces weak points into the network.

With the Internet of Things, more and more devices are becoming connected. The more access points a network has, the more vulnerable it is. Remember, high-speed, fiber optic networks are not inherently secure.

Finally, networks that depend on hybrid devices with encryption "built-in" (such as routers and switches) are exposing themselves to even greater risk. In 2016, Cisco discovered a vulnerability in over 840,000 network devices that exposed the devices' memory to potential hackers.

Healthcare data is a high-value, low-risk target for cyber-criminals. The data itself has a high resale value and is often found traversing either an unsecured network or one where security policies and tools have been applied inconsistently.

As the healthcare industry embraces mobility, cloud computing and data center services, it is exposing itself to a new range of data security risks. Use of public cloud infrastructure (typically leveraging Layer 3 Internet links) puts the data itself out of the organization's control. It is while this data is in motion that it is at its most vulnerable.

Protecting Healthcare Data

So, how can healthcare organizations ensure their network data is secure? The answer is simple. Encryption. By encrypting the data before transmitting it across the network, it is possible to ensure both security and integrity.

By encrypting network data in motion, healthcare organizations are assured that, should the network be breached, the data itself would be rendered useless to unauthorized users. Sensitive information would remain secure, regardless of whether the network was public or private. While there may be some debate as to the risk/reward balance of using encryption in certain industries, the sensitive nature of the data transmitted within the healthcare industry demands maximum security.

In addition, the healthcare industry is subject to strict data protection and regulatory compliance obligations. A breach of which could result in serious financial or operational penalties.

High Assurance Encryption

Not all encryption solutions are the same. The critical nature of healthcare networks (and the data they carry) requires a robust encryption solution that provides certified, high-assurance network security and maximum network and application performance; without compromise.

Thales TCT offers high speed encryptors include the security assurance of certification by leading independent testing authorities. They are certified as suitable for government and defense use by FIPS, Common Criteria, and NATO.

Hybrid network encryptors, such as routers and switches with embedded encryption, do not provide robust network security. In some cases, they may even expose the network to device vulnerabilities and other performance inefficiencies. Truly robust encryption solutions require more than certification alone. Thales TCT high speed encryptors feature the following essential attributes:

- Secure, tamper-proof hardware - dedicated to encryption
- State-of-the-art, client-side encryption key management
- Gapless, end-to-end link and network encryption
- Authenticated, standards-based encryption algorithms

Regulatory Compliance Versus Risk Tolerance

The network encryption security conundrum for many healthcare organizations is clear: compliance versus risk tolerance - a.k.a. "how big must the risk be before we invest in encryption to avoid non-compliance?"

Healthcare decision makers have traditionally needed to weigh up several factors in the risk vs. compliance vs. investment equation. Most of these factors concern either the potential impact of a breach or the financial and managerial cost of implementing a robust data security solution.

Although there is no single healthcare regulatory framework, the security compliance standards introduced by government are very high and penalties for non-compliance or successful data breaches are substantial.

The costs associated with a data breach could be felt directly, or indirectly by the breached organization and include:

- Business disruption
- Financial penalties
- Loss of privacy
- Risk to patient wellbeing
- Loss of reputation
- Compliance failure
- Criminal prosecution

With the availability of certified high-assurance encryption solutions, this is no longer an issue. Encrypting high-speed data networks has never been simpler, with ease of management and "set and forget" implementation.

Furthermore, high-assurance encryption does not come at the expense of bandwidth or network performance. SafeNet high speed encryptors feature near-zero latency, are transparent to other network devices and have zero network overhead.

Whether you are looking for a desktop device to enable encryption anywhere, or a carrier-grade, rack mounted device for ultra-high speed networks; Thales TCT high speed encryptors low management and support costs, interoperability and backwards compatibility contribute to an extremely low total cost of ownership (TCO).

Healthcare Compliance

Regulatory bodies have been put in place to ensure the security, confidentiality, integrity and availability of patient and employee information. They set out an industry standard for protected health information (PHI) that prescribes physical, network and process securities required for compliance.

The compliance landscape is rapidly evolving within the healthcare industry and organizations are playing catch-up as they move to implement more stringent guidelines and legislation. Healthcare organizations need to adopt a data-first approach to network security if they are to avoid non-compliance of the emerging standards, including Health Insurance Portability and Accountability (HIPAA)and Health Information Technology for Economic and Clinical Health Act (HITECH).

HIPAA is designed specifically to address the security of healthcare information that is held or transferred in electronic form. It outlines the obligations of an organization in respect of ensuring the confidentiality, integrity and availability of all PHI it creates, receives, maintains or transmits.

These US healthcare industry data security regulations include criminal as well as civil prosecution for breaches. Criminal penalties range from $100,000 fine or five years in jail to $250,000 fine or 10 years' jail time.

Healthcare Industry Experience

Thales TCT high speed encryption technology is providing vital patient privacy, compliance and integrity of data traversing the latest generation of high-speed networks in healthcare organizations:

1. A US, $5 billion not-for-profit healthcare provider demanded secure access to its medical and management applications for more than 1,500 clinicians. Robust encryption, ease of management and cost efficiency were essential to the organization.
2. A large US-based healthcare insurer and its IT&T subsidiary saw the damage suffered by a competitor after a data breach. It subsequently mandated the implementation of 'stronger, maximum data security measures'.
3. A US-based healthcare network included 3,500 systems users and numerous data network links, over which a full range of medical and patient information is transmitted and shared. A robust network encryption solution was required to deliver a relatively low total cost of ownership over five years, improved security, flexibility and seamless integration.
4. A US not-for-profit veteran's healthcare service provider sought to enhance its patient care by providing 24/7 patient monitoring. The introduction of an HD CCTV monitoring system demanded maximum security without impacting on real-time video streaming.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com