CYPHRE
a RigNet company

ROBUST ENCRYPTION CURES HEALTHCARE DATA PROTECTION ILLS

Privacy is Paramount for Sensitive Patient/Customer Information

Patient information is a favorite target of cybercriminals. A health record is 50 times more valuable to a cybercriminal than a Social Security number.

Unfortunate healthcare providers, insurers, and other authorized parties frequently suffer breaches at the hands of global bad actors. Cyberattacks compromise the personal health information (PHI) of millions of people annually. Nothing is more vital than finding a way to share patient data with absolute security, while maximizing productivity.

Hospitals, insurers, and local healthcare providers must make better protection for PHI a top priority. Adding a formidable layer of security against the continued onslaught from hackers is the only way forward, but unique challenges abound.

Connectivity between internal networks and trusted third-parties creates many potential open doors to cyberattacks. In fact, any exchange of sensitive health information across organizations or within a hospital system is vulnerable. Even information transferred physically via flash drives is exposed to copying and theft.

The value of IoT-connected healthcare devices lies in their ability to allow physicians to efficiently monitor patient health, while improving communications between physicians and patients. However, every piece of medical equipment and every device that is part of the healthcare Internet of Things (IoT) provides a potential unsecured access point through which hackers may access the network and all its information. IoT data originates in variable file types and sizes, making it a complex matter to protect.

Data exposure and device failure can open manufacturers to compliance violations such as HIPAA and other regulatory guidelines.

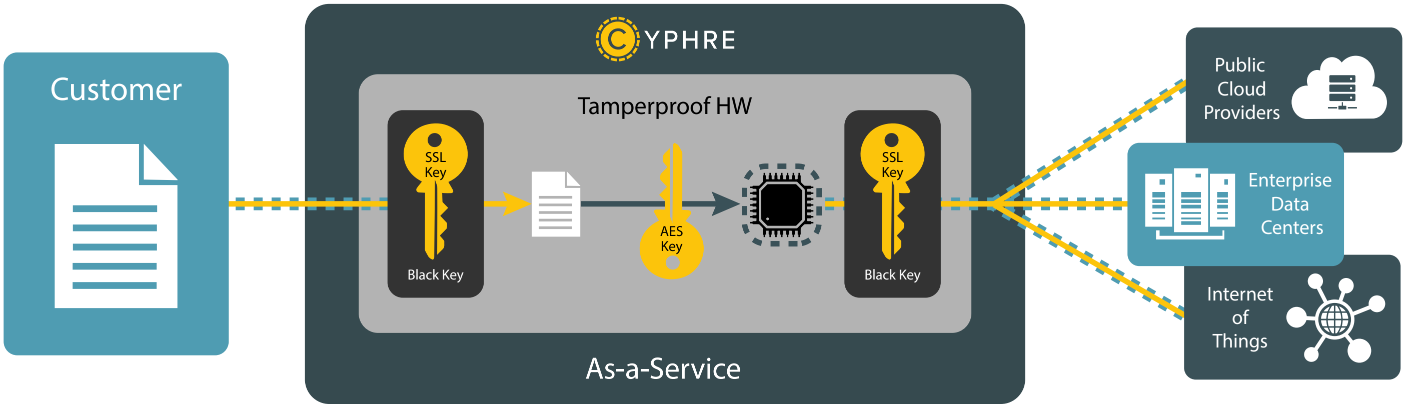
Add to these challenges today's stringent compliance, reporting, and regulatory requirements and the demand for guaranteed 100% cloud data availability and control.

Building Immunity Against Network Infections

Fortunately, there are many examples where the proper application of encryption technology across the entire IT infrastructure can fully secure healthcare information, both behind firewalls and during transfer over private intranets or the public Internet.

Whether at rest or in motion, data is best protected by encryption. Encryption provides the highest level of security, but the way encryption is achieved matters vitally. When single encryption software keys are memory resident on a host server, they are vulnerable to attack and data can be stolen. This presents a well-known vulnerability and major opportunity for hackers to exploit.

> **89% of healthcare** organizations have experienced a data breach, which involved patient data being stolen or lost, over the past two years.



Cyphre's BlackTIE® technology augments vulnerable single encryption keys with hardware-encrypted Black Keys to nullify breaches, hacks, and other cybersecurity threats. Chip-resident Black Keys are completely isolated from hacker exposure. BlackTIE® assigns one key per file rather than one key for many files, establishing maximum protection for encrypted data at rest and limiting the 'blast radius' of any breach. With authentication taking place on the hardware, no software installation is required on the host server. By offloading encryption activities from the host system Cyphre hardware increases encryption performance.

BlackTIE® also protects traffic as it leaves the network. Cyphre's automatic protection of information in transit requires no proactive action by the teams moving the data. This establishes a "zero knowledge" stance for employees, eliminating them as a possible point of exposure. Network administrators can easily monitor and control all file sharing activities within an organization, as well as integration with LDAP authentication systems.

Hardware-driven encryption from Cyphre protects enterprise data even if hackers break into the server, thus neutralizing a common breach technique that targets software-only security. Cyphre's crypto-hardware-based keys provide virtually unbreachable protection against common attacks such as cold boot attacks, malicious code, brute force attacks, and more.

Cyphre's BlackTIE® encryption technology is a powerful solution for healthcare companies moving critical files to the cloud. Cyphre uniquely safeguards both personal information and financial data from global cyberthreats of all types.

About Cyphre

Cyphre, a RigNet company (NASDAQ:RNET), is a cybersecurity company deploying disruptive data protection innovations by enhancing industry standard encryption protocols with our patent pending BlackTIE® technology.

www.cyphre.com @getcyphre Cyphre /getcyphre