

ENCRYPTION MAXIMIZES “CYBERSECURITY ROI” FOR FINANCIAL SERVICES

Ironclad Data Protection Pays Long-Term Business Dividends

With the average cost of a data breach heading north of \$6 million, ever-increasing cybersecurity threats combined with weak security protection can spell disaster for financial sector companies.

More than almost any other industry, financial companies are targets of internal and external cyberattacks. Financial services firms are hit by security incidents 300 times more frequently than businesses in other industries. Moving to a cloud computing environment, which inarguably offers tremendous benefits, significantly increases the danger of exposing private information to exploitation. When financial companies move key data and applications to a cloud service provider (i.e. Amazon Web Services), massive amounts of information are transmitted to and from cloud service providers (CSP) across corporate networks and the Internet on a daily basis. This presents a massive potential exposure threat to the most critically important wealth information: private account data.

More than almost any other industry, financial organizations must turn to world-class data encryption technology for protection of data at rest and in transit. Financial IT organizations must also ensure their data encryption strategy complies with government regulations and industry best practices.

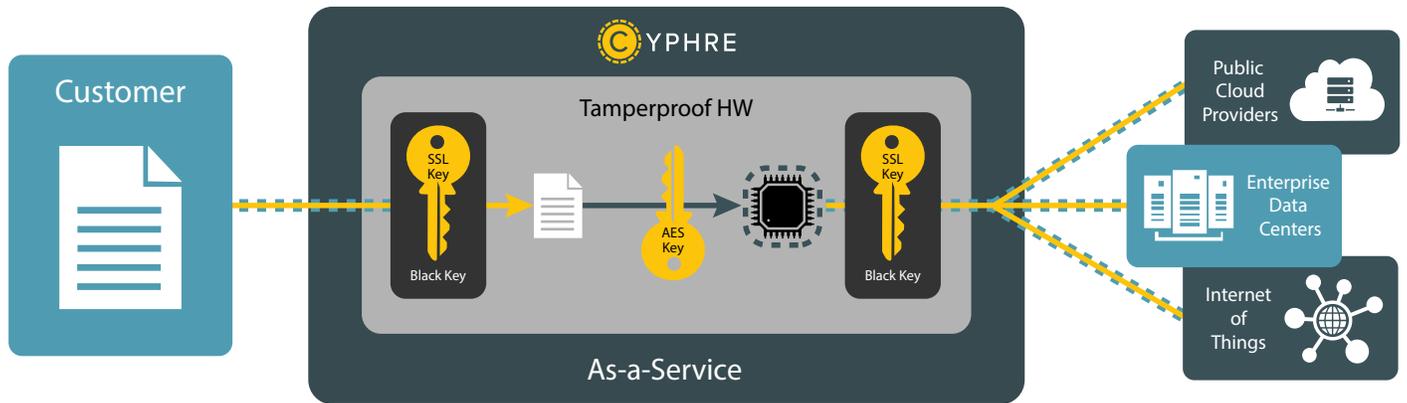
Banking on Encryption to Put Data in a Virtual Vault

Fortunately, there are many examples where the proper application of **encryption technology** across the entire IT infrastructure can fully secure financial 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.

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

“Financial services firms are hit by security incidents **300 times more frequently** than businesses in other industries.



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 provides a powerful solution for financial services companies moving critical files to the cloud. Cyphre uniquely safeguards clients from identity theft and unauthorized access to bank accounts and financial management systems. It enables financial institutions to abide by the privacy and security framework set out by the Federal Financial Institutions Examination Council (FFIEC).

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.

