CYPHRE
a RigNet company

PROTECT YOUR DATA WITH BLACKTIE™ ENCRYPTION

Patent-Pending Encryption Technology to Secure Your Cloud Data From Wide-Spread Threats

BlackTIE™ Benefits

Flexible Deployments

Deployment models include cloud, hosted, on-premises, suited and priced to meet IT requirements.

Embedded Protection

Integrated hardware-driven encryption and software interface improves speed and security.

Key Management Options

Zero Knowledge for key management with the option to control your own keys or give Cyphre control.

Black Key Encryption

Extra layer of encryption on top of TLS (data in-flight) & AES (data-at-rest) designed to ensure keys are never exposed in memory.

One File/One Key

BlackTIE™ uses a unique encryption key for each individual file rather than a single key for an entire account.

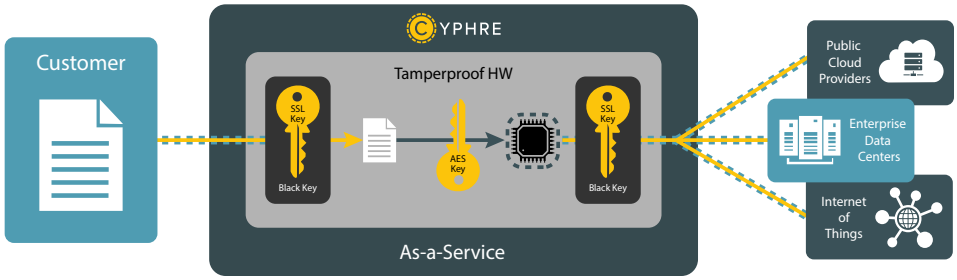
Enterprise Data Security

Enterprises endure malicious intrusions on a daily basis whether on employee computers, on the corporate network, or in the cloud. Millions of dollars spent annually on IT upgrades, insurance premiums, and compliance fines can be saved by employing Cyphre's BlackTIE™ encryption technology. Cyphre's BlackTIE™ technology augments vulnerable single encryption keys with hardware-encrypted Black Keys to nullify breaches, hacks, and other cybersecurity threats.

The largest threat to cloud data at rest and in flight is the period when security keys are memory resident on the host server. Cyphre's patent-pending BlackTIE™ technology augments vulnerable single encryption keys with hardware-encrypted Black Keys to render hijacked keys useless, thus nullifying the threat. Chip-resident Black Keys are completely isolated from hacker exposure, and in fact even from Cyphre. For more heightened security, BlackTIE™ uses a one-file/one-key approach to encrypting all data-at-rest.

$3.8 million
average consolidated cost of a data breach

Cyphre's BlackTIE™ technology leverages a threat mitigation appliance based on NXP Semiconductor's QorIQ processor. Hardware-based encryption protects enterprise data even if hackers access the server, neutralizing a common breach technique that targets software-only security. A browser-based interface along with desktop and mobile applications offers an intuitive user experience that maximizes productivity and collaboration.



CYPHRE
a RigNet company

Applications for BlackTIE™ Security

Enterprise File Sync & Share

Cyphre's BlackTIE™ encryption technology can be integrated into cloud storage solutions. This extra layer of protection secures any cloud-based collaboration at the individual, group and enterprise levels. This allows users to access, store, share and organize files from any device, while adhering to the organization's control and compliance standards.

Cloud Encryption Gateway

Cyphre's Cloud Encryption Gateway (CEG) leverages Cyphre's BlackTIE™ encryption technology to protect enterprises as they extend a diverse set of hybrid cloud services to their users. Best be defined as a Cloud Access Security Broker (CASB), the solution allows enterprises to ensure advanced encryption protection for any data resting in an array of public cloud storage and other critical applications.

Secure IoT Integration

Internet of Things (IoT) device offerings are expanding at unprecedented rates. Many of these are generating or acquiring sensitive data that is vulnerable to piracy in the cloud. With Cyphre, IoT devices incorporate BlackTIE™ encryption technology to securely store and manage cloud data.

BlackTIE™ Industry Applications

Technology
Cyphre's enterprise cloud security solution allows IoT product OEMs and other technology companies to embed BlackTIE™ encryption technology into their products and services, providing secure data management and protecting their clients.

Telecom
Cyphre's advanced BlackTIE™ encryption technology offer the necessary security to protect the increasing amount xof personal data being managed and to nullify attacks and to avoid the associated high costs and liabilities.

Healthcare
Medical records are ten times more valuable than data of other industries making the healthcare industry an enticing target for hackers. Cyphre's enterprise cloud security solutions enable medical providers to securely share patient data with peace of mind, convenience and reliability.

Law Enforcement
New security concerns are rising for law enforcement mainly due to cloud migration driven by limited resources and the need to securely and rapidly share information. Cyphre's BlackTIE™ encryption technology empowers secure data storage and integrity of sensitive information.

Finance
The financial sector is one of the most vulnerable industries to cyber breaches. Cyphre's enterprise cloud security solution safeguards consumers from identity theft and unauthorized access to bank accounts.

Defense and National Security
The United States government has experienced an alarming number of high-level data breaches in recent years. BlackTIE™ provides the additional layer of data security the government needs to nullify threats associated with storing and sharing some of the nation's most sensitive information.

About Cyphre

Headquartered in Austin, Texas, Cyphre cloud encryption technology provides the highest level of security for cloud data. Period. Product Offerings include Encrypted Cloud Storage and Enterprise Collaboration services, Secure IoT Integration and the Enterprise Cloud Encryption Gateway.

www.cyphre.com @getcyphre Cyphre, LLC /getcyphre

Copyright © Cyphre 2017