CipherCloud®
Trust in the Cloud™

Active Encryption addresses CSA Top Threats including:

- Account hijacking
- Credential theft
- Forced disclosure
- Data breaches
- Malicious insiders
- Insecure APIs
- Shared technology

cloud security alliance®

HEADQUARTERS:
CipherCloud
333 West San Carlos Street
San Jose, CA 95110

CONTACT:
www.ciphercloud.com
sales@ciphercloud.com
1-855-5CIPHER (1-855-524-7437)
linkedin.com/company/ciphercloud
Twitter: @ciphercloud

CIPHERCLOUD ACTIVE ENCRYPTION™

Your data is active—your encryption should be as well

CipherCloud Active Encryption™ is uniquely suited to enable cloud adoption providing the highest levels of security with exclusive enterprise control. While encryption is used in many contexts, it is only effective if properly deployed and following security best practices.

Go Beyond Encrypting Data at Rest

Many cloud providers encrypt data at rest—a useful step if the physical media is stolen. However, most cyber threats today target the application layer—not storage. Merely encrypting data at rest does not protect against the top threats published by the Cloud Security Alliance (CSA) including credential theft, account hijacking, insecure APIs, privileged users, shared technology or forced government disclosure.

To solve these problems you need security that is persistent and only you control. With CipherCloud, enterprise decide what to encrypt with granular policy controls, and never share the keys. Active Encryption maintains the functionality of encrypted data, for searching, sorting, reporting, third-party tools, and can even control data encrypted on mobile devices. When evaluating any encryption solution you should ask these questions:

Does it Protect Multiple Clouds?

Cloud providers typically only worry about protecting one cloud—their own. But enterprises increasingly need consistent visibility, policy controls, data protection and compliance across a wide range of business-critical clouds. CipherCloud delivers true multi-cloud security enabling you to apply policies across clouds, and protect data consistently in multiple applications.

Where is Data Encrypted?

When CSPs offer encryption it only applies to data at rest. This leaves significant exposure as the application, admins, APIs, external processes, and more can always access the clear-text on-demand. CipherCloud Active Encryption is persistent and complete, covering data in transit, data in use, and data at rest, as well as data sitting on mobile devices.

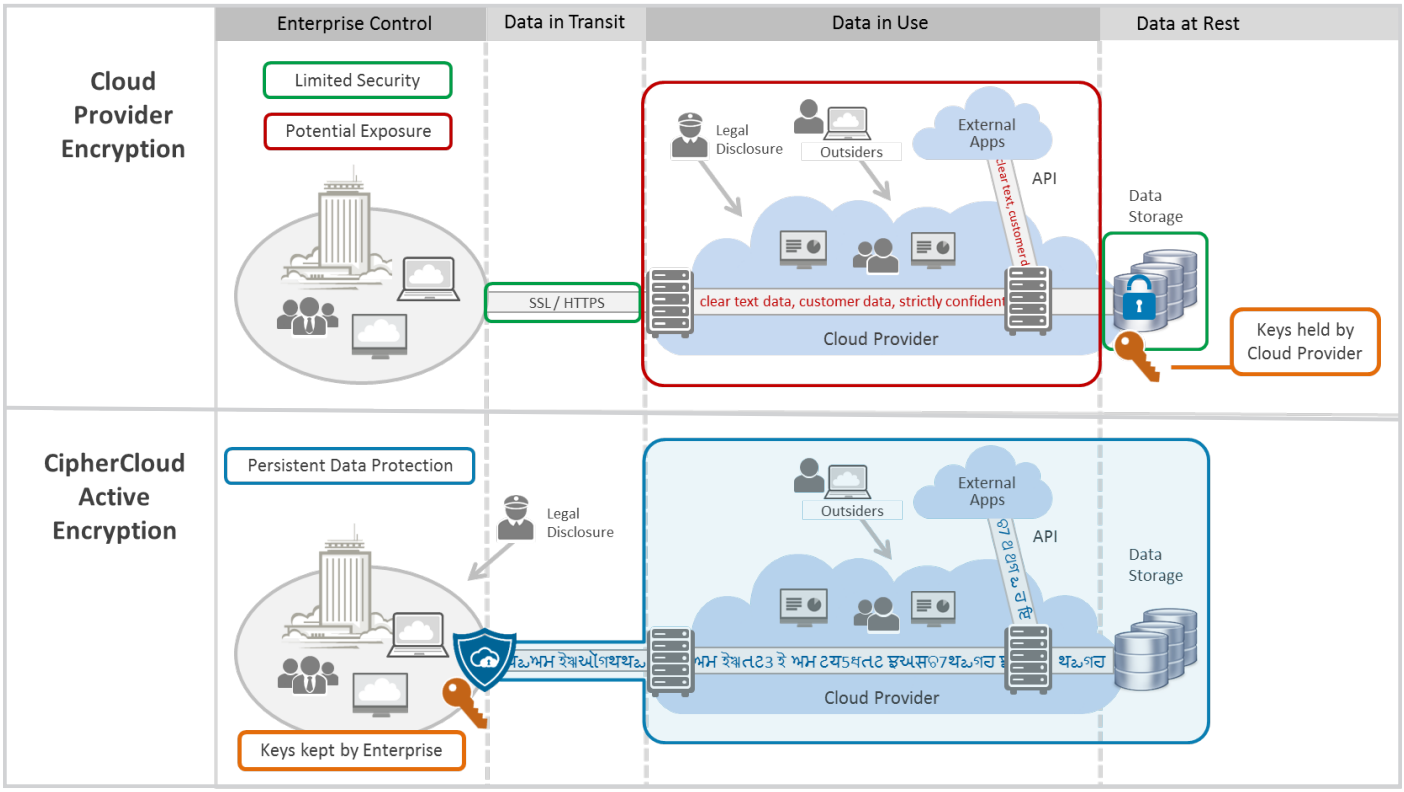
Who Protects the Data?

Effective security requires a separation of duties. If the cloud provider encrypts and stores your data, it can and will access it—intentionally, automatically, by accident, through external tools, or even through court orders. You are always responsible for your data, regardless of where it goes, and with CipherCloud you directly control encryption and never relinquish control to outsiders.

Are There Protection Gaps?

Beyond the fundamentally different security models, cloud provider encryption often has additional gaps in protection that can multiply your exposure. Because the application layer can always access the encrypted data so can rogue insiders, or account hijackers with stolen credentials. In addition, search indexes are often unencrypted, keys reside persistently in application memory, and data is usually decrypted in external applications and activity logs. Active Encryption eliminates all coverage gaps. From when the data leaves your controls to when it returns it is never accessible until you decide to unlock it.

All trademarks are property of their respective owners. CipherCloud | ©2016



Are Keys Shared?

With cloud provider encryption, the keys are always shared, or controlled completely by the CSP. Some systems provide customers with limited sharing control or work with cloud-based HSMs, but in practice, the cloud application always has access to keys and the protected data. CipherCloud follows security industry best practices providing customers with exclusive key ownership with standards-based key storage or integration with on-premises enterprise key management tools.

Can You Control Data Residency?

In some countries there are strict requirements that highly sensitive data remain on-premises and never go into the cloud. CipherCloud tokenization meets the most stringent data residency requirements, substituting random values in the cloud, while retaining sensitive data fields in an on-premises database. No cloud-provider security solutions support tokenization.

Will This Meet Regulatory Compliance?

Most regulations do not specify which technologies to use, but there is a strong consensus among compliance officers, auditors and regulators that encryption, if properly applied, is an important component of compliance. Cloud provider encryption does not meet most regulatory mandates because the data owner does not maintain exclusive control. But CipherCloud Active Encryption has been deployed by hundreds of regulated organizations to meet requirements including GLBA, PCI, HIPAA, and global data privacy laws.

Does the Solution Support all my Integrations?

Cloud-based encryption solutions typically do not integrate with on-premises systems, and have limited integration with extended clouds. CipherCloud has extensive experience supporting hundreds of integrations with on-premises and third-party clouds, extending effective data protection to your entire ecosystem.

Persistent end-to-end encryption covers data in transit, data in use, data at rest, and data on mobile devices.

	Cloud Provider Encryption	CipherCloud *Active* Encryption
Clouds Protected	**Single-cloud protection.** Different systems and policies are required for each cloud.	**Multi-cloud protection** across a wide range of business applications. Build policies once and apply them consistently across dozens of clouds.
Where is Data Encrypted?	**Only encrypts data at rest,** when it is stored on a server. Whenever data is accessed, or processed it's in the clear.	**Active encryption is persistent—always on.** From when it leaves your control until it returns, your data is never exposed.
Who Protects the Data?	The same entity encrypts the data and holds the keys—not a security best practice.	**Provides a critical separation of duties.** You protect your data and make all decisions about who can access it—critical for compliance.
Protection Gaps	Unencrypted data is exposed to account hijackers, CSP admins, third-party tools, law enforcement, and more. Also, search indexes are not encrypted, and keys reside persistently in memory.	**No protection gaps.** Data always remains encrypted while in use, and is never accessible to unauthorized outsiders. CipherCloud delivers true zero-knowledge protection.
Are Keys Shared?	**Keys are controlled by the CSP.** Some systems allow customers limited key sharing, but the provider always has access.	Keys are never shared—controlled exclusively by the customer.
Data Residency Control	**None.** Customers cannot retain select data on-premises.	CipherCloud **tokenization** meets strict data residency requirements, substituting random values in the cloud, while retaining sensitive data on-premises.
Regulatory Compliance	Does not meet requirements for most data protection and data privacy laws.	Deployed by hundreds of organizations to meet requirements GLBA, PCI, HIPAA, and global data privacy laws.
On-Premises Integration	Not supported	Extensive support for on-premises systems such as data loaders and custom apps.
Ecosystem Support	Limited	CipherCloud supports over 100 third-party tools and external cloud applications.

CipherCloud is the industry leader in enabling cloud adoption by ensuring data protection, visibility and compliance. CipherCloud delivers a comprehensive multi-cloud security platform that integrates advanced data protection, content control, monitoring, cloud discovery and risk analysis. As the technology pioneer in searchable, strong encryption and tokenization technologies, CipherCloud is the only cloud security vendor to have received FIPS 140-2 validation.

CipherCloud has unrivaled market leadership with over 3 million business users across 25 countries, in industries including banking, finance, insurance, healthcare, pharmaceuticals, telecommunication and government.

CipherCloud
Trust in the Cloud™

FIPS VALIDATED 140-2

WP-CC-VSCSP-20160526
CipherCloud | ©2016
All trademarks are property of their respective owners.