White Paper

The 10-Minute Guide to Cloud Encryption Gateways

What They Are, How They Work & Why You Need One

CipherCloud®
Trust in the Cloud™

333 W. San Carlos Street
San Jose, CA 95110

Summary

Today, virtually every type of business application is available in the cloud—sales, marketing, service, financials, human resources, supply chain, procurement, collaboration, and analytics to name a few. However, the explosive growth in cloud applications has far outpaced the technologies used by most cloud application providers to protect them, and as a result, many organizations have concerns about security, privacy, residency, and compliance with information stored in the cloud. This has led some organizations to consider delaying their move to the cloud. However, there are innovative solutions being developed that are addressing these concerns through a technology called the cloud encryption gateway from CipherCloud.

Everyone is short on time, so we've designed this whitepaper with an easily digestible format to give you just the information you need to know about cloud encryption gateways in 10 minutes or less.

"Cloud encryption gateways that can be configured to encrypt or tokenize data are needed to reduce risk and allow businesses and governments to go beyond the firewall and adopt public and private clouds applications."

Lawrence Pingree
Research Director
Gartner

Contents

What is a Cloud Encryption Gateway?

Figure 1: On the left, unauthorized users see only encrypted, unreadable text. On the right, authorized users can see the same data that has been decrypted.

Most cloud application providers store sensitive data "in the clear," meaning it's stored in an unprotected format. This is a big concern for Chief Information Security Officers (CISOs), compliance organizations, business decision makers, and everyone else in your company that understands how a data breach can result in the loss of sensitive information, damage your brand and company, and potentially cost you millions in exposure and possible legal costs.

The CipherCloud Encryption Gateway provides a way for companies to encrypt sensitive information as it moves to any cloud application and then decrypt it again as data is delivered to end users. This protects the data from being accessed by other tenants in a Software as a Service (SaaS) solution, SaaS administrators, and other unauthorized personnel inside and outside your company. This revolutionary technology maintains the cloud application user experience, with near zero latency, and without making any changes to the cloud application itself.

How the CipherCloud Gateway Works

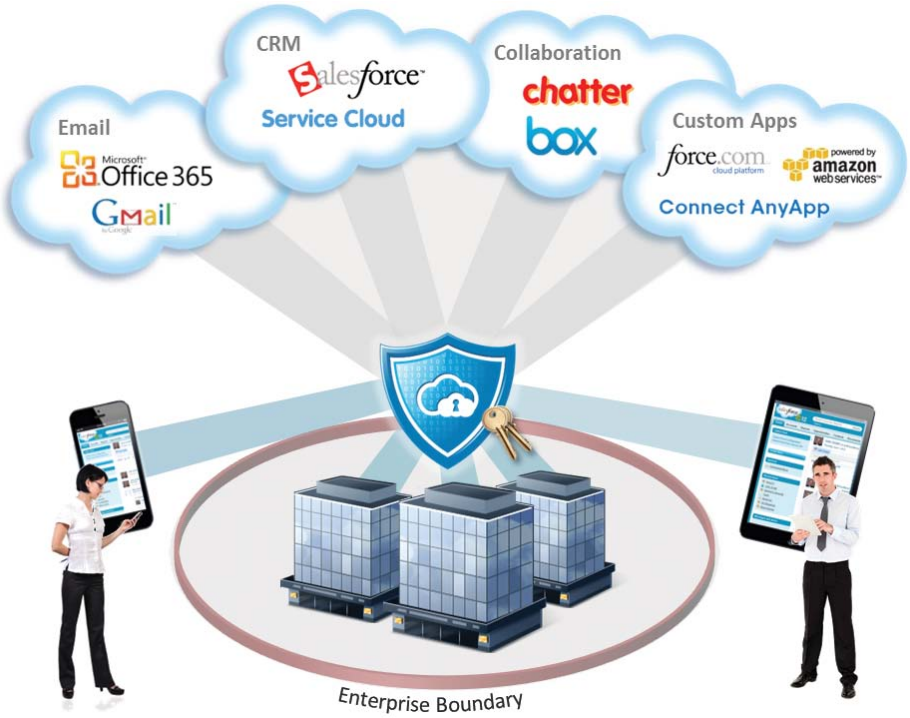


Figure 2: The CipherCloud Gateway encrypts sensitive data, in real time, before it's sent to the cloud.

CipherCloud takes a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network. The CipherCloud Gateway is deployed between your users and your cloud applications and acts as a reverse proxy server that monitors all incoming and outgoing traffic (e.g., HTTP, SMTP, SOAP, and REST) between enterprise users and all of your cloud applications. The CipherCloud Gateway examines all outgoing cloud requests, in real time, to identify sensitive data, encrypt or tokenize that data, and then forward the modified request to the cloud application. Similarly, encrypted or tokenized data returning from the cloud application is converted, again in real time, into cleartext (i.e., text that can be read) prior to being displayed to the end user.

How the CipherCloud Gateway Works, Cont'd

"That's a small price to pay to keep regulated or sensitive data secure"

The CipherCloud Gateway provides multiple forms of encryption and tokenization based on the level of protection needed. This includes AES-256 strong encryption, which is the highest level of protection available. You can identify which cloud data you consider sensitive, such as proprietary information, personally identifiable information such as a national ID number or a social security number in the U.S., or other regulated data. When that data is posted into the cloud application, the Gateway applies the encryption method you select to protect the data before it leaves the enterprise network. It's able to do this while preserving the formats of the data, such email and phone number formats, and maintaining native application functionality such as searching, sorting, and reporting.

The Cloud Gateway uses FIPS 140-2 validated cryptographic modules, which meets an exceptionally high standard for security required by many government organizations.

The CipherCloud Gateway also has integrated key management capabilities, where your company holds the keys, so that only you, not the cloud provider or other party, can access your sensitive data.

Protect Structured & Unstructured Data

CipherCloud not only protects structured data stored in cloud applications such as tables, rows, and columns of a database, but can also encrypt and tokenize email messages and attachments, including spreadsheets, PDF files, and JPEG graphic files. Prior to uploading files into a cloud application, CipherCloud's malware detection capability identifies and blocks infected files from being uploaded, enabling organizations to protect themselves against attempts by hackers to penetrate data-rich cloud environments.

CipherCloud also provides an audit trail of all activities, so that an organization can track what users are logging in, from what IP addresses, at what time, and what records they are accessing from cloud applications. In addition, CipherCloud can also secure remote and mobile access with devices such as Android, Apple iPhone, and RIM Blackberry smartphones.

Lightning Fast Performance

CipherCloud's encryption capabilities introduce a performance latency of less than 100 milliseconds, which isn't noticeable by end users (by comparison, it takes 300 to 400 milliseconds to blink). That's a small price to pay to keep regulated or sensitive data secure and under your own control.

It's About More than Just Security

Organizations across industries, including financial services, healthcare, technology, and the public sector, depend on the CipherCloud Gateway to address concerns about data security, as well as privacy, residency, and compliance.

Data Security
Breaches have become an everyday occurrence, and the costs are immense—estimated at over $194 per record according to the Ponemon Institute, the leading independent research firm on information security. With CipherCloud, you retain control of the data itself and its encryption keys. If a cloud application provider is compromised or your users' account credentials are stolen, attackers can see only the encrypted versions of your sensitive data.

Data Residency
There are dozens of laws that govern the flow and storage of data across national borders, including the EU Data Protection Directive, which broadly restricts the flow of personal information from within Europe to any country whose domestic laws do not provide an "adequate level of protection." CipherCloud has enabled cloud adoption in Germany, Canada, the United Kingdom, Lithuania, and other countries with strict data residency laws.

Compliance
Many regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require encryption of sensitive data. If the cloud application vendor has a breach, the sensitive data will remain encrypted and protected. User activity monitoring also gives you visibility into internal activity with sensitive data.

Data Privacy
According to Shahed Latif, a global steering committee partner for cloud computing at KPMG and author of the book, *Cloud Security and Privacy*, "Most cloud service providers absolve themselves from privacy concerns by saying 'We don't look at your data.'" With CipherCloud, you hold the keys, so even the cloud application provider doesn't have access to your data.

What to Look for in a Cloud Encryption Gateway

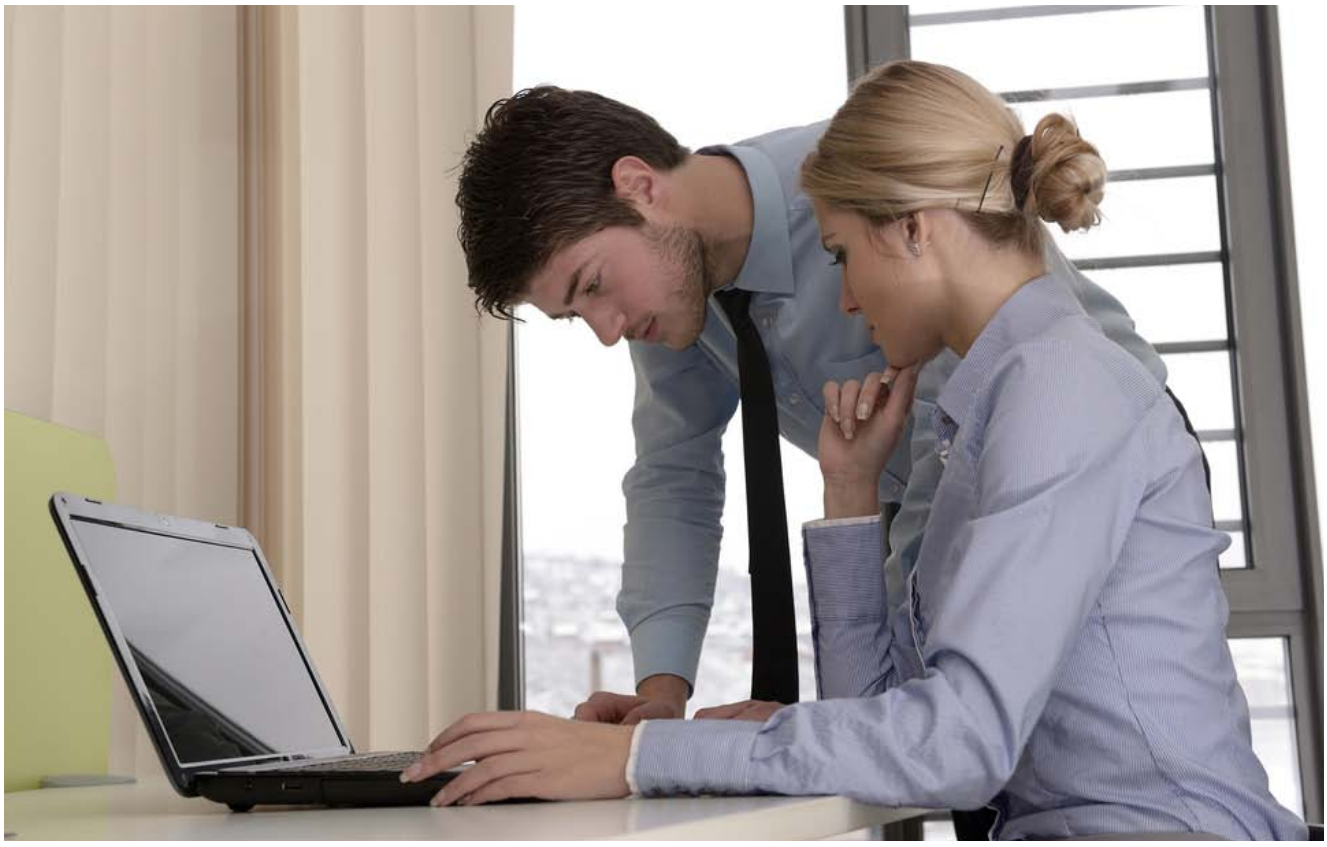
Cloud encryption gateways are rapidly evolving technologies where there are major differences among the different solutions. The following are key "must have" capabilities to look for.

"Must Have" Capabilities	Important Functionality
Enterprise-class Gateway with Support for All Clouds	• Application-aware to exercise granular control without breaking cloud applications • Stateless with near-zero latency • Deployable on-premise or in the cloud • Out-of-the-box connectors for multiple cloud applications • Enforce unified data protection policies across any cloud application, and over any communication protocol (HTTP, SMTP, SOAP, RESTful, etc.)
Strong Encryption & Tokenization	• AES-256 strong encryption • FIPS 140-2 compliant • Robust key management
Retain Cloud Application Capabilities	• Operations preserving: indexing, searching, sorting, and reporting • Format preserving: strings, dates, telephone, email, and domain names
Mobile Device Support	• Support for remote employees regardless of the device: laptops, tablets, and smart phones • Support for the latest technologies, including HTML5 applications
Multiple Cloud Application Support	• Application-aware to exercise granular control over application data • Support for Salesforce, Force.com, Chatter, AWS S3, Google Gmail, and Microsoft Office 365 • Connectors for Yammer, Jive, and SuccessFactors
Expanded Cloud Security Access Brokerage Capabilities	• Malware protection • Event and transaction logging • Data leak protection (DLP)

All of these capabilities are provided by the CipherCloud Gateway.

Take the Next Step

Now that you've invested ten minutes in understanding the basics about the CipherCloud Encryption Gateway, take the next step by seeing a short demo at www.ciphercloud.com, or have your questions answered by a CipherCloud product expert by contacting us at +1.408.520.4937 and info@ciphercloud.com.



CipherCloud is the leader in cloud information protection enabling organizations to securely adopt cloud applications by eliminating concerns about data privacy, residency, security, and regulatory compliance.

Visit **www.ciphercloud.com**
for more information, online demos, or free trials.

Email **sales@ciphercloud.com** or call +1.408.520.4937

Corporate headquarters:
99 Almaden Blvd,
San Jose, CA
95113, USA