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, data residency, and compliance for information stored in the cloud. The CipherCloud platform provides a practical way for organizations to protect sensitive information before it goes to any cloud application, by leveraging a combination of encryption, tokenization, anti-malware, data loss prevention (DLP), and auditing capabilities. The platform provides a range of options to ensure the data is protected from unauthorized access, or accidental disclosure by cloud administrators, malicious users, or other third parties. This powerful technology secures sensitive information while maintaining the functionality and user experience of the protected cloud applications.

CipherCloud provides out-of-the-box integration with the most widely used cloud applications including Salesforce, Force.com, Microsoft Office 365, Google Gmail, Amazon Web Services (AWS), and Box. In addition, CipherCloud AnyApp provides the ability to integrate with any public or private cloud application.

This paper gives an overview of the capabilities of the CipherCloud platform as well as details on security, configuration, and data flow within typical network environments.
In order to secure data before it gets sent to the cloud, the CipherCloud platform must be in the path of the traffic to the cloud. There are a number of ways to achieve this, but the most common and convenient approach for enterprises is to implement a “reverse proxy”. A reverse proxy is a type of proxy server that receives requests from the clients, and then forwards them to the cloud application after applying information protection policies. The advantage of a reverse proxy is that it eliminates the need to modify existing network configurations on client machines.
The CipherCloud gateway is set up to intercept all requests and responses exchanged between users and the corresponding cloud applications such as Salesforce or Office 365. As part of the configuration, a new URL is assigned to the gateway, and users are directed to access cloud applications via this URL.

For example at Acme Corporation, the typical login URL to Salesforce - login.salesforce.com will be replaced with a similar URL that points to the CipherCloud proxy, such as salesforce.acme.com. After the CipherCloud gateway is installed and configured, if any user tries to circumvent the gateway and login directly to the cloud application, they will either be blocked due to access control policies, or they will see encrypted data within secured fields.

CipherCloud provides many options to configure how a user logs into the cloud application, what security policies are enforced, and what information needs to be protected.

When the gateway receives an outbound request to access the cloud:

- The gateway decrypts the SSL-encrypted request sent by a browser and examines the contents to determine what sensitive data the request contains (based on the policies and rules already configured for a CipherCloud installation).
- Sensitive information in the request or query is encrypted or tokenized based on defined rules. CipherCloud also examines attachments and any uploaded files and processes the information or files accordingly.
- A log entry is created for this request in the user activity monitoring logs.
- Lastly, CipherCloud rewrites the HTTP header and places the message in a new envelope, along with a new address to send the request to the cloud application, and also sends along an updated cookie to reflect the new domain.
Coming back, the cloud application responds to the request it received from a user by sending back an HTTP response along with the relevant cookies (if applicable). CipherCloud rewrites the cookies appropriately to provide the correct path for the customer site, rewrites the headers in the HTTP response, and replaces any encrypted or tokenized values with plain text values. In addition, the CipherCloud gateway intercepts any file downloads and email and processes them accordingly.

The CipherCloud gateway processes both cloud requests and responses in real-time without any noticeable delay, and without persisting any session information. By caching static content such as style sheets and graphics at the gateway level, CipherCloud can actually improve performance of cloud applications.
The two distinct approaches to data protection are encryption and tokenization. Encryption is the process of transforming plain-text information using a mathematical algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually known as the key. This ensures that any sensitive data that ultimately resides in the cloud is stored as cipher text. What’s stored in the gateway is only the encryption key, so customers maintain control of the keys and can access data in an authorized manner, which satisfies data privacy, compliance and residency concerns for many enterprises.

With tokenization, randomly generated values are substituted for the original data, which never leaves the enterprise. These “tokens” that are stored in the cloud look like actual data, have no mathematical correlation to the original data. The original data and mappings for the substitutes are stored locally in database. Tokenization is useful for the most stringent regulatory requirements in countries with strict data residency laws.

The following table outlines the key differences between encryption and tokenization in more detail:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Encryption</th>
<th>Tokenization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Storage</td>
<td>In the cloud - encrypted</td>
<td>On-premises – in a local DB</td>
</tr>
<tr>
<td>Architecture</td>
<td>Stateless – no session information or data stored</td>
<td>Stateful – data is stored in a local database</td>
</tr>
<tr>
<td>Scalability</td>
<td>Easy to scale without replication or synchronization</td>
<td>Requires real-time replication of databases</td>
</tr>
<tr>
<td>Latency</td>
<td>Near-Zero</td>
<td>Low-Medium (dependent on network throughput and deployment architecture)</td>
</tr>
<tr>
<td>Cost Overhead</td>
<td>Low – requires a single virtual server.</td>
<td>Medium- requires larger servers, databases for persistent storage, backup and DR services, and more administration.</td>
</tr>
</tbody>
</table>
CipherCloud uses enterprise-grade, standards-based AES 256-bit encryption, while still preserving the functionality of applications, maintaining searching, sorting, and other capabilities.

The AES (Advanced Encryption Standard) was established by U.S. National Institute of Standards and Technology (NIST) in 2001 and is deployed in the U.S. Government and organizations globally. AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES encryption has been certified by NIST under FIPS 197. In addition, CipherCloud is in the certification process for FIPS 140-2.

The encryption algorithms offered by CipherCloud have been publicly published and extensively reviewed and tested by many independent organizations. In addition, CipherCloud’s implementation has been independently assessed by a world renowned cryptographer, and has gone through rigorous testing, code review and validation by dozens of major enterprise customers including 5 of the world’s 50 largest banks.

Preserving application functionality
 CipherCloud uses patented technology to provide granular control over the level of encryption and searchability for specific pieces of information. Data can be encrypted on a per-field, per-word, or per-character basis with configurable variables for random or predefined number of initialization vectors (IVs) as well as configurable use of order-preserving hashes (one-way functions for a specified number of leading characters). In addition, CipherCloud provides options for local indexing of selected data to optimize search functions. All of these options can be fine-tuned to meet the precise security requirements of each organization.

Encryption with the CipherCloud gateway

CipherCloud uses proprietary technology to provide granular control over the level of encryption.
CipherCloud provides enterprise-class key management in compliance with NIST SP 800-57 standards. Multiple key storage options allow keys to be stored securely on the CipherCloud platform or stored separately on a KMIP-compliant key management server.

Keys stored within the CipherCloud platform have multiple layers of protection. First, administrative access to the server is password-protected. Information about key configuration is kept on the server in an encrypted configuration file, accessible only to administrators. The actual encryption keys are locked within a secure key store on the CipherCloud platform.

CipherCloud provides capabilities to split keys between multiple custodians (to reduce internal threats) as well as key rotation and expiration without affecting legacy data.
**Tokenization Details**

CipherCloud provides seamless integration for either encryption or tokenization as well as a range of other security capabilities. With tokenization, randomly generated values are substituted for the original data, which never leaves the enterprise. The original data and mappings for the substitutes are stored locally in a JDBC-compliant databases such as PostgreSQL, MS-SQL or Oracle.

CipherCloud’s tokenization is configurable on a per-field, per-word, or partial field basis. Multiple tokens can be generated for repetitive words or strings to prevent frequency analysis.

CipherCloud’s encryption and tokenization solutions offer comparable levels of security. Tokenization has more limited application to meet stringent data residency regulations or corporate policies that require specific types of data not leave the organization, even if encrypted. Encryption generally offers lower overhead, higher performance, lower latency, and greater scalability because it is stateless and does not require data synchronization or replication. Tokenization also introduces additional security requirements for the local database to be secured from insider threats.

---

**Malware Detection**

With built-in cloud malware detection, CipherCloud provides real time protection against viruses, spyware, trojans, bots, rootkits, and more.

The CipherCloud platform scans all in-bound and out-bound cloud content for malicious code and cleans and/or quarantines infected content on-the-fly.

Signatures are updated several times a day to provide zero-day malware protection with easy access to all protection status information and settings.
User Activity Monitoring

To satisfy compliance and forensics requirements, and provide customers with peace of mind, the CipherCloud platform monitors all user interactions across all clouds and transparently captures data to generate an automatic audit trail of all user activity.

CipherCloud supplements the logs provided by Cloud Provider and logs all “write” actions (and optionally all “read” actions). User activity logs can then be fed into existing log management solutions. For specific cloud interactions, the CipherCloud platform records the user involved in the activity, a timestamp capturing the date and time, what actions users performed, and what records they accessed. In addition, CipherCloud records both the source and destination IP addresses of user activity.

Data Loss Prevention (DLP)

CipherCloud provides out-of-the-box DLP capabilities and can also integrate with enterprise DLP solutions (such as Symantec and RSA). Because the CipherCloud platform is inline and scanning content, DLP policies can be enforced to protect personally identifiable information (PII), personal health information (PHI), credit card data, financial transactions, or intellectual property. CipherCloud provides a range of enforcement options including encryption, tokenization, notifications, or blocking or sensitive information.

The platform includes out-of-the-box compliance templates cover US and international regulations including:

- Payment Card Industry (PCI)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accounting Act (HIPAA)
- Sarbanes-Oxley (SOX)

In addition, templates covering common DLP policy patterns include:

- Credit Card Numbers (CCN)
- US Social Security Numbers (SSN)
- SWIFT Codes
- ABA routing numbers
- National drug codes (NDC)
DEPLOYMENT

CipherCloud can be deployed in the enterprise or in the cloud:

• Enterprise Deployment: the CipherCloud gateway is installed on a server or virtual machine behind their corporate firewall. This is ideal for customers who want to restrict access to cloud applications only from within the corporate network or VPN.

• Private Cloud or Hosted: CipherCloud can be installed in a virtual private cloud using Amazon Web Services (AWS) or customers contract with third-parties such as Rackspace or NTT) to host and manage their CipherCloud installation.

The CipherCloud platform may run on any Red Hat or CentOS compatible physical or virtual server. After installing the software, here are some high level tasks to perform to complete deployment:

1. Determine the custom URL (custom host name) to use for gateway access, for example: salesforce.acme.com.
2. Create or import an SSL certificate.
3. Use the Management Console wizard to configure data protection policy.
4. Use the Appliance Admin Console wizard to import or create encryption keys.
5. Start protecting data stored in the cloud.

PERFORMANCE AND SCALABILITY

A single gateway can typically handle up to 5,000–7,000 users depending on the number of requests per second, amount of hardware, memory, and network resources dedicated to the machine. As needs increase, customers can simply add more CipherCloud virtual machines or scale down just as easily.

In addition, multiple CipherCloud gateways can be installed in an active-active configuration with load balancing to provide the highest levels of scalability and failover.

The CipherCloud platform is designed for high-performance encryption for large scale deployments with extremely low latency. The gateway is stateless with no local database management system (DBMS) for encryption. The gateway processes 99.96% of requests in less than 100 milliseconds, and provides static content caching for boosting cloud application performance. Multiple instances of the CipherCloud platform can work seamlessly behind a load balancer with common encryption keys and flexible plug-ins for redirection and clustering.
As organizations deploy an increasing array of cloud applications, it becomes difficult to provide centralized control or security across disparate platforms. CipherCloud solves this by securing multiple cloud applications or multiple organizations within one platform. This unique capability enables centralized control and consistent policy enforcement for all cloud applications used by an organization.

Single CipherCloud gateway platform protecting multiple cloud applications
SUMMARY

Cloud computing provides compelling advantages for businesses deploying enterprise applications. However, concerns about security, data privacy, residency, and regulatory requirements give many companies pause as they consider migrating portions or all of their IT operations to cloud-based services. CipherCloud helps to alleviate these concerns by allowing organizations to safeguard enterprise data destined for the cloud and satisfy their own data privacy, residency, security and regulatory requirements for using cloud services and applications.
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