Best Practices for Protecting

CONTENT & INFORMATION IN THE CLOUD

Four-Step Plan to Prepare for Your Deployment

CipherCloud®
Trust in the Cloud™

Table of Contents

Introduction

Your enterprise has recognized the need for cloud information protection. Perhaps your organization wants to take advantage of the cost savings and operational improvements the cloud offers, or maybe you have already adopted the cloud but need to step up protection around cloud-bound data to ensure compliance regulations. Either way, you're exploring your options.

What steps can you take to ensure the smoothest adoption and deployment of the best platform to protect your information in the cloud and meet your enterprise's needs? CipherCloud offers the following 4-step best practices plan to help you minimize your pitfalls and maximize your success.

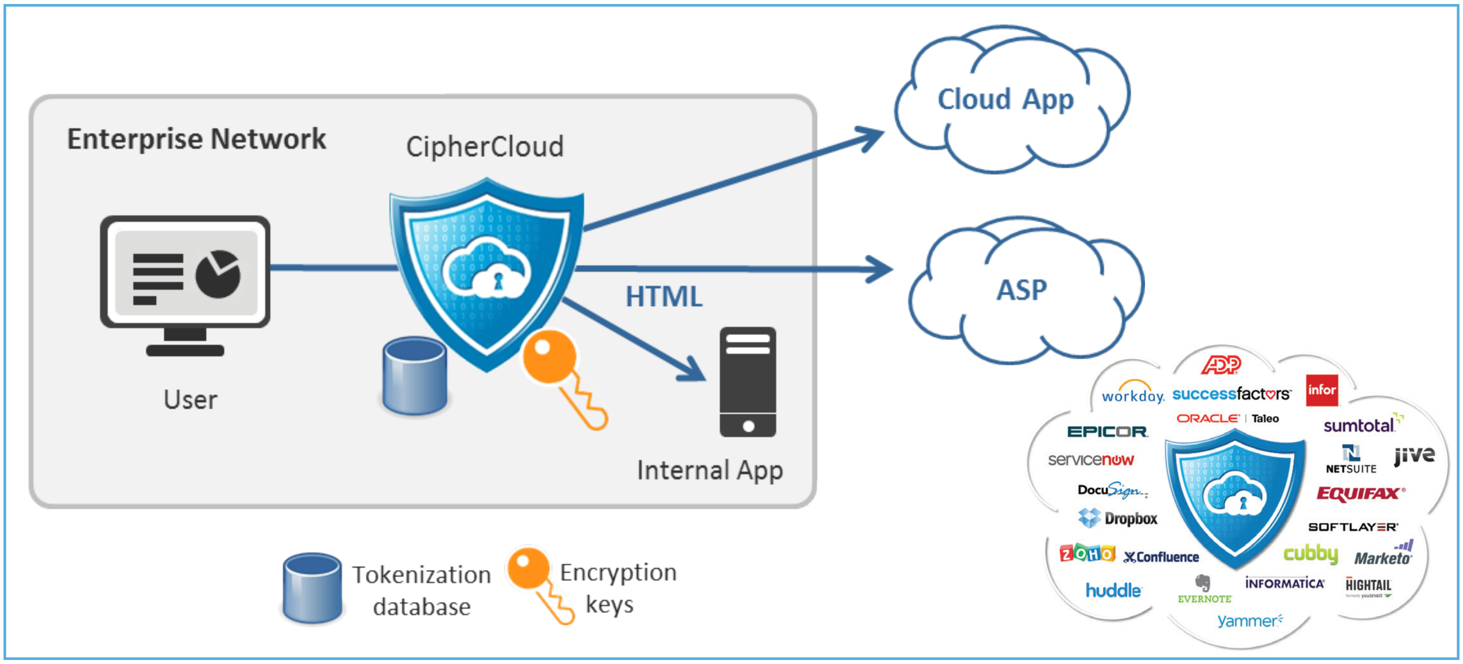
Understand what a cloud information protection gateway can do

The best security policy takes a multi-layered approach, addressing specific concerns about access, traffic, and content—all the data that you must protect. Different solutions protect different layers and, ideally, work together to secure your entire data ecosystem against intrusion, data exfiltration, and the like, and different solutions constitute different pieces of the overall regulatory compliance puzzle.

So where does cloud information protection fit in?

What is a cloud information protection platform?

As the name suggests, a cloud information protection platform specifically protects the data your enterprise sends to the cloud. Cloud information protection platforms sit between your enterprise's data center(s) and the cloud applications your enterprise uses, protecting sensitive data from the point it passes through the protection platform server in your data center: in transit, at rest, and in use in the cloud application itself. And "cloud" doesn't just refer to third-party cloud applications like Salesforce or Microsoft Office 365. Depending on configuration, a protection platform can also protect content hosted in internal, private enterprise clouds, securing it against exfiltration by disgruntled (or merely careless) employees within your own organization.



A Cloud Information Protection Platform Protects the Data You Send to the Cloud

Where does the protection platform sit?	¤ A cloud protection platform sits between your users and the cloud applications you use, typically within your data centers.	¤ Sensitive data is protected from the point it passes through the cloud information protection platform server in your data center
What types of data do you need to protect (and where might your data reside)?	¤ Data in transit ¤ Data at rest ¤ Data in use in the cloud itself ¤ Data used in third-party applications and by third parties such as partners ¤ Data used/accessed in internal cloud applications	¤ Data moving from your data center to the cloud ¤ Data in storage ¤ Data being accessed in a cloud application such as Salesforce (SFDC) ¤ Data used in many cloud applications, including Salesforce, MS Office 365, Gmail, NetSuite, AWS, and more. ¤ A cloud information protection platform can also protect content hosted in internal, private enterprise clouds.
Protection Options	¤ Encryption ¤ Tokenization	¤ Apply AES 256-bit encryption, which renders the data indecipherable to anyone who does not possess the keys. ¤ Generates random values as substitutes for the original data; also keeps critical data out of the cloud.
Benefits	¤ Key control ¤ Functionality ¤ Performance	¤ You hold the keys, no one else. This satisfies many compliance regulations and can provide “Safe Harbor” in many instances. ¤ You and your users maintain the application functionality and convenience you went to the cloud for in the first place—search, sort, reporting, and so on. ¤ Your users continue to have a positive-use experience with near-zero latency impact.

A cloud information protection platform offers three main benefits:

¤ **Key control.** Encryption is critical to both data protection and regulatory compliance, but when you allow a third party, such as a cloud applications provider, to access the encryption keys themselves, not only do you place your data at additional risk of disclosure, but you also lose your protection under the safe harbor exemptions common in many regions' data privacy regulations. A cloud information protection platform puts control of the keys directly and exclusively in the hands of the enterprise.

¤ **Functionality.** Outside of simple data storage, most cloud applications derive their value from the ability to perform search, sort, reporting, and other operations on cloud-housed data. If encryption significantly reduces or destroys that functionality, the cloud applications themselves become useless. A cloud information protection platform preserves core operations and formats of the data so that even when it is encrypted or tokenized, the cloud application works as expected.

¤ **Performance.** User experience matters. Poor user experience in enterprise applications was a key driver of cloud application adoption in its earlier stages, and poor user experience in protected cloud applications continues to drive adoption of other, unauthorized cloud applications. That is why a cloud information protection platform preserves cloud application usability and functionality.

Encryption vs. tokenization: What's right?

Even high-level security officers at many enterprises are unsure of the differences between encryption and tokenization. Encryption transforms information, using mathematical algorithms called ciphers, to make it illegible to anyone who does not possess the key. Tokenization houses actual data in a local database, randomly generates tokens associated with this data, and sends only those tokens to the cloud.

Safe Harbor:

Disclosed data is useless if it remains unreadable. In recognition of this, most data privacy laws offer "safe harbor" to enterprises whose data has been breached, but whose encryption keys remain safe.

Identify and document your security and compliance needs

Identifying your security and compliance needs

Deciding what to protect	1.Reviewing existing corporate data policies 2.Review relevant regulatory policies and guidelines 3.Update and align corporate data privacy policies with government regulations 4.Evaluation corporate data that must remain private—financial data, R&D info, patents, trade secrets, HR, and so on.
Determine level of granularity	The key consideration in most cases regarding what to encrypt is evaluating whether a data field's status contains Personally Identifying Information (PII). The various regulations provide guidance on what constitutes PII.

A cloud information protection platform gives you granular control over the protection of individual fields of data. Before you can begin to encrypt, tokenize, or otherwise protect any of those fields, however, you must have a clear understanding of what data you need to protect, and how. In most cases, enterprises do this in four main steps:

1. Review existing corporate data policies
2. Review relevant regulatory policies and guidelines
3. Update and align corporate data privacy policies with government regulations
4. Of additional interest is corporate data, such as financial data, strategic or R&D documents, trade secrets, and any HR documentation that could reveal confidential employee information.

These steps seem simple, but require a significant amount of due diligence. Regulations and compliance standards can be vague; you'll have to carefully review each field of data that you plan to put into the cloud to determine whether it requires protection, and, if it does, what kind of protection. If you deem a field sensitive, you'll need to justify why. If you deem a field safe to leave in the clear, you'll have to justify that, too. To do so, it's best to schedule a discussion around protection requirements. Involve business, compliance and risk management, legal, security, and operations staff in the discussion.

As you work through your data protection requirements, remember that not every field requires encryption or tokenization. Even a major enterprise in a highly regulated field like financial services may find that of several thousand possible data fields, it only needs to protect a few dozen to ensure anonymity and data privacy for all of its customers. The key consideration in most cases is any data field's status as Personally Identifying Information (PII). **The table on the next page lists examples of PII, per several common regulatory standards:**

Mail Merge: A common Challenge

Cloud applications can greatly ease the generation of an enterprise's email marketing and other mass communications. In order to do so, however, they require the use of customer names and addresses, which are considered PII under all data privacy regulations. You don't want to lose the functionality of the data, but neither can you permit it to be in the clear while in the cloud. Make sure you figure out how you plan to keep that data safe while still enabling mail merge functions to be performed on it.

Compliance Regulations on Identifying PII (personally identifiable information)

National Institute of Standards &Technology (NIST)

- Names
- Personal identification numbers
- Address information
- Biometric data

Health Insurance Portability and Accountability Act (HIPAA)

- Geographic information any smaller than state
- Dates, including birth and death dates and admission and discharge dates
- Telephone numbers
- Email addresses
- Identifying numbers, including SSNs and medical record numbers

Payment Card Industry Data Security Standard (PCI-DSS)

- Account numbers
- Cardholder names
- Expiration dates

Gramm-Leach-Bliley Act (GLBA)

- Names, addresses, SSNs, and email addresses
- Account numbers
- Online login ID information, including usernames, passwords, and answers to personal questions
- Customer conversations and requests

What kind of data does not require protection?

So what does not require protection? Typically, information that, if taken out of context, would not provide any personally identifying information. For example, transaction amounts tell nothing about an individual when taken out of context of a particular customer's account or personal information. Neither do transaction dates or call times and durations. Additionally, information that anyone could find through public sources, such as online research or general disclosure, typically does not require protection.

You do not need to encrypt or tokenize everything, nor should you attempt to. Instead, you must focus on only what truly requires additional protection.

Once you've identified which data fields do require protection, you must understand how that protection can impact the functionality of your enterprise's chosen cloud applications.

Your enterprise didn't arbitrarily decide to adopt cloud applications. You doubtlessly identified specific operations that, if performed within third party cloud applications, would result in measurable business benefits. Before you commit to performing encryption or tokenization on data bound for the cloud, make sure that those operations won't reduce the cloud's benefits. What functions do you need your cloud applications to perform? Search, sort, and reporting are three of the most common, and without expert integration, encryption and tokenization could reduce or eliminate that functionality. Not good. Other examples of functionality that could be impacted include workflow, validation rules, and custom server-side programming.

A cloud information protection solution can ensure the uninterrupted functionality of your data, but only if correctly deployed with a reasonable set of data protection policies. Use your solution provider's representatives and resources to understand which data protection strategies preserve data usability, and when and how to apply each strategy. This step helps determine the ultimate success of your cloud information protection integration with your cloud application providers. Your cloud information protection platform provider understands the work that needs to be done, and how to do it.

Searchable Strong Encryption (SSE): The Holy Grail of Secure Functionality

Among all the different encryption and tokenization methods CipherCloud uses, Searchable Strong Encryption (SSE) may be the greatest. Announced in October 2013, SSE enables full data functionality in the cloud, without reduction to either security or performance. It does this by using the cloud information protection gateway to perform secure local indexing and search functions while retaining the strong encryption of data sent to the cloud. Among the search functions supported are:

- Case insensitive searches
- Wild card searches
- Boolean operations

Perform infrastructure preparation and sizing

Now you're getting close to deployment. The next things to consider in conjunction with your cloud information protection provider are the nuts and bolts of your infrastructure and what is required for successful deployment.

Work with your protection provider to document the following information about your enterprise's needs:

Define Your Enterprise's Cloud Deployment Needs

¤ Number of users	¤ Number of servers
¤ Number and type of clouds in use (or planned for use)	¤ Number and location of data centers
¤ Inbound data volume	¤ Outbound data volume
¤ Traffic routing requirements	¤ Database requirements
¤ SSL requirements	¤ Security access needs
¤ Number and types of sensitive data fields and their encryption and tokenization requirements (which you have, naturally, already identified)	¤ Mobile access requirements
¤ API integrations	¤Desired rollout schedule

All of this information is necessary for your protection provider to help you determine what deployment model to use and what specific infrastructure needs your enterprises has. Your provider is an invaluable resource during this step. With their experience in deployments, they are qualified to provide detailed checklists of infrastructure prep information necessary for a successful rollout. Work closely with them through this process.

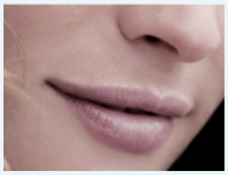
What comes next

Once you and your cloud information protection platform provider have put all the pieces together, you'll be ready for a proof of concept, testing cycles, and, ultimately, deployment of a cloud information protection platform designed to empower your organization to leverage the benefits of the cloud while avoiding its risks.

When it comes to cloud adoption and what you've done to protect your enterprise's sensitive or regulated data, you're making progress. You've recognized that cloud adoption is no longer an "if" question, but a "when" and "how" consideration, and you know that the "how" could make or break your cloud deployment. Have you begun to give the specifics of your cloud information protection solution needs much thought?

> “Reach out to CipherCloud’s cloud security and data protection experts for guidance based on years of experience in the field and with industry-leading enterprises

Real examples of how it can be done

	Customer	Industry	Key Regulations	Solution	Summary
	Top 3 US Bank	Banking, Finance	Dodd-Frank, SOX, GLBA	Salesforce	Large bank places its consumer loan origination portal in the cloud
	World’s Largest Healthcare Company	Healthcare	HIPPA, HITECH	Salesforce	Developed portal for connecting hundreds of hospitals and surgery centers via the cloud- while meeting HIPAA/HITECH regulations
	Large British organization	Education, Government	Privacy regulations in multiple regions	Salesforce	English and French open collaborative education cloud portal to many countries
	Military-Grade Nanotechnology Developer	Technology, Military	ITAR	Gmail	Semiconductor provider to Aerospace & Defense relies on encrypted Gmail
	Top 5 Canadian Bank	Finance	PIPEDA, EU Privacy Laws, US Patriot Act	Salesforce	Large Canadian bank places their CRM system managing merger & acquisition and IPO information in the cloud
	Global Customer Loyalty Leader	Financial Services	PCI, GLBA, regional privacy laws	Microsoft Office 365	Migrated 4,000-employee email program and customer info safely to the cloud
	German developer of leading skincare products	Cosmetics, skincare	German and international privacy laws, offshore regulations	Salesforce	Skincare products developer launches customer portal in the cloud
	Life sciences company	Genomic development	HIPAA, HITECH	NetSuite	Life sciences company protects patient, doctor, and genomic info in the cloud

CipherCloud, the leader in cloud information protection, enables organizations to securely adopt cloud applications by overcoming data privacy, residency, security, and regulatory compliance risks. CipherCloud delivers an open platform with comprehensive security controls, including AES 256-bit encryption, tokenization, cloud data loss prevention, cloud malware detection and activity monitoring. CipherCloud's ground breaking technology protects sensitive information in real time, before it is sent to the cloud while preserving application usability and functionality.

CipherCloud has experienced exceptional growth and success with over 2 million business users, more than 250 million customer records, in over 10 industries, and with marquee customers around the globe.

The CipherCloud product portfolio protects popular cloud applications out-of-the-box such as salesforce.com, Box, Google Gmail, Microsoft Office 365, and Amazon Web Services. Additionally, CipherCloud for Any App and CipherCloud for Databases enable organizations to extend data protection to hundreds of third-party cloud and private cloud applications and databases.

CipherCloud, named as SC Magazine's 2013 Best Product of the Year, is backed by premier venture capital firms Andreessen Horowitz, Index Ventures, and T-Venture, the venture capital arm of Deutsche Telekom. For more information, visit www.ciphercloud.com and follow us on Twitter @ciphercloud

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

Email **sales@ciphercloud.com** or call 1-855-5CIPHER (1-855-524-7437)

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