CloudLock for Salesforce FAQ

CloudLock, Inc. 203 Crescent Street, Suite 105 Waltham, MA 02453
Phone: (781) 996-4332

Table of Contents

What is the CloudLock Security Fabric?

The CloudLock Security Fabric gives organizations the visibility and control they need to protect sensitive data - payment card information (PCI), protected health information (PHI), personally identifiable information (PII), intellectual property (IP) - across a number of public cloud apps such as Google Apps, Microsoft Office 365, Salesforce, Dropbox, Box, ServiceNow, AWS and more than 91,000 connected cloud apps in one unified platform. CloudLock continuously monitors these apps in near real time (i.e. as fast as the underlying platform permits, in some cases in a matter of seconds) and detects and responds to security risk such as over-sharing, inadvertent exposure, malicious data extraction and cyberthreats. Focused on providing security insight across data, users and apps, the API-based, cloud-native architecture does not treat the cloud as a problem but as a business enabler. Contrary to traditional man-in-the-middle approaches, the SaaS-based CloudLock Security Fabric deploys in minutes, without requiring any hardware, agents or changes to the network environment. The CloudLock Security Fabric consists of eight core cloud security services:

- **Content Analysis** – continuously monitors structured(e.g. credit card information, social security numbers) and unstructured (e.g. Word documents) sensitive data in real time.
- **Context Analysis** – analyzes documents and files for sensitive information based on file ownership, sharing and access patterns.
- **User Behavior Monitoring** – monitors user activity to detect potential unusual behavior or significant changes that may suggest malicious behavior.
- **Policy Automation** – detects if sensitive data such as IP,PCI,PHI and PII is being shared inappropriately within and outside of the organization.
- **Central Auditing** – tracks user access and records an audit trail of all actions performed.
- **Incident Management** – centrally manages and investigates incidents across an organization's public cloud portfolio.
- **Encryption Management** – empowers end users to selectively encrypt sensitive information based on individual files or fully automated policy escalations.
- **Security Analytics** – delivers security insight of key cloud security indicators across an organization's cloud portfolio.

CloudLock Security Fabric ships with the following APIs:

- **CloudLock AppConnect API** – connects to cloud apps natively, i.e. deploys in a matter of minutes without requiring agents, gateways or any reconfiguration of existing networks.
- **CloudLock Enterprise API** – easily integrates with back-end systems to leverage CloudLock's real-time security intelligence for use in an organization's mission-critical systems such as Security Information and Event Management (SIEM) and ticketing solutions.

How is the CloudLock Security Fabric different from other offerings?

- The CloudLock Security Fabric is a single unified cloud platform that provides a single source of security risk intelligence for your public cloud apps. We have bundled a core set of security services into one product. This includes Google Apps, Salesforce, O365, Dropbox, Box, ServiceNow, Okta, Centrify, OneLogin, Force.com and AWS. Since the solution is cloud-native and API-based, our vision is to be the Cloud Security Fabric for the Enterprise.

- It provides near-real time continuous monitoring rather than using the concept of static, point in time scans. Near real-time means as fast as the underlying platform allows us to, i.e. in some case as fast as a matter of seconds.

- It provides full real-time incident management capabilities.

- The Fabric is available with a set of APIs that allow you to feed the security intelligence from CloudLock into your existing back-office solutions. The CloudLock Enterprise API will initially focus on incidents and policies but will expand based on customer feedback. The CloudLock Cybersecurity API allows us to integrate CloudLock directly with a set of core public cloud apps. Right now, this API is internal but our intention is to make this public over time so that it will be easy to add additional cloud platforms.

- Unlike man-in-the-middle approaches, CloudLock's API-based cloud-native solution helps organizations protect their cloud environments directly in the cloud without forcing them to funnel traffic through gateways or reverse-proxy configurations, greatly enhancing time to value and accuracy while reducing complexity.

- CloudLock not only continuously monitors cloud apps for security issues from the time of deployment but can also flag incidents retroactively, in some cases as far back as the time the original cloud app was deployed (dependent on the underlying API capabilities of our cloud partners).

- CloudLock sees sensitive data from all relevant sources, i.e. users, apps and machines.

What additional information is available for me right now?

Please check out our website (https://www.cloudlock.com) and our public Community portal.

What is CloudLock for Salesforce?

Using an API-based approach, CloudLock for Salesforce delivers high time-to-value while avoiding any negative impact on the user experience or Salesforce performance. CloudLock complements and extends Salesforce Shield functionality, enabling organizations to enforce regulatory and security compliance throughout the platform, including Salesforce Sales Cloud, Service Cloud, Communities, and Force.com, to address three fundamental needs:

- Surface sensitive information and prevent its leakage from the Salesforce environment
- Guard against cyber threats by alerting on anomalous user behavior indicative of potential risk
- Protect sensitive information within the Salesforce platform by coupling Salesforce's native encryption with automated, policy-driven quarantine capabilities

What is CloudLock for Salesforce Selective Encryption?

Selective Encryption for Salesforce leverages CloudLock's policy-driven content detection to identify exposed sensitive information and then placed into a quarantined record housing Salesforce encrypted fields to safely store the data. Selective Encryption works on all editable fields on any object, including chatter feed items, feed comments, and file attachment.

- Expand on, operationalize, and automate native Salesforce encryption capabilities
- Automate the detection and quarantining of sensitive information through customizable policies regardless of where information lives within Salesforce
- Protect sensitive data with encryption without impacting native functionality or workflows, such as search or reporting

What type of encryption is used?

CloudLock for Salesforce automates the detection and quarantine of sensitive information based on policies regardless of where it resides in Salesforce utilizing the platform's native encryption capability. Salesforce Shield uses AES 256-bit encryption.

Does Salesforce Selective Encryption work for files and attachments?

Yes. However, files and attachments are quarantined and placed in a secure area within Salesforce for authorised Administrators to access with required permission sets assigned.

Does Salesforce Selective Encryption work for Chatter and Communities?

Yes. This is a primary use case among all CloudLock customers.

Who can see encrypted quarantined records within Salesforce?

There are 2 levels of access: A special permission set should be configured for an administrator to view quarantine records. A second permission set is required to view encrypted original content that violates a CloudLock security policy.

How long does it take for Salesforce Selective Encryption to work?

In near-real time. In other words, as soon as the incident is detected by CloudLock via a Salesforce API.

Is the quarantine message customisable?

Plans to provide customisable messages for the CloudLock quarantine action will be available in a future release.

Do I need to purchase additional services from Salesforce for Selective Encryption to work?

No. This is available out-the-box when CloudLock Selective Encryption is purchased.

Can I create triggers, workflows, reports & dashboards in Salesforce from quarantined data?

Yes. It is a custom object in Salesforce and is extensible like any other object (with appropriate permissions).

Can CloudLock detect 3rd party Apps and Cloud Malware?

Yes. With CloudLock for Salesforce, you can detect, classify, and control third-party applications connected to the Salesforce environment via the AppExchange and Force.com (4,000 apps) based on potentially risky access scopes and excessive permission sets. To efficiently assess apps, use the CloudLock Community Trust Rating, CloudLock's real-time, crowdsourced cloud application security analysis.

Does CloudLock provide a centralised Administration Console?

Yes. CloudLock is a SaaS solution and uniquely allows for a single unified dashboard via a web portal to present all security incidents, reports and logs and potential risks across multiple SaaS applications and cloud platforms (e.g. Google Apps, O365, Salesforce, ServiceNow, Dropbox and Box, Amazon, Azure and Okta). The web portal also enables CloudLock Administrators to manage and configure policies, take action on any incidents that occur that breach policy.

What is CloudLock In App Security?

CloudLock provides "In App" security by extending its capabilities into Salesforce with CloudLock Mosaic. Salesforce Administrators can incorporate security into existing workflows, operating CloudLock as a managed package within the platform. Users may elect to manage Salesforce-specific incidents within Mosaic or manage security incidents from across the cloud ecosystem, including SaaS, IaaS, PaaS, and IDaaS platforms. This enables you to report and analyse security incidents related to your entire cloud environment (e.g. MS O365, Salesforce, Dropbox, ServiceNow, AWS and Okta) directly from the Salesforce dashboard. Leveraging out-of-the-box and custom workflows as well as custom salesforce objects for key security capabilities, Salesforce administrators can create their own security reports and dashboards directly in Salesforce, eliminating the need to manage multiple solutions.

What measures are in place to ensure CloudLock is transparent to end-users ?

CloudLock's unique cloud-native API-only approach allows for seamless on-boarding across all cloud platforms which can be completed in minutes and does not require any changes to the underlying infrastructure or network configuration. CloudLock has been designed from the ground up to specifically leverage the API-only approach, and works closely with the cloud platform vendors (e.g. MS O365, Google Drive and Apps, Salesforce, ServiceNow, Box , Dropbox, AWS, Okta) to allow for the best user experience, without breaking business workflows unlike the Man-in-the-Middle methodology of gateways, proxies or agents. There is zero impact to the user experience or performance of the cloud application.
Without interfering or impacting with the end-user, CloudLock ensures no latency or single point of failure and most importantly, has no impact to the underlying functionality of the Cloud application. CloudLock ensures that end users continue to use and connect to their desired cloud application as normal.

Administrators are able to configure policy to notify end users if required when CloudLock security policy has been violated.

Does CloudLock support Salesforce Shield?

Yes. CloudLock complements and extends Shield functionality. CloudLock's Selective Encryption app for Salesforce leverages Shield's native AES-256-bit encryption.

- **Data Governance:** CloudLock's customisable policy engine can ensure data compliance by leveraging Salesforce Shield to selectively encrypt sensitive data or files. When sensitive data is identified, the field (or entire file) is immediately encrypted using Salesforce Platform encryption. Additionally, files can be quarantined with standard field level encryption.

- **CloudLock's Free Event Monitoring Viewer** - Provides CSV data insights into 3 core areas: Historical trending, Adoption trends, Performance trending as well as a unified dashboard for visualising incidents with assigned priorities and classifications. Automated remediation with defined and configurable policies based on IP, Frequency, Role, Threshold while identifying where and how data is being exported globally.

- **Field Audit Trails:** Provides you with a historical trail of field history: Audit and Compliance so you can focus on the data changes that matter to you and set policies to discover sensitive data and view audit trail on how it got into system to comply with internal or external audits.

What is the CloudLock Event Monitoring Viewer?

The CloudLock Event Monitoring Viewer is a free visualisation tool that provides out-of-the-box visibility into Salesforce event log files with in easy-to-use interface. Leveraging Salesforce's Event Monitoring capabilities, specifically the Event Log Files API, the Event Monitoring Viewer displays and organizes all log files by date and event type and enables drill-down into each file. In addition, the application maps locations for all events tied to IP addresses, offering quick insight into where events are occurring.

CloudLock, Inc. 203 Crescent Street, Suite 105 Waltham, MA 02453

www.cloudlock.com support@cloudlock.com (781) 996-4332