

## Overview

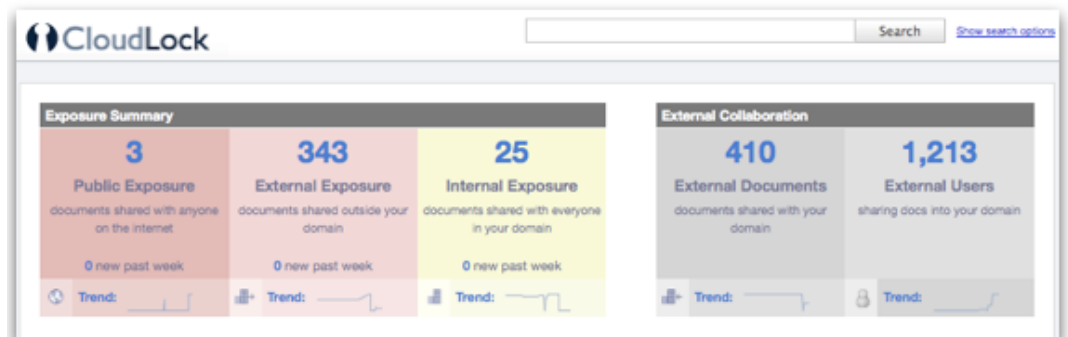
This document details the security mechanisms and processes that CloudLock has implemented in order to ensure and enforce the safety, protection, and privacy of our customer data. The security measures CloudLock has implemented span across the technology, operations, and legal aspects of protecting customer data.

CloudLock is a SaaS application running on the Google App Engine platform. At CloudLock, we understand that when an enterprise organization is reviewing the security of a SaaS application, they need to establish the risk profile to determine whether the application increases or decreases the organizational risk. As is the case with any other SaaS application, there are two components that make up the risk profile:

- The operational security controls of the SaaS vendor operations team – this requires a mature operation and a heavy investment in processes, policies, documentation and technology
- The Security controls of the SaaS product itself

### Contents

- CloudLock Operational Security
- Internal Controls, Processes & Tools
- Legal Terms & Privacy
- CloudLock is Hosted on Google App Engine
- CloudLock Product Security
- Technology
- Metadata Collection
- Installation and Granting API Access
- Secured Application Access
- Application-Level Auditing
- Customer Controls



## CloudLock Operational Security

These security controls are put in place and are audited by Google's largest customers in the commercial and federal spaces.

### Internal Controls, Processes and Tools

CloudLock operations are maintained at the highest standard to ensure the security of our customers' data. Some of the steps taken to achieve this include:

- All administrator activity is logged and audited
- Least privileged access and separation of duties - Only designated, named operational staff members are authorized to access production systems
- Security scans and penetration testing are performed on a scheduled basis
- Change and configuration management
- Access Controls & Maintenance
- SSP – Our system security plan that documents the hundreds of controls in place at CloudLock
- All employees have signed a legal document, separate from their employment agreement, that explicitly addresses the need for security, privacy and compliance and forbids them from accessing customer data without written customer consent
- Single sign-on to production systems using CloudLock Google Apps accounts
- 2-Factor authentication to prevent access by external people should an account get compromised
- Operational accounts are changed twice a month
- Security scans and penetration testing are performed on a scheduled basis

### Legal Terms and Privacy

Protecting customer data goes beyond technology and processes. CloudLock offers the following assurances:

- [SLA](#)
- [Privacy Policy](#)
- [Terms of Service](#)

### CloudLock is Hosted on Google App Engine

CloudLock is hosted on Google App Engine, Google's web application hosting environment which is SAS 70 Type II, SSAE 16 Type II, and ISAE 3402 certified. Some of the benefits of running on Google App Engine:

- An application hosted on Google App Engine runs on the same infrastructure that powers other Google applications such as gmail and Google Apps
- The same security, privacy and data protection policies you enjoy with Google Apps applies to all App Engine applications
- By running on App Engine, your data never leaves the Google infrastructure

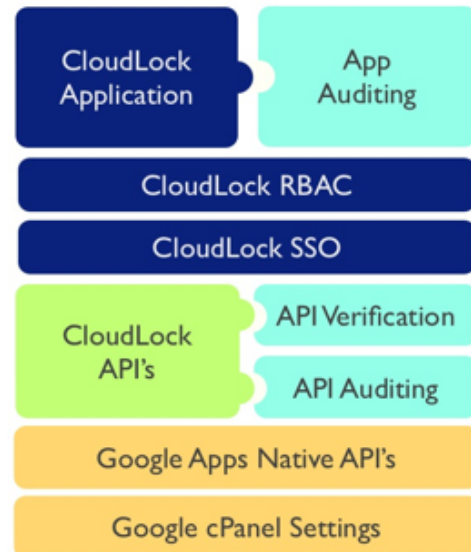


## CloudLock Operational Security

### Technology

CloudLock was built from the ground up with security in mind. A combination of architectural components have been implemented at the framework level to ensure the highest possible standard of security and privacy for our customers' data with:

- Single Sign-on (SSO) for authenticated access to the application
- Secure access to the application using https
- Role based access controls (RBAC)
- Application level auditing of all user actions in an immutable audit utility
- Leverages Google App Engine's secure run-time environment



### Metadata Collection

CloudLock collects metadata only from a customer's Google Apps domain using secure and authenticated Google Apps APIs. CloudLock works without opening or reading the content of any documents or sites.

### Installing and Granting API Access

As a Google Apps Marketplace application, adding CloudLock to a Google Apps domain is simple and secure. The installation process consists of two key steps:

1. Whitelisting CloudLock as an application that can authenticate and access your domain with a secure authentication key
2. Authorize CloudLock to access the following APIs:
  - docsFeed – Access to domain documents
  - provReadOnlyFeed – Access to domain users
  - provReadOnlyGroupsFeed – Access to domain groups
  - sitesDataFeed – Access to domain sites

Administrators can remove or disable the application at any time from their domain administrator interface. CloudLock's data management and privacy practices have been audited and certified by industry leader TRUSTe and VeriSign to ensure the compliance with the highest industry standards.



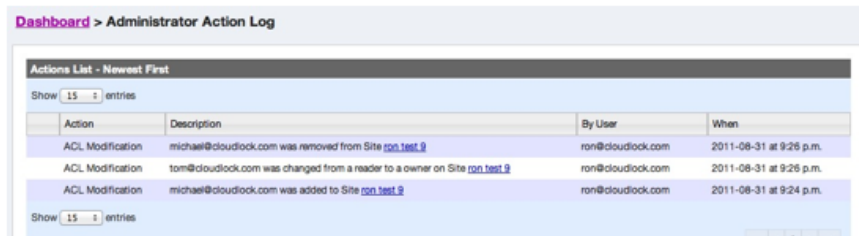
## Secured Application Access

CloudLock supports single sign-on using Open ID, which allows for simplified, central access management to the CloudLock service. CloudLock uses industry standards to authenticate and authorize end user access to the application including:

- Integrated Single Sign On for secure authentication with customer's Google Apps domain using Google Open-ID
- Encrypted access to the CloudLock application is through https (AES 256 encryption)
- Only domain admins are authorized to access CloudLock
- Role-based access controls for additional users. A domain admin can add additional users to CloudLock and assign specific roles.

## Application-Level Auditing

Modifications made to a Google Apps domain using the CloudLock application are fully audited in an immutable audit log.



Dashboard > Administrator Action Log

Actions List - Newest First

Show 15 entries

| Action           | Description                                                                               | By User           | When                    |
|------------------|-------------------------------------------------------------------------------------------|-------------------|-------------------------|
| ACL Modification | michael@cloudlock.com was removed from Site <a href="#">ron.test.9</a>                    | ron@cloudlock.com | 2011-08-31 at 9:26 p.m. |
| ACL Modification | tom@cloudlock.com was changed from a reader to a owner on Site <a href="#">ron.test.9</a> | ron@cloudlock.com | 2011-08-31 at 9:26 p.m. |
| ACL Modification | michael@cloudlock.com was added to Site <a href="#">ron.test.9</a>                        | ron@cloudlock.com | 2011-08-31 at 9:24 p.m. |

Show 15 entries

## Customer Controls

Customers have full control to revoke the permissions granted to CloudLock for API access through the Google Apps administration panel (C-Panel). For large enterprise organizations, CloudLock is able to provide a private deployment on a dedicated instance that does not go through the Google Apps Marketplace.

If you have any questions or comments please share them with us:

[security@cloudlock.com](mailto:security@cloudlock.com)

### Contact us:

For further information about the company and CloudLock for Google Apps, call (781) 996-4332 or visit [www.cloudlock.com](http://www.cloudlock.com)