

Protecting Your Data In Google Docs

Compliance In The Cloud

By Ron Zalkind, CTO CloudLock Inc.

Introduction

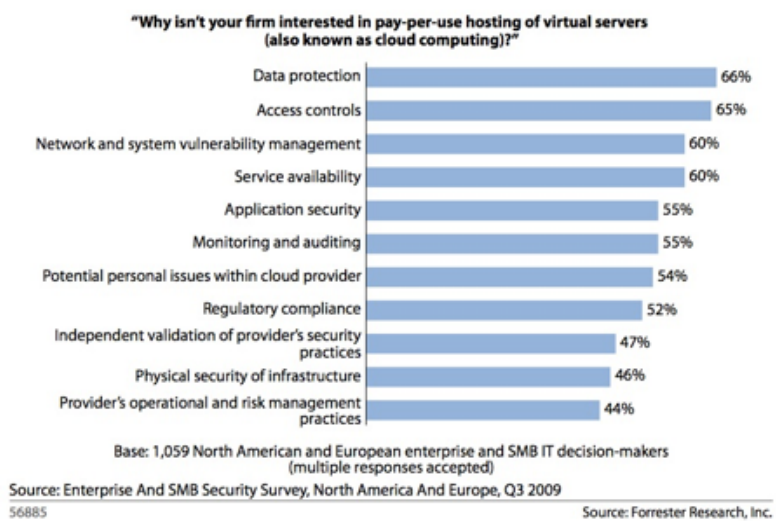
The rate at which businesses adopt cloud services is impressive. Google Apps, Google's cloud email, calendar & collaboration solution for businesses, powers over 3 million businesses and is expanding at a rate of 3000 new businesses a month.

Yet many companies are still hesitant to move to the cloud, and those that do may not fully utilize cloud services to their full extent. When asked, companies have repeatedly stated that their number one obstacle to fully leverage cloud solutions is the **security** of their data.

Contents

- [Google Apps Security & Privacy](#)
- [Handing Over Control](#)
- [Steps to Control and Protect Your Data in Google Docs](#)
- [Configuring the Google Docs Service](#)
- [Extending Administrator Capabilities Using APIs](#)
- [Inventory Your Documents](#)
- [Usage Monitoring and Analytics](#)
- [Understanding Document Sharing Options](#)
- [Managing Access Rights to Sensitive Documents](#)
- [Compliance And Regulation](#)
- [e-Discovery for Google Docs](#)
- [Retaining Document Ownership](#)
- [Conclusion](#)
- [About CloudLock](#)
- [About CloudLock for Google Apps](#)

Figure 3 Data Security, System Integrity, And Availability Are Top Security Concerns With Cloud



Using Google Apps, a Software-as-a-Service solution, means that your data (documents) will be created and used in the cloud. Therefore you must trust Google with the security and privacy of your data, and as with any cloud solution, this means giving up control. If you are a business owner, CEO or any IT executive faced with protecting your company's data for regulatory, privacy, and operational reasons this loss of control is a concern.

This paper will highlight key security aspects of your data in Google Apps, the consequences of experiencing loss of control, and steps you can take to adapt your data governance practices to protect your data in the cloud and increase the ROI in Google Apps as you enable a safer and more protected means of collaboration.

Introduction to Google Apps Security and Privacy

Google is committed to the security and privacy of your data. Their terms of service, privacy statement and security white paper guarantee that your data is yours, that the infrastructure powering the service is secure and that it has been verified through certification and accreditation. Beyond the standard service provider statements, you should still understand the fundamental aspects of security using Google Apps so that you can be prepared to overcome the intrinsic loss of the control points you have grown accustomed to.

Google built Google Apps on top of their existing cloud computing infrastructure and data centers that power core services such as Google search and Gmail. Google has published a detailed security white paper describing the security measures employed for Google Apps.

These security measures should seem very familiar. They cover the security practices employed by many managed service providers or newer infrastructure-as-a-service solutions like Amazon Web Services with measures at the physical, network and organizational layers. However, unlike other service providers, Google has a unique infrastructure: one that is shared across all its services including their search solutions. Facing these unique service offerings, companies must ask the following questions:

Where is my data?

Your data created with or uploaded to Google Apps will be stored in Google's data centers that are distributed globally. Google's cloud infrastructure takes care of replicating and distributing your data so that there is no single point of failure.

Who can 'see' my data?

Your data will not be stored in clear text and will not be human-readable. Access to the data is limited to authorized Google personnel only and monitored regularly. Your company's employees will be able to access their data by signing in to the service with dedicated Google Apps accounts or through your single sign on system (requires integration).

Will Google search through my data?

User content is only scanned or indexed in the following cases:

- Some user data, such as email messages and documents, are scanned and indexed so users within a customer's domain can search for information in their own Google Apps accounts.
- Email is scanned so Google can perform spam filtering and virus detection.
- Email is scanned so Google can display contextually relevant advertising in some circumstances (like free edition users).
- Except when users choose to publish information publicly, Google Apps data is not part of the general google.com index.

Scanning and indexing procedures are automated and involve no human interaction. It is safe to say that Google doesn't search through your data in Google Docs as part of their automatic scanning and indexing operations.

When I delete data is it really gone?

When a user of Google Apps deletes data and confirms deletion (e.g. by emptying the trash) this data is deleted from Google's infrastructure and cannot be referenced. The data will then be overwritten with other customer data.

What happens to my data if I stop using Google Apps?

Google has published in its [Terms of Service](#) that your data is yours, and should you stop using the service, your data will be deleted immediately. Deleted doesn't mean no one can recover it, it just means it is de-referenced and will be overwritten by other data over time.

Will Google share my data with 3rd parties such as the government?

Google adheres to strong privacy policies. Google will not *willingly* share it with anyone. A potential case where Google will grant access to your data might be under court order such as the USA PATRIOT Act.

The challenges around privacy and terms of service are not new and are the same when evaluating a more traditional outsourced IT service to a managed service provider.

You need to be aware of the legal and compliance aspects of working with any specific service provider and decide if it suits your company's requirements and constraints.



Trust Google Apps

Built with [safety](#), [security](#), and [privacy](#) in mind.

Is Google Apps a multi-tenant service and is my data safe from other customers?

Google Apps is a multi-tenant service as are most other Google services. It means that as a customer, your apps and data use a shared infrastructure. Google has gone to great lengths to embed security into all aspects of their multi-tenant architecture ensuring that only you can access your data. This is achieved through service authentication and authorization at all layers of Google's infrastructure. For more details please refer to Google's [security white paper](#).

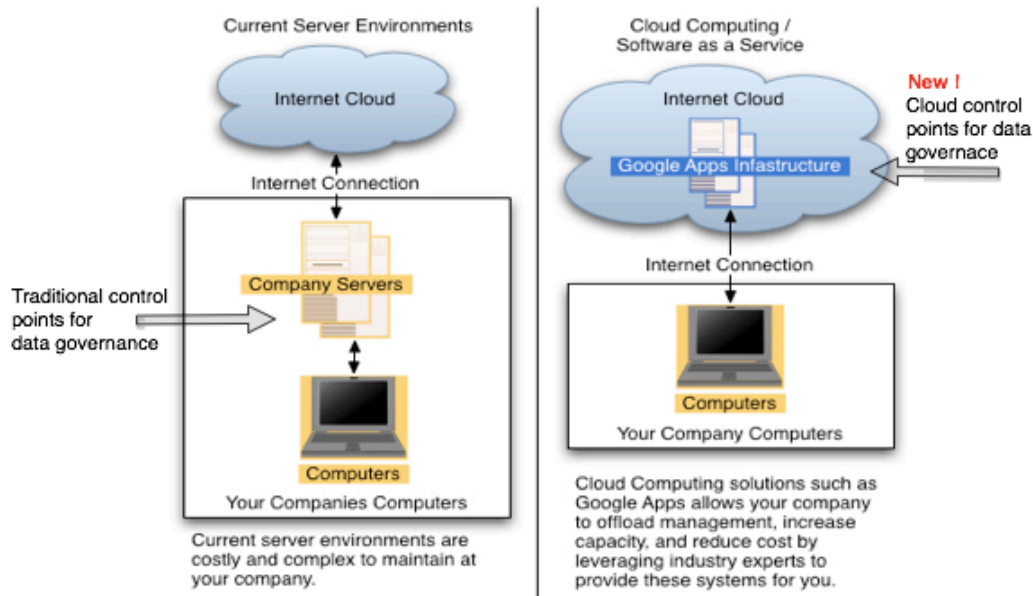
As with any service provider you should assess the security solutions offered by Google, consider their marquee reference accounts, and establish your own position about trusting Google.

Handing Over Control

As a Software-as-a-Service (SaaS) solution, Google Apps offers all the benefits of outsourced IT operations and infrastructure. Companies that adopt Google Apps realize that their competitive advantage is in providing great service to their customers and not in managing on premise systems. However, using SaaS means that IT concedes some control to the SaaS vendor.

What IT could control on-premise, behind physical walls and a traditional hardware, network, host, and operating system stack isn't available with SaaS solutions. Your firewall, NAC, antivirus, backup and other systems can't operate on such services. To some extent, Google does take away some of the need for traditional control points as they take care of service up time, backup and disaster recovery. However, there are other aspects of the service that are still under your responsibility, especially as it pertains to data and **data governance**.

Organizations using Google Apps have the same responsibility to be compliant, safeguard privacy, and ensure the security of data as they do on-premise. Preventing data breaches, managing access to sensitive information, auditing privileged users, and establishing data governance practices are more relevant than ever, as SaaS solutions extend beyond your physical walls and expose a new threat surface to your data. The question now becomes: How can you establish these control points when the traditional solutions no longer apply?



(diagram from Google: <http://www.google.com/apps/intl/en/business/faq.html>)

Google Apps, while offering tremendous cost savings and productivity gains, doesn't offer enterprise-class controls to companies who have been running messaging, collaborating and storing documents on premise. You are asked to trust Google with your data. But trust is hard to achieve when you lack visibility and control. Protecting your data extends beyond Google as a service provider and into the use of the service by your users, protecting the data from miss use and abuse is a top priority for many organization.

In the next section we will focus on Google Docs, the collaboration and documents service in Google Apps, and cover specific steps to be taken to regain control and complement Google Docs with enterprise-class controls for data protection that will allow you to trust the security of the solution.

Steps to Control and Protect Your Data in Google Docs

Google Docs is one of the services comprising the Google Apps platform. It offers online documents with real time collaboration. Companies who use Google docs enjoy the benefits of:

- Online documents that can be accessed from anywhere
- Real time collaboration so users can work on a document at the same time
- Upload any file and access it from anywhere
- No need to worry about backups

To manage and control Google Docs, Google offers basic administrator capabilities out of the box. These primarily include:

- Service configuration
- User and password management
- Rudimentary usage reporting

First we'll talk about how to configure the service within Google Docs, including document sharing, visibility, and using service organizations. We'll then go on to see how using Google Apps' in conjunction with [third party apps](#) can extend the built-in admin capabilities to provide enterprise-class data protection in Google Docs.

Configuring the Google Docs Service

While there are few setup and control options when configuring the Google Docs service for your company, you should understand what the different options are and choose carefully.

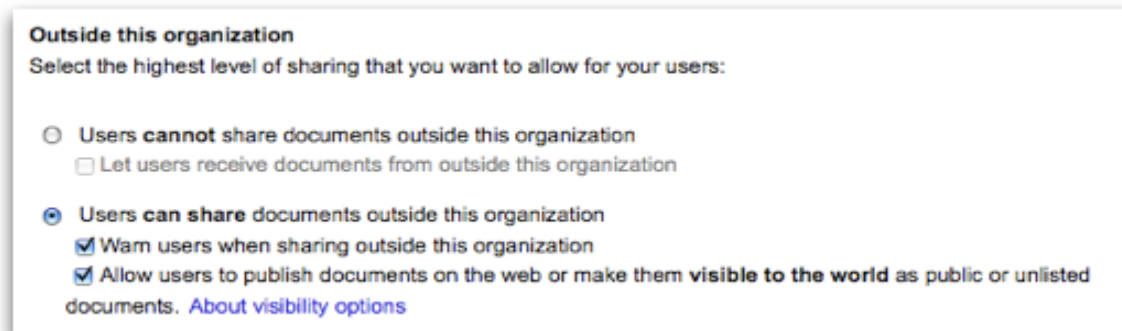
Service Settings

Turning the service on/off

Your main control point is to turn the service on/off. This setting has no granularity, but if you do not want your users to have access to Google Docs, you can turn the service off.

Sharing outside your domain

This option controls whether your end-users will be able to share documents with people outside of your company's domain. Sharing with outside people is highly effective; you will be able to collaborate with contractors and service providers with ease and speed.



Google allows you to control outbound and inbound sharing separately, meaning you can choose to share outside of your company but prevent outsiders from sharing documents with your company. Companies who turn off outside sharing usually do so due to fear of sensitive information leaking out. Though this is a valid concern, we'll later cover [third-party applications](#) that discover and review or approve documents that are shared outside of the company.

Sharing With The Public

Since Google Docs is a SaaS solution, Google makes it possible to make a document available for public access. This means anyone can access the document over the Internet (we will discuss some configuration options further below).

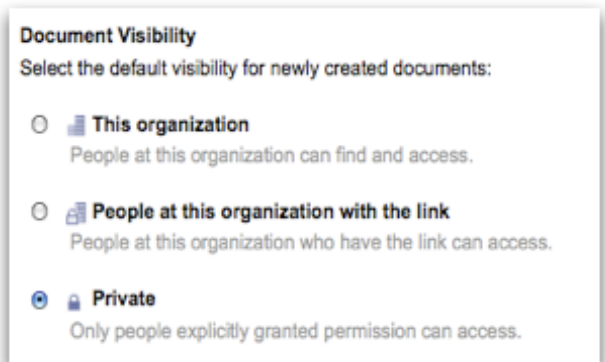
Security-conscious IT pros may cringe at the thought, but there are good use cases for this option. For example: Let's say you teach a class at university.edu and want to share class notes with students from your university and with other universities. These notes can be published to the public, and by doing so, anyone can access them without the need for you to manually share with your students (and it would be practically impossible to otherwise share with other universities).

The down side of enabling this option is that some users are trigger-happy and share a document with the public when they shouldn't. To enjoy the benefit of public sharing while avoiding unwanted exposure you'll need to regularly verify which documents have been shared with the public.

Document Visibility Options

This configuration option controls the scope of users who will be able to access the document when it is created. The options are to either make the document private or to make it accessible to everyone in the company.

Best practices suggest that you should always select private as the default. (see image). If users need to share with a broader audience they should make that choice consciously.



Configure Google Docs Service Using Organizations

You can create an organizational structure to control which Google Apps services are available to users. By default, all organizations 'inherit' the domain level (top level) setting and you can override the domain settings for each organization.



Using the university.edu example from above, the university might turn on Google Docs for students, yet turn it off for the staff.

Extending Administrator Capabilities Using APIs

Instead of building enterprise-class data management capabilities into Google Apps, Google chose to publish a robust set of APIs that allows developers to extend functionality, generate reports and integrate to other systems. Customers have been developing an in house solution and vendors have leveraged the [Google Apps marketplace](#) to offer management products that can be installed into your Google Apps domain.

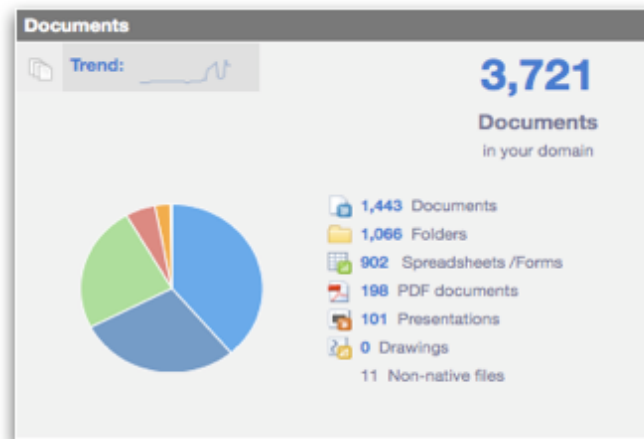
In the following section, you'll see how using a third-party data protection application from the Google Apps Marketplace ([CloudLock](#)) extends the security capabilities in Google Apps. The steps described below will require either custom development or the use of third-party applications as the default Google Apps administrator capabilities do not support these guidelines.

Inventory Your Documents

You can't manage what you can't see. To put it simply: in order to control the Google Docs service, you must be able to see the documents. You will want to know:

- Which documents are being created by your users
- When they were created
- Who the document owners are
- With whom documents are shared (collaborators)

As an admin, without using Google's APIs or a third-party application, you are not able to view any of the documents your users have created and the entire service appears as a 'black box' to the domain administrator. However, using an application like [CloudLock](#), you'll be able to secure your company's sensitive information, manage adoption and provide end user support. For example:



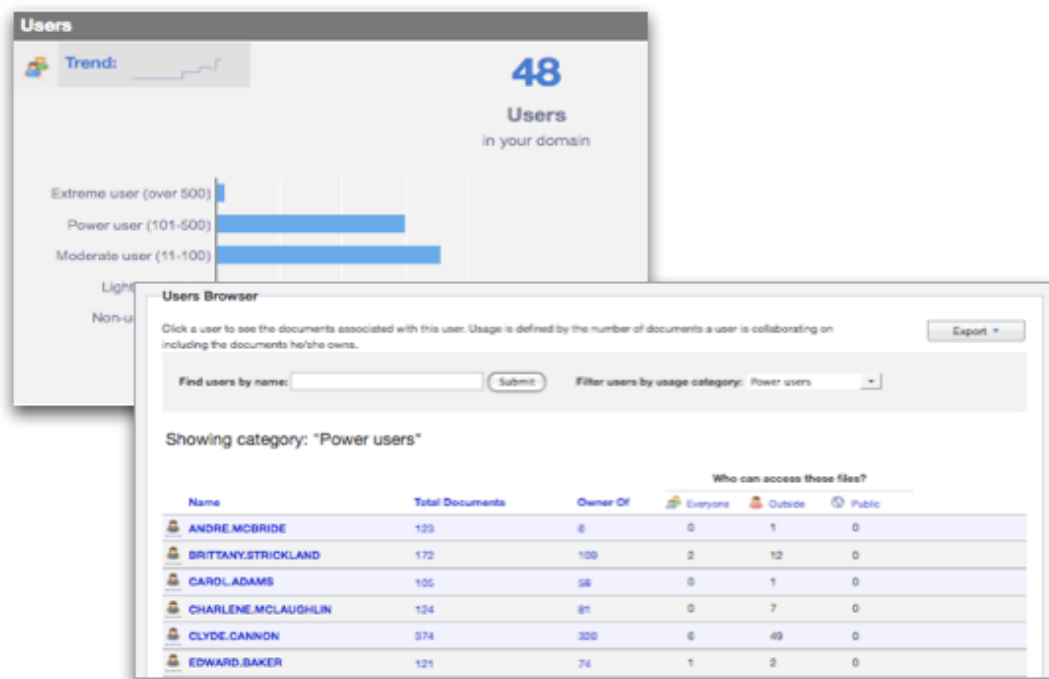
Document inventory reporting in CloudLock

Usage Monitoring and Analytics

Once Google Docs is deployed in your domain, it is important to manage adoption and have control over how users are using the service. Google provides basic controls to the administrator, but does not offer any visibility into documents and the users who create them. In any company-wide rollout, IT needs to:

Monitor users' usage of docs - Identify who your power users are, who collaborates with whom, how often documents are created and whether the service is being adopted and used as intended. Implementing basic ongoing usage monitoring and understanding what users are creating, will allow you to take measures to improve user adoption.

Identify early adopters - As with any new solution, you need to manage change. Finding your early adopters will help in both receiving early and frequent feedback about the solution, and in understanding and defining usage policies especially as they relate to security and privacy. Early adopters will help you understand how to best use Google Docs in your company and how to adjust your usage policies accordingly.



User inventory reporting in CloudLock

Understanding Document Sharing Options

One of the biggest advantages of using Google Docs is the ease of collaboration. However this benefit introduces security risks, as documents are no longer protected by your 'four walls'. Stored in the cloud, your documents can very easily be shared with external sources (intentional or malicious) that no longer require physical access to your network on premise in order to access a document.

It is important to understand the various sharing options so you can establish and review document-sharing policies and to educate your end users. Users can share a document in several ways:

Share inside the company – You can share a document with one or more people from the domain. An email notification will be sent to the collaborators and a new document will appear in their document inbox. You can also share a document with an email list (group) or everyone in the company.

Share outside the company - If you have configured the Google Docs service to allow sharing with people outside your domain, users will be able to share with anyone external to the company. Note that without a [third party application](#), admins cannot report on documents that are shared outside of the company.

Share with the public - Users can make a document available to the public. In this case anyone on the Internet can search for the document and access it. This option can be useful for documents that should be accessible by anyone external to your company, for example, a general survey form.

Viewer vs. Editor - When sharing a document explicitly with another person, by default they are designated as editors of the document. Editors can view, modify and change the permissions of a document. In contrast, viewers can only view the document.

'Second Hand' sharing, the latent security risk - The editor role in Google Docs is a powerful one as it allows the editor to share the document further with additional people, including people outside of the company. They can also make the document public without the consent of the document owner.

Documents that are owned by external users – Documents can be created by external users and shared with your organization. These documents can be created by contractors, vendors, or even employees using their Gmail accounts and are then shared with users in your organization. Legally these documents are the property of the company.

Consider this scenario: Sarah from Marketing is sharing the timeline of a new product launch with Sam from the external PR agency. As an editor, Sam can now share the document further with external sources that have not been approved, and the timeline of the new product launch (and perhaps even the existence of a new product), which is confidential information, is now compromised. Sarah and her company haven't consented to share this information beyond the PR agency, but have no control or visibility that such a violation occurred.

Managing Access Rights to Sensitive Documents

Companies have always faced the challenge of managing access to data. The need to ensure that only the right people have access to sensitive information and to audit privileged users (administrators) hasn't changed when moving to cloud services such as Google Apps.

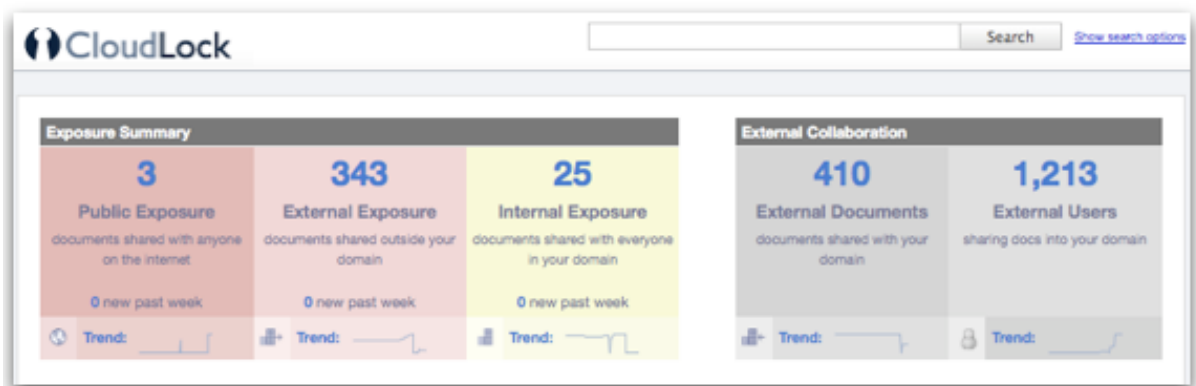
Traditionally, in order to report and audit access rights, you would need to deploy agent software on all your file servers that would scan and monitor file system activity and correlate user and group information from Active Directory to report on effective access rights.

The access rights structure and the fact that users and documents are managed in the same system (as opposed to a file system and active directory which are separate systems) makes access management reporting, monitoring and auditing simpler in Google Apps. However, it does require the use of APIs or [third party software](#).

When building or evaluating an access management solution for Google Docs you should be able to:

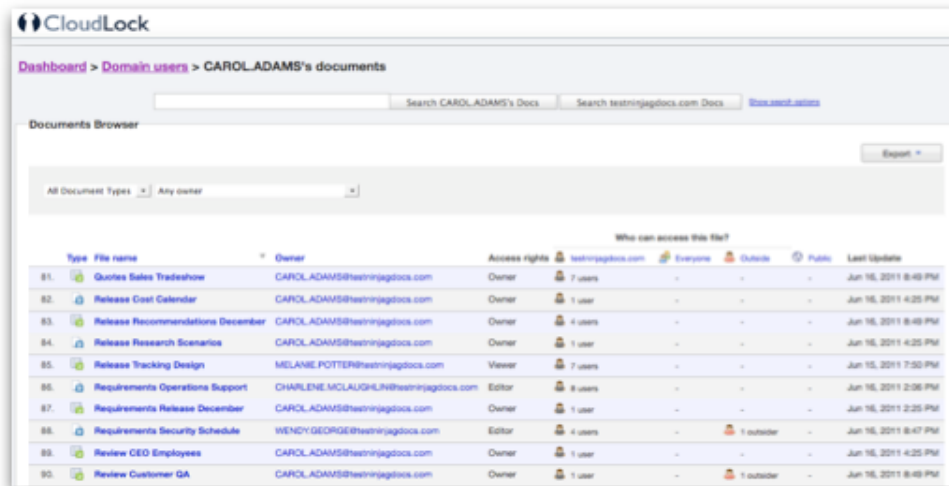
Identify exposed documents - Identify all the documents that are shared with the public, with external people and with the entire company. Take a look and see if there are documents that are owned by external users.

Once identified, verify with end users that these documents are shared correctly.



The document exposure summary in CloudLock for Google Apps

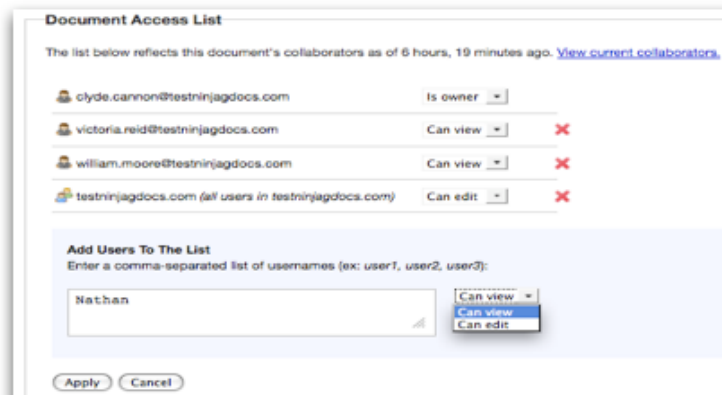
Report on User Access Rights – Report on which documents a specific user can access and if they are a viewer or editor. This is especially handy when employees change roles, or for a contractor who no longer works with the company. Once you review access rights for a given user, you should be able to remove unwanted access rights.



Type	File name	Owner	Access rights	Who can access this file?	Last Update
81.	Quotes Sales Tradeshow	CAROL.ADAMS@testninjaagdocs.com	Owner	7 users	Jun 16, 2011 8:49 PM
82.	Release Cost Calendar	CAROL.ADAMS@testninjaagdocs.com	Owner	1 user	Jun 16, 2011 4:25 PM
83.	Release Recommendations December	CAROL.ADAMS@testninjaagdocs.com	Owner	4 users	Jun 16, 2011 8:49 PM
84.	Release Research Scenarios	CAROL.ADAMS@testninjaagdocs.com	Owner	1 user	Jun 16, 2011 4:25 PM
85.	Release Tracking Design	MELANIE.POTTER@testninjaagdocs.com	Viewer	7 users	Jun 15, 2011 7:50 PM
86.	Requirements Operations Support	CHARLENE.MCLAUGHLIN@testninjaagdocs.com	Editor	8 users	Jun 16, 2011 2:06 PM
87.	Requirements Release December	CAROL.ADAMS@testninjaagdocs.com	Owner	1 user	Jun 16, 2011 2:25 PM
88.	Requirements Security Schedule	WENDY.GEORGE@testninjaagdocs.com	Editor	4 users, 1 outsider	Jun 16, 2011 8:47 PM
89.	Review CEO Employees	CAROL.ADAMS@testninjaagdocs.com	Owner	1 user	Jun 16, 2011 4:25 PM
90.	Review Customer GA	CAROL.ADAMS@testninjaagdocs.com	Owner	1 user, 1 outsider	Jun 16, 2011 8:49 PM

User access reporting in CloudLock for Google Apps

Document Access Rights - See which people can access any given document. This is especially relevant when a sensitive document is compromised, corrupted or for some other reason at risk.



Document Access List

The list below reflects this document's collaborators as of 6 hours, 19 minutes ago. [View current collaborators.](#)

clyde.cannon@testninjaagdocs.com	Is owner	
victoria.reid@testninjaagdocs.com	Can view	✖
william.moore@testninjaagdocs.com	Can view	✖
testninjaagdocs.com (all users in testninjaagdocs.com)	Can edit	✖

Add Users To The List
Enter a comma-separated list of usernames (ex: user1, user2, user3):

Can view
Can view
Can edit

Document access rights management lets you see and fix access rights

Identify sensitive documents – Identify documents with sensitive content and review their access rights. Enable auditors to inspect all documents for compliance while logging access to these documents in the audit trail.

Fix access rights - Change access rights as needed. You'll need to remove unwanted collaborators and grant access to the right people when access rights are determined to be incorrect.

Audit - You should keep record of the changes in your environment as they pertain to your document inventory, document sharing, document exposure and the actions privileged users (administrators) have performed.

Permissions Change History

Originally Published: Jun 15, 2011 7:45 PM (1 month ago) Last Updated: Jul 15, 2011 8:01 PM (3 days, 1 hour ago) Last Viewed: July 15, 2011 at 8:01 p.m. (3 days, 1 hour ago)

Date	Can View (new)	Can Edit (new)	Title	Owner
Jul 18, 2011 9:09 PM	True	False	2009 description tracking	admin@testinjadocs.com
Jul 8, 2011 2:35 PM	True	False	the internet	admin@testinjadocs.com
Jul 8, 2011 2:21 PM	False	False	2009 description tracking	admin@testinjadocs.com
earlier	False	False	2009 description tracking	RON.ZIMMERMAN@testinjadocs.com

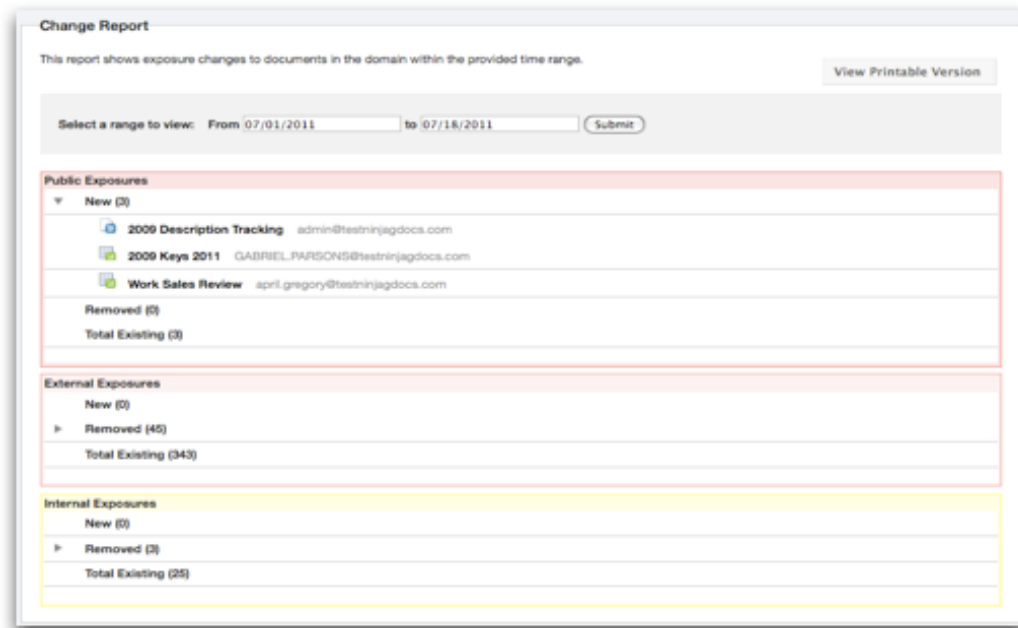
Dashboard > Administrator Action Log

- Jul 15, 2011 8:01 PM: admin viewed document ["2009 Description Tracking"](#)
- Jul 15, 2011 8:01 PM: admin removed access rights to the document ["2009 Description Tracking"](#) from the following user(s):
 - shane.rowe@testinjadocs.com
- Jul 15, 2011 7:47 PM: admin removed access rights to the document ["1x1 Partner Task"](#) from the following user(s):
 - stacy.vega@testinjadocs.com

Audit trail features in CloudLock for Google Apps

End user enablement - It is always difficult and time consuming for IT to manage access to documents without the help of end-users. The IT Department, being custodians of the data, do not always know the value of a document and its level of sensitivity. By enabling business users and managers to participate in the document access rights approval workflow, IT can reduce their workload and actually achieve better security.

Ongoing monitoring and tracking changes – after you have reviewed all documents and users, fixed access rights and exposures make sure you have an on-going monitoring in place to stay on-top of newly created documents and changes in permissions. Be sure that you can easily track changes in your entire domain.



Tracking changes with CloudLock for Google Apps

Alerting – an efficient way to stay on top of changes happening in your domain is to set up alerting. When you get policy-based alerts for permissions and exposure changes you can effectively ensure that you are closely monitoring the risks to the documents stored in your cloud file server.

End user enablement - It is always difficult and time consuming for IT to manage access to documents without the help of end-users. The IT Department, being custodians of the data, do not always know the value of a document and its level of sensitivity. By enabling business users and managers to participate in the document access rights approval workflow, IT can reduce their workload and actually achieve better security.

Comply With Regulations

If your company needs to comply with regulations such as SOX, HIPAA, FISMA, FERPA, PCI DSS or if you follow internal governance practices and undergoing internal audit, you need to have a data governance strategy and procedures in place. At the heart of any good governance strategy you need to:

Develop and implement an access rights control process - Review your current access rights control processes and identify what needs to be adjusted to support Google Docs. Companies that already employ access control processes for their on-premise data will have to extend the responsibilities of those involved to cover Google Apps as well. These processes need to be documented, assigned an owner in the organization, and must list the specific steps taken to manage access.

Monitor the control process - Regularly monitor and verify that the control process set in place is adhered to and is effective.

Audit the control process - Undergo a systematic review (yearly / quarterly) of the access control process to prove to internal and/or external auditors the existence of, and adherence to the access control process.

Allow auditors to inspect your domain – While auditors need to have access and visibility into the documents in your domain, their roles should be limited to an ‘audit’ function only, and their actions should be recorded and tracked.

Records management – Some regulations and internal compliance processes require a secure area where documents are stored that cannot be deleted or modified. Make sure that you have the facility to store documents where they are protected.

e-Discovery for Google Docs

The growing adoption of Google Docs as a data repository makes it a target for litigation holds and discovery processing. Usually, meeting the litigation hold request entails the following 3 steps:

Step One: Find all the relevant documents

Extract documents based on meta data and keywords searches, for example:

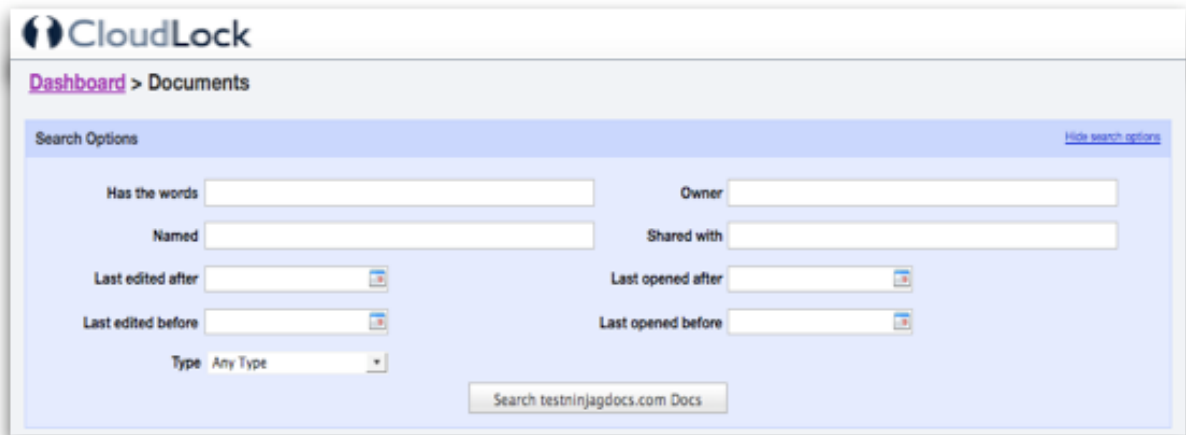
- All the documents owned by a specific user
- All the documents collaborated with a specific user
- All the documents that contain a specific keyword

Step #2: Copy and store relevant docs

Create a copy of these documents and store them in a protected area where they cannot be deleted or modified by end users.

Step #3: Extract and process

Extract these documents for further processing.



The screenshot shows the CloudLock interface for searching Google Docs. The page title is "CloudLock" and the breadcrumb is "Dashboard > Documents". Under "Search Options", there are several search criteria: "Has the words" (text input), "Owner" (text input), "Named" (text input), "Shared with" (text input), "Last edited after" (calendar picker), "Last opened after" (calendar picker), "Last edited before" (calendar picker), "Last opened before" (calendar picker), and "Type" (dropdown menu set to "Any Type"). A search button at the bottom contains the text "Search testninjagdocs.com Docs". A "Hide search options" link is visible in the top right corner of the search area.

Keywords and meta data search with CloudLock for Google Apps

CloudLock's advanced search capabilities give users the ability to search ALL the documents created or shared with your domain (including documents that you are not shared on explicitly).

The content search gives you the robust capability to search for specific keywords inside native Google documents (this includes: Documents, Presentation, Spreadsheets etc.).

Retaining Document Ownership

Google Apps has some unique characteristics as it applies to document ownership.

Technically, a document is always owned and bound to the life cycle of the user marked as its owner. This can affect the company's ability to retain ownership in several unexpected ways:

Employee account deletion - Since a document is bound to a user, when you delete a user, all their documents are deleted. This makes user account deletion and employee termination a higher risk activity that needs to be managed carefully. A recommended guideline is to suspend a user account (this will not delete their documents) and once termination is completed and verified you will need to transfer ownership of all the user's documents prior to deleting their account. Bulk transfer of ownership is possible through custom API development or through 3rd party applications.

Document shared from an external source - If you are working with external contractors or partners and they share a Google Docs document with you, they own the document. This is true even if they have created that document for you as part of their contract. This is important because the document is owned by your company yet you don't have control over it. If that contractor no longer works at their parent company and their account is deleted you will lose your document.

You should periodically identify all the documents that are owned by people outside of your domain and establish a review process with business users that would mark all the documents that should be owned by the company. You'll need to use [3rd party applications](#) (or write custom code using APIs) to transfer ownership from an external owner as Google doesn't support a transfer of ownership operation from users who are not members of your domain.

Document created using personal Google accounts - Many of your end users will be using Gmail for their personal account and occasionally will create a document in their personal account then share it with their work account. This is another case where the company logically owns a document but technically the document is owned by an external user that can delete it without any control by the company.

Conclusion

While the security concerns associated with data stored in Google Docs are valid, companies can achieve the same level of data protection in Google Docs as they have with their on-premise data. Using the built-in admin tools with a third-party security application such as CloudLock for Google Apps, you can take advantage of the cost savings and collaboration benefits of the platform while retaining the same enterprise-class data protection you need.

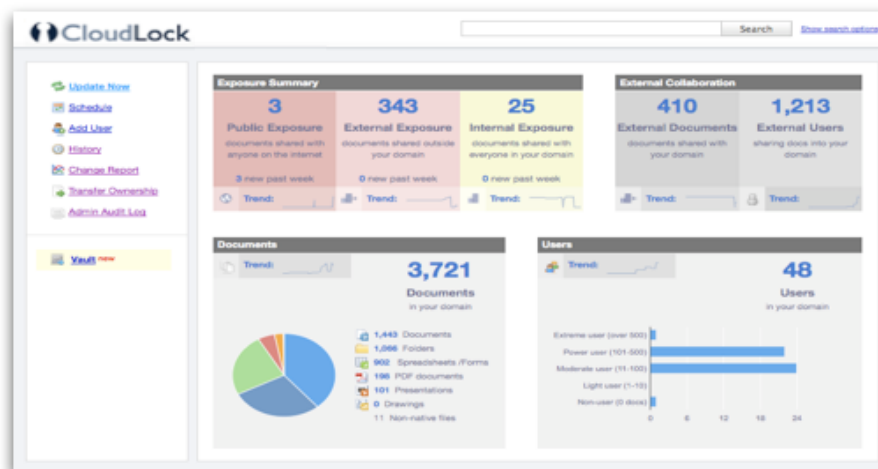
About CloudLock

For security conscious IT leaders looking to leverage the cloud, [CloudLock](#) is the cloud data protection company that enables control of data while gaining the collaboration and cost savings benefits of the cloud.

Unlike expensive custom solutions, CloudLock's enterprise-class products are directly integrated with cloud application providers and are immediately available at a fraction of the cost.

About CloudLock for Google Apps

CloudLock for Google Apps provides you the control and visibility you need over your domain's Google Docs. It allows you to secure and audit Google Docs, find and fix documents that are exposed outside and inside of your company. You can also perform audit, comply with regulations, set monitoring and alerts, and more.



Because it is a Google Marketplace application, adding CloudLock for Google Apps to an organization's Google Apps domain is fast and easy. Simply follow the step-by-step wizard to gain access to the service and configuration settings. All documents within your Google Docs environment can then be securely accessed instantly.

[Add it now](#)

[Get a free 7-day trial today!](#)