

“Now that I have CloudLock for Google Apps, I can delegate tasks to the security team and designated data owners, and can make sure that we are in control of our data - both for meeting data privacy regulations and following data governance best practices.”

Brian Bolt,
Systems Engineering
Team Lead,
Boise State University

CloudLock Customer Case Study: **Boise State University**

Control Sensitive Data Stored in Google Docs.



Boise State University selects CloudLock for Google Apps to comply with FERPA and other data privacy regulations.

Located in the heart of Idaho's commercial, cultural and civic capital, Boise State University plays a crucial role in the region's economic development and famed quality of life. Idaho's largest institution of higher education with nearly 20,000 students offers nearly 200 degrees and certificates in seven colleges. While remaining committed to the strong teaching legacy that has resulted in 11 Idaho Professor of the Year awards since 1990, Boise State's focus on innovation and creativity is fueling the fastest growing research program in Idaho. This robust growth contributed to U.S. News & World Report listing Boise State as one of the top up-and-coming schools in the nation for the past two years.

The Problem

In 2008, Boise State moved their student email system to Google Apps. They followed up this successful deployment with a move of faculty and staff to Google Apps in 2009. At the conclusion of the project, Boise State was the largest higher education institution using Google Apps as their sole messaging system.

Whether your services are operating in a self-owned and operated data center or in the Cloud, the IT staff has a responsibility to ensure compliance with privacy policies and regulations. Despite the successful adoption of Google Apps, Boise State's IT team needed visibility into the Google Docs in their Google Apps domain. They needed to know how many files were stored in Google Docs and they wanted the ability to identify excessive permissions.

The CloudLock Solution

CloudLock for Google Apps was installed in Boise State's staff and faculty domains directly from the Google Apps Marketplace. Within minutes they gained new insight into their Google Docs.

"I was surprised to see the number of Google Docs in our Google Apps domain. I knew that the Boise State faculty and staff were leveraging Google Docs; but until now, I did not know the extent of the usage," said Brian Bolt, System Engineering Team Lead, who was the original project manager for the Google Apps migration project.

"Now that I have CloudLock providing visibility into Google Docs, I can delegate tasks to the security team and make sure that we are able to see how Google Docs are shared."

Bi-Directional Visibility Into Google Docs and User Permissions

With over 5,500 accounts in the staff and faculty domain, Boise State University discovered over 60,000 files in their Google Docs environment. Those files, including both Google Docs, and other non-native Google Docs files, are at the heart of the day-to-day operational activity of the university. With CloudLock for Google Apps, designated IT staff now have the ability to view descriptive information about Google Docs without requiring access to the contents within any Google Doc. The university is now able to see:

- Which documents are shared with the 'public' or Internet
- Which documents are shared outside the organization
- Which documents are shared with 'Everyone' within the domain
- Who has access to what and what is accessible to whom

"The visibility that CloudLock provides, including whether Google Docs are shared externally, is immensely valuable," said Bolt.

Revoke Excessive Rights - Prevent Data Breaches

Once the initial scan of the Google Apps domain is complete, the domain administrator is able to take immediate action to address and prevent potentially harmful exposures of Google Docs. Within the intuitive CloudLock panel, a domain administrator can:

- Notify document owners - send an email advising the document owner about the current visibility of a particular document
- Change permissions – immediately revoke rights on documents without end-user involvement

“Having a tool that provides an administrative function for removing excessive permissions to Google Docs fills a longstanding need. Additionally, because CloudLock commits changes to a read-only log file, we now have a historical view of the changes made from within CloudLock,” said Bolt.

Enable End Users to Manage Entitlements

Managing access rights is typically the responsibility of IT staff. Google Apps provides native access to APIs that are useful for accessing information with a Google Apps domain, but only domain administrators, with knowledge of the underlying Google Apps APIs, have the ability to view the descriptive Google Docs information. With CloudLock's easy to navigate interface, the domain administrator can easily administer Google Docs, as well as delegate access to non-admin users.

An upcoming CloudLock end-user entitlement feature will enhance CloudLock's foundational access controls and will enable the Google Apps domain administrator to delegate CloudLock privileges to Google Apps accounts that are not domain administrators. This feature will allow:

- Effective policy enforcement - ensure that Google Docs owners comply with corporate sharing policies
- Increase accountability - provide Google Docs owners with visibility and control

"CloudLock gives me the ability to let non-admin users manage their Google Docs without providing them full administrative access to the Google Apps domain. With CloudLock, I can provide the University's Information Security Officer the ability to view, and if necessary, change access to Google Docs in our domain. Before CloudLock, the only available alternative required me to elevate their Google Apps account to an administrator of the domain," says Bolt. "And when the end-user enablement feature goes live, I can give the Google Docs owners that same ability."

Benefits of a Google App Engine Solution

"Any document management solution requires collecting, storing and processing large quantities of information," said Bolt. "Our security team appreciates the fact that the CloudLock solution is developed and hosted on the Google App Engine platform; and since CloudLock is powered by Google's App Engine, our data never leaves Google's Cloud Infrastructure."

**For More Information Regarding CloudLock for Google Apps Please
Contact sales@cloudlock.com**

**To start a free trial of CloudLock for Google Apps visit
<http://www.cloudlock.com/>**