

CloudLock Customer Case Study: Kenshoo – Digital Marketing Software

Data Governance and Auditing for Google Apps

Kenshoo Selects CloudLock for Data Governance and Auditing for Google Documents and Sites



Kenshoo is a digital marketing software company that engineers technology solutions for search marketing, social media and

online advertising. Advertisers, agencies, and marketing providers use Kenshoo Enterprise, Kenshoo Local, and Kenshoo Social to direct more than \$15 billion in annual customer sales revenue. The Kenshoo Universal Platform delivers automation, business intelligence, integration, and scale to make better marketing investments.

Kenshoo powers 6 of the top 10 hotel groups, 7 of the top 10 retailers in the world, 7 of the top 10 telecoms, 9 of the top 10 ad agency networks, and 23 of Fortune 50 companies. With campaigns running in more than 100 countries, Kenshoo customers include Annalect, Barnes & Noble, CareerBuilder, Facebook, Havas Digital, Hitwise, iREP, John Lewis, LendingTree, Sears, Starcom MediaVest Group, Tesco, Travelocity, Walgreens, and Zappos.

The Problem

Kenshoo is a global company with multiple international offices. The challenges of managing a distributed environment pushed the IT department to make the transition to Google Apps.

“After moving to Google Apps, I started looking for auditing tools that would give me the visibility and controls I need to manage our Google Apps Documents and Sites,” said Eyal Menahem, Corporate IT Manager at Kenshoo.

Menahem was introduced to CloudLock by DoIT! Corp, a leading Google Apps reseller in the Mediterranean and Africa. “We see the tremendous value that CloudLock provides to our customers. This is a must-have application for enterprises of all size that are serious about security and compliance for Google Apps,” said Vadim Solovey, CEO & Executive Partner at [DoIT! Corp](#).

“With CloudLock I can easily monitor and audit all our external sharing and get alerts on new exposures. I've evaluated other auditing tools and CloudLock is by far the best.”

Eyal Menahem,
Corporate IT Manager,
Kenshoo

“CloudLock is a must have application for enterprises of all size that are serious about security and compliance for Google Apps.”

Vadim Solovey, CEO &
Executive Partner DoIT!
Corp

Auditing External Sharing and Exposures

“With CloudLock I can easily monitor and audit all our external sharing and get alerts on new exposures. I've evaluated other auditing tools and CloudLock is by far the best,” said Menachem.

CloudLock gives enterprises the tools they need to make sure sensitive data is not exposed, by enabling:

- **Full Control of Permissions and Access Rights** – CloudLock gives Google Apps domain administrators an effective way to manage documents, sites, collections, and users in the domain as well as documents shared from outside the domain. CloudLock users can change and correct permissions for all documents and collections, including those they are not shared on.
- **Automated Monitoring and Alerting** - CloudLock provides ongoing monitoring of the entire domain with email alerts on newly exposed documents and changes in permissions for existing documents.
- **Bulk Operations** – With CloudLock, domain administrators can enforce access controls by adding or removing collaborators, changing ownership, and changing collaborator access rights on all or some documents in the domain.
- **Change Report** – CloudLock's ongoing monitoring of all the users and documents allows domain administrators a view into changes in ownership and changes for every document created or shared with the domain. The ad-hoc reporting to see what has changed between any two dates.

Delegating Security to End Users

Enabling CloudLock's End User Enablement lets domain administrators delegate security to the data owners, letting IT and users share the security burden collaboratively.

CloudLock allows domain administrators to maintain control of Google Docs while showing data owners their exposed documents. The documents are classified and tagged by the following 4 categories:

- **Public Exposure** – Documents that are exposed to everyone on the Internet
- **External Exposure** - Documents that are exposed to outsiders
- **Internal Exposure** – Documents that are shared with everyone in the domain
- **New Exposure** – Includes all the newly exposed documents in the last 7 days

Implementing Acceptable Use Policies with CloudLock's Security Policy Engine

CloudLock's consolidated dashboard provides immediate visibility into all documents, users, and exposures, highlighting risks for the entire domain and allowing a quick drill-through into exposed data to view and take immediate actions to secure exposures.

In addition to the CloudLock dashboard, CloudLock's security policy engine enables companies to define specific acceptable use policies (AUPs). CloudLock's Security Policy Engine provides organizations the framework necessary to define policies and make sure that collaboration practices are monitored and remain compliant with governance policies and procedures.

"With CloudLock's security policy engine we can set policies on specific users or departments and make sure violations are immediately flagged and addressed," said Menachem.

For more information on CloudLock for Google Apps please contact sales@cloudlock.com

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