Adaptive Security for Google Drive

Are you concerned about what type of content is being uploaded and shared in your Google Drive account? What are the compliance risks? Which user accounts may have been compromised?

See how Elastica can keep your Google Drive account safe and compliant.

- **Automate**
  - classification and governance of compliance-related data, such as PII, PCI and PHI

- **Enforce**
  - content-aware and context-aware policies to safeguard sensitive data

- **Detect and prevent**
  - threats based on patent-pending data science algorithms

- **Streamline**
  - incident response tapping granular log data with powerful analysis tools
Peace of mind comes from the knowledge that Elastica Securlet™ for Google Drive is working on your behalf to keep your data in Google Drive safe, secure and compliant.

It’s easy to get going!

Exposure Risk
Elastica’s Securlet™ for Google Drive highlights files that are exposed publicly, externally or internally.

Compliance Risk
ContentIQ™ automatically highlights possible Compliance Risks, without you having to manually define keywords or regular expressions.

Users with Sensitive Content
Users with the most compliance risks are highlighted.

Abstract Policy Definition
Define content-aware and context-aware policies to automatically remediate risks and exposures as they occur, prevent data leakage and thwart malicious activity. Alternatively set up email notifications to alert users or administrators of such activity.

Risk Remediation
If you want to manually rid a certain set of files from risks of various kinds, simply filter down the set and apply bulk remediation.

Malware Detection
Identify potential malware attacks through automated monitoring of account behavior. Create policies that generate alerts and/or block suspicious account activity in real-time.

Sensitive Content Risk
Patent-pending ContentIQ™ technology, based on advanced semantic analysis, frees you from manually having to define keywords or regular expressions.

Usage Analytics
Filing based on user, content type, and risk type is a breeze. You get a slick desktop style experience.

Users with Exposures
Users with the most exposures are identified.

Real-time Enforcement
Prevent security or compliance incidents from occurring with real-time enforcement of policies triggered by ThreatScore™ or content-aware policies.

User Centric ThreatScore™
Account takeovers can put your content at serious risk. Elastica’s machine learning based Intrusion Detection assigns a ThreatScore™ to each and every user, enabling you to directly zoom into risky users.

Incident Response
Incidents happen. Elastica Securlet™ for Google Drive enables you to go back in time and zoom into a specific user, document or activity and correlate events.
Elastica is the leader in Data Science Powered™ Cloud Application Security. Its CloudSOC™ platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of Elastica Security Apps deployed on the extensible CloudSOC™ platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against intrusions and compliance violations, and investigation of historical account activity for post-incident analysis.