BLUE COAT | elastica

SOLUTION BRIEF

Adaptive Security for Cloud Apps

Are you concerned about what type of content is being uploaded and shared in common cloud apps? What are the compliance risks? Which user accounts may have been compromised?

See how Elastica can keep your cloud accounts safe and compliant.

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

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

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

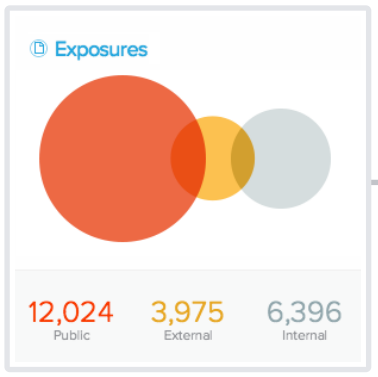
Streamline
incident response tapping granular log data with powerful analysis tools

It's easy to get going!

Connect to an Elastica Securlet™ for a specific cloud app using the corresponding API in seconds.

Exposure Risk

Elastica Securlets for cloud apps highlight files that are exposed publicly, externally or internally.

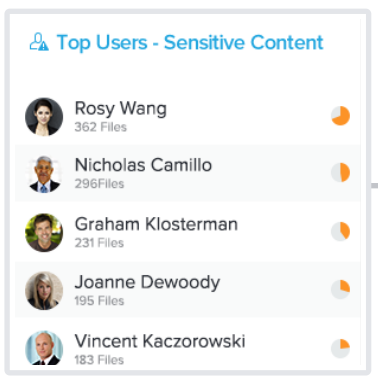


Compliance Risk

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

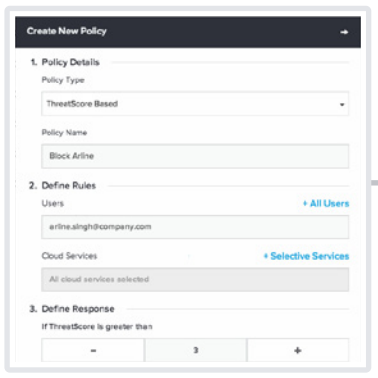
Users with Sensitive Content

Users with the most **compliance risks** are highlighted.



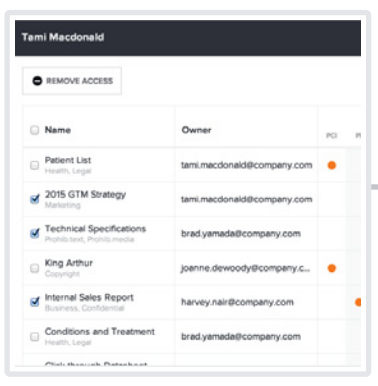
Abstract Policy Definition

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.



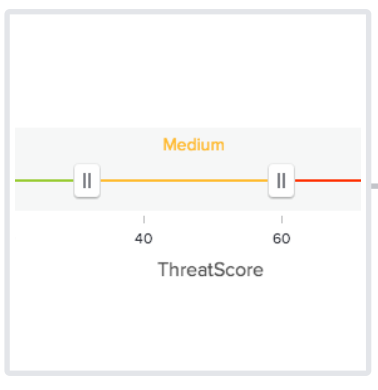
Risk Remediation

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.



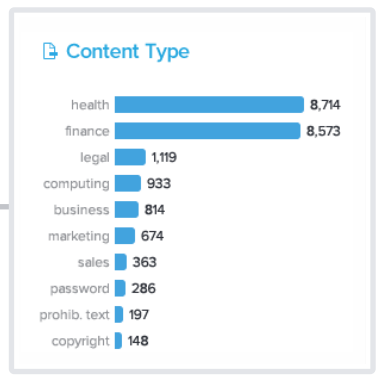
Malware Detection

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



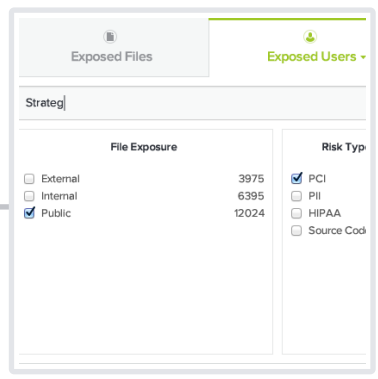
Sensitive Content Risk

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



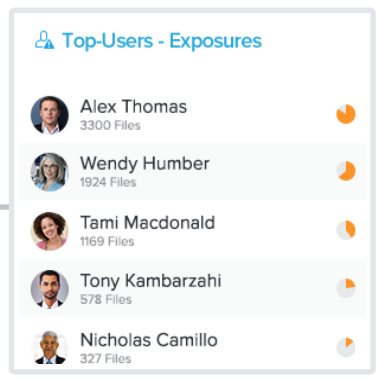
Usage Analytics

Filtering 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

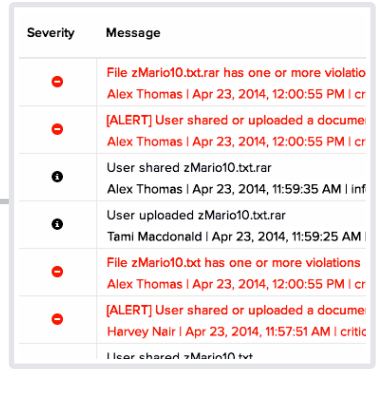
Prevent security or compliance incidents from occurring with real-time enforcement of policies triggered by ThreatScore™ or content-aware policies.

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

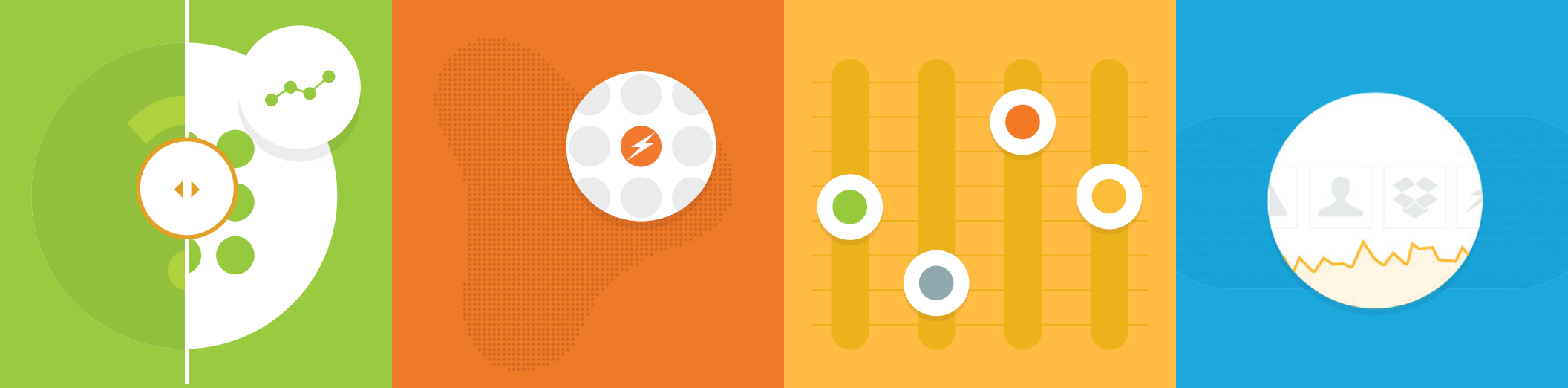
Incidents happen. Elastica Securlets for cloud apps enable you to go back in time and zoom into a specific user, document or activity and correlate events.



END RESULT

Peace of mind

comes from the knowledge that Elastica Securlets for cloud apps are working on your behalf to keep your data safe, secure and, compliant.



Data Science Powered™ Cloud App Security

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.

elastica

A BLUE COAT COMPANY

3055 Olin Avenue, Suite 2000, San Jose, CA 95128
sales@elastica.net • elastica.net