BLUE COAT
Network + Security + Cloud

At-A-Glance
Elastica CASB

Data Science
- Machine learning & computational linguistics-driven ContentIQ™ engine identifies more true positives & dramatically reduces false positives
- Machine learning-based algorithms deliver more detailed user-to-cloud activity intelligence (StreamIQTM)

Visibility
- Best CASB UI
- Discovery & intelligence on over 15k cloud apps
- App Business Readiness Ratings based on analysis of 60+ risk attributes
- Integrated SWG + CASB for dynamic app control
- Dashboard view of at risk sensitive data & suspicious user behavior

Data Governance
- Security for sanctioned (API) & unsanctioned apps (Gateway)
- Highly accurate content identification & DLP with ContentIQ™ & custom learning engine
- Automated DLP remediation & policy controls

Threat Protection
- Inline gateway for control over all cloud app traffic
- Uniquely granular visibility & policy control over traffice to/from cloud services (StreamIQ™)
- Uniquely accurate & automated risk analysis, user behavior visibility & policy control (ThreatScore)

Incident Response
- Best CASB for fast, detailed incident investigation
- Query-based log discovery for targeted analysis
- Relevant log details presented in useful natural language
- Integrate with SIEM platforms

Sanctioned Apps

Company Accounts
SECURED THROUGH CASB GATEWAY, CLOUD APIs, AND TOKENIZATION

Personal Accounts
SECURED THROUGH CASB GATEWAY

Shadow IT Audit

Unsanctioned Apps

Too Popular to be Blocked
SECURED THROUGH CASB GATEWAY

Can be Blocked
AUTOMATIC SHADOW IT CONTROLS IN PROXYSG/ WSS

elastica CloudSOC™

DETECT

PROTECT

INVESTIGATE

Block/Control 15k apps w/ ProxySG + AUDIT

Governance over sanctioned apps/accounts

Inline Visibility/Control over sanctioned & unsanctioned apps & personal accounts

BLUE COAT
Network + Security + Cloud

At-A-Glance
Elastica CASB

"95% of cloud security failures will be the customer's fault"
Source: Gartner Predictions for 2016

Limitations of Other CASBs

Native App Security	• Visibility limited to one app • Inability to track user behavior & threats across multiple apps • Staff must develop expertise in and maintain yet another security mgmt system • Disparate app security platforms make it arduous to consolidate, track & standardize security for visibility, data governance, threat protection, & incident response • Encryption keys held by App provider – challenging compliance requirements
API-only CASBs (no Gateway)	• Only sanctioned apps with rich APIs are supported • No governance of unsanctioned apps/accounts • No correlation of suspicious user activity across cloud apps or across company & personal accounts • No inline encryption of data

CASBs w/ reverse proxy architecture	• Reverse proxy requires URL redirects that can:
	  • Can't be implemented with hard-coded native mobile apps
	  • Break unexpectedly when cloud app platform updates change URLs

Elastica Advantages

- Support for sanctioned & unsanctioned cloud apps w/ API + Gateway
- Single Pane of Glass cloud security mgmt w/ excellent UI plus ability to extend & integrate with 3rd party mgmt platforms
- Accurate DLP across sanctioned & unsanctioned apps
- Inline encryption of data
- Detailed visibility & control over user transactions w/ sanctioned & unsanctioned apps & accounts
- Detect & correlate threats across multiple cloud apps & accounts
- Forward proxy architecture enables visibility into more apps including native mobile apps
- Data science-driven intelligence engines deliver more accuracy & reduce need for manual intervention

Qualifying Questions

- Do you know how many cloud apps are being used across your enterprise? Do you know which apps and which users? How do you monitor and control use of unsanctioned cloud apps & accounts? Typical organizations have 800+ cloud apps in use. More than 90% of cloud apps are not business ready.
- How do you make sure you use compliant cloud apps? 95% of cloud apps are not SOC2 compliant, 84% are not PCI compliant, 91% are not HIPAA compliant.
- Do you use Office 365, Google Apps, Salesforce, Box, Dropbox, ServiceNow, AWS or other cloud services? Most organizations use one or more of these for strategic business operations.
- How do you monitor & protect your data in sanctioned & unsanctioned apps? Are you sure you are compliant handling PII/PCI/PHI/etc? Accidental over-sharing happens all the time. In 2015, 10% of files broadly shared in the cloud contained sensitive data.
- How do you protect against unauthorized access to your cloud accounts? Your cloud provider doesn't protect you from front door attacks using hacked or stolen credentials.