Hunting The Shadow

Government Safe Passage to Cloud

| BAYAN ACHKAR - Senior Systems Engineer |
“The rapid adoption of cloud services has led to a new class of security, compliance and data governance headaches. Enter the Cloud Access Security Broker.”

CASB: #1 SECURITY CATEGORY FOR INQUIRIES
Seismic Shifts Causing Organizations to Rethink Security

- **Evolving Network Usage Patterns**
- **Next-Generation Endpoint Revolution**
- **Shift to Cloud Application Usage Models**

Shadow IT  Shadow Data
Requires New Security Architecture

Traditional On-Premises SOC
- Risk Assessment
- Intrusion Detection
- Malware Detection
- Proxy/Firewall
- DLP
- Incident Response
- Investigations
- Compliance

Integrated Cloud SOC
- Shadow IT Risk Assessment
- Cloud Intrusion Detection
- Cloud Malware Detection
- Cloud Policy & Remediation
- Cloud DLP
- Cloud Incident Response
- Cloud Investigations
- Cloud Compliance
- Tokenization

Unmonitored activities outside on-premises reach Cloud Traffic
CASB

• What is CASB?
• Why it is Important?
• The 4 Pillars of CASB
  1. Visibility: Shadow IT.
  2. Compliance: HIPAA, PCI, PII.
  4. Data Security: Tokenization/Encryption/DLP.
The SaaS (Software-as-a-Service) era is here. According to Gartner, SaaS and cloud-based business application services revenue will grow to $32.8 billion USD in 2016. Modalities: Pure Cloud, Hybrid, Private

A cloud access security broker (CASB) is a software tool or service that sits between an organization’s on-premises infrastructure and a cloud provider's infrastructure.

Eliminate Risk require a new approach to data governance, risk management and security because of the ubiquitous nature of access, the collaborative nature of SaaS applications, and the myriad ways that confidential data can be stored within applications.

By 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services, which is up from fewer than 5% in 2015.
USE OF SANCTIONED & UNSANCTIONED CLOUDS
Each Represent unique Security Challenges
Multiple Sources of Data

- Cloud API
- Cloud Proxy
- Logs
- Proxy
- Outside Perimeter
- Enterprise Perimeter

Cloud Security Solution

- Shadow IT Risk Assessment
- Cloud Intrusion Detection
- Cloud Malware Detection
- Cloud Policy & Remediation
- Cloud DLP
- Cloud Incident Response
- Cloud Investigations
- Cloud Compliance
- Tokenization
Securing Data in Sanctioned Cloud Apps

- **Field-Level Encryption/Tokenization**
  - *Field-level* data replaced with surrogate encrypted or token value in enterprise SaaS apps
  - Functionality maintained (e.g. Searching on protected data)

- **File-Level Encryption**
  - Encrypt *files* in applications like Box, Dropbox, Google Drive
CASB – DATA PROTECTION

Authorized Users → Blue Coat Cloud Data Protection Platform(s) → Non-authorized Users

Direct Connection to Salesforce.com

FUNCTIONALITY PRESERVED
How many apps do you think your employees are using?

IT DEPT. PERCEPTION: 40-50 apps
REALITY: 812 apps

Source: 1Elastica Q4 2015 Shadow Data Report
Malicious Activity

**Session Hijacking**
Malware agents (or bots) on end-user systems can hijack cloud app sessions.

**Account Takeover**
User credentials may become compromised through phishing attacks or similar techniques.

**Malicious Insiders**
A disgruntled employee may abuse company assets.
Extract User Activity with Cloud Proxy or APIs

Analyze web traffic (including SSL) and extract granular detail in real-time.
Protect Against Malicious Attacks
Typical Shadow Data Risk

23% of files per user are broadly shared (average)

12% of these files contain confidential data

48% CODE

33% PII

14% PHI

5% PCI
Data Classification and Protection

Automatically classify, detect and remediate content uploaded to cloud apps leveraging semantic analysis

Create & enforce granular policies based on wide range of criteria, including: users, device, location, file properties, access properties, content, activity, threat score
Threat Protection & Incident Response

Visibility
behavior in app, inline traffic activity & logs

Analyze & Act
on suspicious activity

Automate Protection
w/ policy controls & malware scanning

Incident Response
for security investigations

Cloud APIs
Securlets™

Proxy logs
Elastica Audit

Cloud App Traffic
Elastica Gateway
Blue Coat Leadership in CASB

Cloud Generation Security Gateway combining Proxy SG with the broadest set of CASB capabilities in the market

Cloud App Visibility
- Identify Shadow IT & Monitor cloud app usage in real time

Data Governance & Controls
- Govern sensitive data with granular controls

Data Protection
- Encrypt & Tokenize data in-transit, at-rest, and in-use to ensure compliance

Threat Protection
- Combat evolving threats leveraging user behavior analytics