The Industry Need for Cloud Generation Security

John Andreadis, CISSP, CISA
Phimm Phonpaseuth
| Cloud Security, Canada
Market Demand for Cloud is Increasing


Forbes / Tech

JUN 18, 2015 @ 01:19 PM 6,900 VIEWS

Report: Cloud Market Cap To Pass $500 Billion By 2020

Cloud apps are becoming an essential part of business

- Cost effective
- Remote access
- Agility and speed
- Improved Productivity
- Better collaboration
Reality of Technology World

Every time you opt for new technology, you have to secure it.

You wouldn’t run your business without email…

…and you wouldn’t use email without security

As business adopts cloud apps…

…I…you must secure them
Cloud Enabled

I want instant access to all my project files, the freedom to share docs and to collaborate with anyone, anywhere, anytime—from any device or location.

Cloud Secure

I must keep my critical business assets and customer info safe from data breaches, keep my organization compliant, and know what cloud apps my employees are using.

No longer a split decision

Have your cloud......and secure it too
Compliance and Security

There is a difference between Security and Compliance in the Cloud!
Are client records being shared publicly?
Who is accessing your cloud data?
Indian government leaked shadow data through Google Drive

Error Exposes 1.5 Million People's Private Medical Records on Amazon Web Services [UPDATED]

Morgan Stanley Fires Rogue Employee After Customer Data Leak
Accidental Over-sharing

Alice shares a file with Bob

Bob shares that file with others

Or shares via other apps
Shadow Data

Of the Average User's Documents Stored in the Cloud, 26% of these files per user are broadly shared (average).

10% contain compliance related data.

- 80% MISTAKE
- 7% HIJACKED
- 12% INSIDER

—Aberdeen Study 2014

© 2015 Elastica, Inc. All Rights Reserved. Confidential Information. Do Not Distribute.
Malicious Activity

Session Hijacking

Malware can be used to hijack a user’s account and gain access to critical data. In these cases, malware agents (or bots) on end-user systems hijack cloud app sessions.

Account Takeover

A major data breach can come down to a single user password being compromised. Whether due to a phishing attack or a broader password breach, it represents a single point of failure that can expose critical data.

Malicious Insiders

A disgruntled employee may divulge sensitive data, download confidential information, or delete data prior to leaving a company.
Window of Exposure

\[ w(e) = \text{Window of Exposure} \]

\[ w(d) = \text{Window of Detection} \]

\[ w(p) = \text{Window of Prevention} \]

Vulnerable to Attackers Until Prevented
Innovation for the Cloud Generation: Securing A New World of Devices, Networks and Applications

Protection from Advanced Threats

Ensuring Safe Cloud Usage

curing Mobile Workforce

Cloud Generation Security
Innovation for the Cloud Generation: Protection from Advanced Threats

PROTECTION FROM ADVANCED THREATS

PROTECT AND MANAGE ENDPOINTS AND DEVICES
• Proactively block known and unknown threats with machine learning.

SECURE DATACENTER ENVIRONMENTS
• Protect servers, data repositories, and ensure compliance across physical, virtual and cloud-based workloads

PROTECT WEB & EMAIL
• Inbound and outbound web and email security, with protection against targeted attacks, spear phishing, advanced malware, spam and bulk mail

MANAGING ENCRYPTION RESPONSIBLY
• Leveraging policy to responsibly decrypt and feed security controls for visibility

DISCOVER AND REMEDIATE
• Leverage combined intelligence to automatically remediate impacted assets
Innovation for the Cloud Generation: Securing a Mobile Workforce

FOLLOW AND PROTECT USERS
• Symantec Intelligent Endpoint + Blue Coat Cloud Gateway protect users anywhere they go

GAIN CONTROL AND VISIBILITY
• Leverage cloud-based gateway to perform endpoint protection for non-traditional devices

SECURING A MOBILE WORKFORCE
Innovation for the Cloud Generation: Ensuring Safe Cloud Usage

ENSURING SAFE CLOUD USAGE

PROTECT INFORMATION
• Inspect and classify sensitive content
• Protect content before it leaves organizational control
• Encrypt and tokenize content as it interacts with cloud applications and devices

MANAGE CLOUD APPLICATION USAGE
• Consolidate security control and visibility over sanctioned cloud applications
• Gain visibility into shadow IT computing usage

Mobile/BYOD/IoT Endpoints
Complications of Cloud Adoption

- Who Owns the Comprehensive Service Level Agreements?
- Single Pane of Glass?
- Redundancy & High-Availability?
- Vendor Compatibility?
Advantages of a Consolidated Cloud

• Clear SLA and RCA
• Single Pane of Glass
• Unified Reporting and Management
• Inherent Performance Benefits
• Redundancy & High-Availability
• Global Scale
• Same level of visibility, protection, and forensic capabilities for remote traffic

Simplicity Delivered
A Portfolio to Deliver Cloud Generation Security
Positioned for a Continued Future of Industry Leadership

Protection from Advanced Threats
Securing a Mobile Workforce
Ensuring Safe Cloud Usage

Cloud Generation Security
Existing Security Challenges for Cloud Apps

- Shadow IT/Data - large number of unknown cloud apps
- Manual efforts cannot scale to audit Cloud apps
- Managing audit data for large set of applications
- Lack of automation tools to address issues in cloud apps
- Time constraints in completing audit tasks, released reports, etc.

What is the answer to these real world problems?
Platform driven Approach for Cloud App Security

Auditing
- find active hidden cloud services or applications in use
- dissect Shadow IT usage in the networks

Detection
- detect abuse and malicious use SaaS applications
- unearth the potential mistakes made by users which result in information disclosure and data leakage

Prevention
- stop the malicious use SaaS application before actual impact is triggered

Approaches
- Machine learning based algorithms
- Security policies and rules
- Automated signature generation
- Heuristic approaches such as frequency calculation and threshold base lining
- Pattern search and analysis

© 2015 Elastica, Inc. All Rights Reserved. Confidential Information. Do Not Distribute.
Shadow IT Analysis

359 active users
273 apps
87 destinations

45% apps are medium risk or higher

TOP 5 RISKIEST APPS
1. PERFECT MARKET
2. LIVERAIL
3. ENGAGE
4. ZEDO
5. DAUGLES

© 2015 Elastica, Inc. All Rights Reserved. Confidential Information. Do Not Distribute.
Data Science for Cloud Apps

• Analyzing Content in the Cloud
  • Machine Learning for data analysis: extending DLP to the next level
  • Contextual analysis of the data: leveraging data granularity
  • Out-of-box detection of sensitive content: detecting leakages PII / PHI / PCI
  • Robust identification of encrypted files: filtering data
Data Science for Cloud Apps

- Deep Content Inspection (DCI)

1. Computational linguistics
2. Cluster analysis
3. Document structure analysis
4. Information theory
Data Science for Cloud Apps
Traffic flows and analysis
• Event Identification inside SaaS to Track User Activity (StreamIQ)
  • Analyzing SaaS applications network traffic data for extracting granular information
  • Automating the process of generating “Activity Signatures” for users
  • Machine learning algorithms are used for “Event Identification”
  • Testing “Activity Signatures” against known data sets
  • Deploying signatures for detecting real-time user activity in cloud
Monitoring and Control of Cloud Apps
Monitoring and Control of Cloud Apps

API

GATEWAY

elastica CloudSOC™

© 2015 Elastica, Inc. All Rights Reserved. Confidential Information. Do Not Distribute.
A unique baseline behavioral pattern establishes a confidence curve for each user’s typical behavior. Any significant deviation or combination of suspicious events trigger appropriate alarms or policies to quarantine or block that account’s activity.
Data Science for Cloud Apps

StreamIQ

1. Automatically analyze user data assembled by StreamIQ
2. Surface problematic users and user accounts in real-time
3. Highlight risk level of specific activities
4. Flag suspicious behavior for investigation
Tectonic Shift in the Market

Traditional Security Stack
- Risk Assessment
- IDS/IPS
- DLP
- Firewall
- SIEM
- eDiscovery

Unmonitored Activities
Bypass Traditional Security

CLOUD ERA

PRE-CLOUD ERA

Enterprise
New Security Stack for Cloud Apps

Unmonitored Activities Bypass Traditional Security

Traditional Security Stack
- Risk Assessment
- IDS/IPS
- DLP
- Firewall
- SIEM
- eDiscovery

Enterprise

CLOUD ERA
PRE-CLOUD ERA

© 2015 Elastica, Inc. All Rights Reserved. Confidential Information. Do Not Distribute.
Multiple Sources of Data

Full Coverage of Attack Lifecycle

Traditional Security Stack
- Risk Assessment
- IDS/IPS
- DLP
- Firewall
- SIEM
- eDiscovery

Enterprise

CLOUD ERA

PRE-CLOUD ERA
GATEWAY

Sanctioned Apps

Personal Accounts

Secured Through GATEWAY

Cloud Apps

CloudSOC

API

Unsanctioned Apps

Apps to Monitor

Secured Through GATEWAY

Apps to Block

 Fine Tune Web Proxies and Firewalls; Block Apps

Company Accounts

Secured Through GATEWAY AND APP APIs

Cloud SOC Agent

Audit

Enterprise Perimeter

Logs
Conclusion

- Cloud applications are encountering threats from:
  - Employees (unintentional) | Malicious Insiders (intentional) | Attackers (intentional)

- Potential steps towards securing cloud apps:
  - Need for complete platform-driven CASB solution that:
    - uses Data Science as an underlying technology to implement advance techniques
    - unveils Shadow IT usage in the networks
    - dissects layer-by-layer user activity in the cloud
    - detects anomalies and threats in cloud
    - enables auditors to implement protective measures
  - Use of reputable cloud app
  - Requirement of Decent Identity Management system (IDM)
Thanks. Questions?