Cloud Access Security Broker

Ted Hendriks
HP Atalla Pre-Sales Consultant, APJ Region
HP Enterprise Security Products
We are rapidly moving towards a Cloud majority world.

However, Cloud adoption has also introduced a new set of risks, both internal and external:

- Cloud providers are not liable or accountable for enterprise data in the cloud
- Every cloud provider has different sets of controls for their cloud application
- Existing security solutions don’t extend to cloud app
THE NEED FOR SAAS SECURITY

Cloud providers are not accountable

"Customer is responsible for maintaining the confidentiality of its account and password and for restricting and granting access thereto"

"None of the provider entities have any obligation to verify that anyone using customer’s account and password has customer’s authorization"

Existing security controls do not extend to the cloud

- End Point: Any device is accessible to SaaS
- Network: Entirely based on public networks
- Application: Dependency on SaaS provider
MAIN CHALLENGES FOR SAAS SECURITY

Access
- What happens if an employee’s home computer is stolen?
- How can I limit access from unmanaged devices?

Data
- How do I know if sensitive data is shared externally/publicly?
- How do I protect sensitive data when it is downloaded on to an unmanaged device?

Breach
- What if a user’s account is breached?
- What if a disgruntled employee decides to exfiltrate data?
ADALLOM IS A CASB AND IS CHOSEN BY LEADING COMPANIES
Integrates with multiple cloud applications

Work with any user, network, any device (managed & unmanaged)

Secure data at rest and data in motion

Cloud Security Platform – integrates with existing controls (DLP, SIEM etc.)

Ease of deployment (less than 10 mins to deploy)
VISIBILITY, GOVERNANCE, PROTECTION

Visibility
- Gain insights into users, data, activities, access
- Understand how files are being shared with collaborators
- Discover more than 13,000 cloud apps, understand risks
- Find anomalies and threats

Governance
- Address compliance with cloud DLP and eDiscovery
- Complete attestation and audit trails
- Govern access, devices, activities and datasharing
- Manage users including privileged and zombies

Protection
- Data security - Encrypt sensitive files and manage orphans
- Identify risky behaviors
- Fingerprint baseline usage

www.cloudsec.com | #CLOUDSEC2015
OUR PLATFORM APPROACH

Flexible integrations
- API
- SmartProxy™
- Hybrid

Deeper, meaningful context
- Users
- Data
- Access
- Activity
- Location

Unmatched efficacy
- SmartEngine™ Advanced Heuristics
- Adallom Labs

Actionable Insights
- Visibility
  - Dashboard
  - Audit Trails
  - Reports
- Governance
  - Data Security
  - eDiscovery
  - Usage and access
- Protection
  - Anomalous behaviors
  - High-risk usage
  - Security incidents

Adallom Cloud Application Security Platform

Extensible to DLP, SIEM and encryption solutions
CHOICE OF DEPLOYMENT ARCHITECTURE DEPENDING ON USE CASE

API Integration for normal usage

- Scalable model
- Sits out of band (minimal performance impact)
- HP currently using this mode

Smart Proxy for high-security use cases

- Monitors data in real time for more control and governance
## COMPREHENSIVE SECURITY CONTROLS

### Data Protection
- Cloud Encryption/IRM
- Sharing control (3rd party and ecosystem)
- Govern access to data
- Govern lifecycle of data

### Compliance & Risks
- Cloud Risk Reports
- Cloud DLP
- eDiscovery
- Reports on config management

### Access & Activities
- Limit access by device, IP, user, role
- Device pinning
- Granular activity policies

### Threat Prevention
- Anomaly detection
- Security incidents
- Security intelligence
- Heuristics engine

---

**Over 13,000 discoverable apps with the ability to onboard advanced protection for any app in about 2 weeks**

---

Cloud application security platform

<table>
<thead>
<tr>
<th>Data Protection</th>
<th>Compliance &amp; Risks</th>
<th>Access &amp; Activities</th>
<th>Threat Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cloud Encryption/IRM</td>
<td>- Cloud Risk Reports</td>
<td>- Limit access by device, IP, user, role</td>
<td>- Anomaly detection</td>
</tr>
<tr>
<td>- Sharing control (3rd party and ecosystem)</td>
<td>- Cloud DLP</td>
<td>- Device pinning</td>
<td>- Security incidents</td>
</tr>
<tr>
<td>- Govern access to data</td>
<td>- eDiscovery</td>
<td>- Granular activity policies</td>
<td>- Security intelligence</td>
</tr>
<tr>
<td>- Govern lifecycle of data</td>
<td>- Reports on config management</td>
<td></td>
<td>- Heuristics engine</td>
</tr>
</tbody>
</table>

---

Encrypti on and IRM

DLP

SSO

NAC

SIE

M

On-premises controls

www.cloudsec.com | #CLOUDSEC2015
HOW TO DEPLOY

Periodic discovery of 13,000 cloud services with 60+ risk ratings

Manage corporate-approved applications

Phase 1: Out-of-band
- Out-of-band visibility and governance
- Cloud-to-cloud API

Phase 2: In-line prevention for access
- Control access based on device (managed/unmanaged), IP, location, user or role
- Access control proxy

Phase 3: In-line prevention for specific use cases
- Control access, content and activities "Allow Sales to download Box documents on unmanaged devices, but encrypt/IRM"
- Full Proxy

www.cloudsec.com | #CLOUDSEC2015
DISCOVERY OF SHADOW IT

Adallom Discovery Database
13K+ SaaS Applications

- Risk score based on 60+ risk factor service assessment
- Details on top users and service activity

Logs from network devices, firewalls, etc…

Adallom Discovery - Largest and most accurate cloud services database

Enriches Adallom Discovery with 75M users worldwide and 1B+ web requests categorized per day.
DISCOVERY OF SHADOW IT

Cloud security research

IAM connector

+13,000 cloud applications

Cloud-to-cloud discovery

+1 billion transactions per day

Deployment Options

On-premise

Cloud

Logs from network devices, firewalls, etc…

Cloud - to - cloud deployment options
1. How can Acme understand if its employees are using unsanctioned cloud applications
2. How can Acme benefit from all this information
Ted Hendriks
HP Atalla Pre-Sales Consultant, APJ Region
HP Enterprise Security Products

THANK YOU