The Secure Cloud Gateway
-- Where does it hurt?  
Exploring Cloud Application Security Problem

-- CASB / CSG Market Outlook

-- Cloud Application Security Needs

-- A look at the FireLayers Solution  
(XACML, Deployment, Policy)

-- Demo

-- Q&A
Challenges

**Concern**

#1 PRIVACY & SECURITY
Cloud APP Usage
- Security & privacy
- Performance
- Immaturity
- Regulatory compliance
- Integration
- Lock-in
- Costs
- Uptime
- Skills

**Barrier**

#1 COMPLIANCE & CONTROL
Cloud APP ADOPTION
- Loss of control
- Compliance implications
- Confidentiality & auditing
- Availability of data
- Performance unpredictability
- Data bottlenecks
- Data recovery
- Data location
- Licensing
- Viability of provider

**Issue**

#1 SECURITY
Mobile SERVICES USAGE
- Security
- Management of devices and applications
- Performance and reliability of applications
- Network reliability
- Employee resistance
- Lack of support
- Compliance
- Other
Who Takes Responsibility – You or the CSP?

<table>
<thead>
<tr>
<th>SERVICE PROVIDER</th>
<th>ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breach</td>
<td></td>
</tr>
<tr>
<td>Data Loss</td>
<td></td>
</tr>
<tr>
<td>Data Interception</td>
<td></td>
</tr>
<tr>
<td>Account Hijack</td>
<td></td>
</tr>
<tr>
<td>Insecure Interfaces</td>
<td></td>
</tr>
<tr>
<td>Insider Threats</td>
<td></td>
</tr>
<tr>
<td>Service Abuse</td>
<td></td>
</tr>
<tr>
<td>3rd Party Applications</td>
<td></td>
</tr>
<tr>
<td>Loss of Governance</td>
<td></td>
</tr>
</tbody>
</table>
## Threats & Your Responsibilities

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACCOUNT HIJACK</strong></td>
<td>User Management, Passwords/Authentication, Identity Fraud</td>
</tr>
<tr>
<td><strong>LACK OF VISIBILITY &amp; AUDITING</strong></td>
<td>User Activity Monitoring, Suspicious Events, SIEM Integration</td>
</tr>
<tr>
<td><strong>CLOUD NETWORK ACCESS CONTROL</strong></td>
<td>Device (BYOD), Browser/OS, Location &amp; Network</td>
</tr>
<tr>
<td><strong>INFORMATION DISCLOSURE</strong></td>
<td>Down/Upload via Insecure Devices, Public Sharing, 3rd Party Apps Leaks</td>
</tr>
<tr>
<td><strong>COMPLIANCE</strong></td>
<td>Insecure Storage (PII, PCI, PHI), Addressing exceptions (CUECS, SOX)</td>
</tr>
</tbody>
</table>
How To Mitigate Risk

• CASB will become essential to SaaS deployments
• Inject security policies into consumer-based cloud services
• Gain visibility
• Control user access to cloud resources

How You Benefit

• Adopt cloud-based services without compromising compliance and security policies
Cloud Application Security Market

Wake up and smell the hummus.

-- Robin Williams
CASB Market - As it Was

Data Security
- Vaultive
- Perspecsys
- CipherCloud

Threat Prevention
- FireLayers
- Imperva
- Adallom

Visibility
- Netskope
- Skyhigh
- Elastica

Compliance
- Bitglass
- CloudLock
CASB Market - What it is

- Data Security
  - Vaultive
  - Perspecsys
  - CipherCloud

- Visibility
  - netskope
  - skyhigh
  - elastica

- Compliance
  - bitglass
  - CloudLock

- Threat Prevention
  - FIRELAYERS
  - IMPERVA
  - ADALLOM
CASB Market – Where it is going

Data Security

Compliance & Visibility

Threat Prevention

New Generation CASB
Cloud Application Security Needs

*Intellectuals solve problems, geniuses prevent them.*

— Albert Einstein
Cloud Application Security Gateway

Corporate Network

Mobile Workforce

Cloud Provider

Session Tunneling

Real-time Enforcement

Reverse Proxy
Forward Proxy
API

XACML-Based Policy

IAM
ANTI-X
DLP
Encryption
IDS/IPS
MDM

Corp. Device
BYOD
Mobile App
Public Device

Corp. Device
Public Device
Why Choose A Native Gateway

Native Gateway
• Multiple integration options
• Full stack capabilities: network → host → app
• Top performance
• Support any cloud app
• Real-time enforcement
• Proprietary cloud app gateway technologies

Proxy Server with customization
• Limited pre-defined capabilities
• Deep customization required
• Performance Issues

Application API
• Limited to App functionality
• Few apps have APIs
• Dependent on SaaS provider upgrades
• No or limited real-time enforcement
• Additional SaaS Fees
• New development per API
End-2-End Deployment Flow
DEMO & Q&A