Your Time Is Now
Effective Cloud Security Made Simple: Cloud Security Re-imagined with CloudLock

Yoni Fine, Consulting Systems Engineer
BRKSEC-2404
By 2020, 92 percent of global data center traffic will come from the cloud.

Cisco® Global Cloud Index (GCI)
Agenda

• Intro
• Cloud Security Challenges
• What is CloudLock’s API First Approach
• Use Cases
• Architecture, Install & Configure
• Orchestration – FirePOWER, Umbrella, SIEM
• Demo - API’s for your Homegrown Apps
• Conclusion
Our Challenges

- Malware and ransomware
- Gaps in visibility and coverage
- Compromised accounts and malicious insiders
- Data breaches and compliance
By 2018, Gartner estimates:

25% of corporate data traffic will bypass perimeter security.
The very nature of network traffic has changed

Content created in the cloud

Cloud-to-cloud traffic
Security challenges have evolved

IaaS

SaaS

Users

Data

Apps

PaaS

HQ

Roaming user

Branch

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Organizations need to extend their security controls to public cloud environments.
Which means cloud security is a shared responsibility

- **On-Premises**
  - User
  - Data
  - App
  - Compute
  - Network

- **SaaS**
  - User
  - Data
  - App
  - Compute
  - Network

- **IaaS/PaaS**
  - User
  - Data
  - App*
  - Compute
  - Network

*AWS Marketplace & custom app security

<table>
<thead>
<tr>
<th>Your responsibility</th>
<th>Their responsibility</th>
<th>Often neglected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Green</td>
<td>Red</td>
</tr>
</tbody>
</table>
A CASB is a cloud security solution

cloud access security broker, or CASB (caz-bee)

noun

Definition: a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure or utilizes APIs to secure the cloud.

• Addresses gaps in security resulting from the significant increases in cloud service and mobile usage.

• Delivers capabilities that are generally unavailable today in security controls such as web application firewalls (WAFs), secure web gateways (SWG) and enterprise firewalls.

*http://searchcloudsecurity.techtarget.com/definition/cloud-access-security-brokers-CABS
Because native security built into cloud apps is not sufficient

1. Single Platform Only
2. Solves Fewer Problems
3. Lack of Security Expertise & Focus
4. Upcharge
5. No Incident Management
6. Weak Remediation Capabilities
Approaches to CASB
There are three primary methods for securing cloud app traffic

- Reverse proxy
- Forward proxy
- API
Many use a proxy, either reverse or forward

But proxies and Gateways have challenges

The Proxy itself is a clear attack vector

Challenges

- Ensuring that users can’t bypass the proxy
- Requiring VPN access if the proxy is on-premise
- Adapting the proxy to changes with the SaaS app
- Inability to see cloud-to-cloud traffic
- Inability to see data at rest
- Lack of coverage for native apps
There’s a better and easier way
Cisco Cloudlock adds to the Cisco security portfolio

Cisco Cloudlock


- **Extends typical enterprise security functions** including, compliance, audit response and governance, to public cloud platforms.

- **Connects using an API** to secure commonly used apps like G Suite, Salesforce, Box, Dropbox and more.
Cisco Cloudlock is 100% API that connects directly to the application

Unlike proxy-based CASBs, API-based CASBs

- Analyze data already in the cloud (retroactive security analysis)
- Analyze cloud-to-cloud traffic
- Protect cloud usage from unmanaged users and users with mobile devices
- Do not break functionality or impact the user experience
Cloudlock Platform

CASB for SaaS

Protect the usage of business apps in the cloud

- Salesforce
- Dropbox
- servicenow
- Google Apps
- slack
- Office 365
- Box

CASB for IaaS/PaaS

Protect the usage of critical workloads in the cloud

- Salesforce
- Amazon Web Services

CASB Orchestrations

Include the cloud in security workflows

- Splunk
- IBM Security
- VMware airwatch
- Check Point
- Okta
- OneLogin
- FireEye

Cloud Security Fabric™

- User Behavior Analytics
- Apps Firewall
- DLP
- Encryption Management
- Configuration Security
- Central Auditing
CASB Use Cases
Cisco Cloudlock addresses the most critical cloud security use cases

Discover and Control:
- Compromised Accounts
- Insider Threats
- User and Entity Behavior Analytics

Discover and Control:
- Data Exposures & Leaksages
- Privacy & Compliance Violations
- Cloud Data Loss Prevention (DLP)

Discover and Control:
- Cloud Malware
- Shadow IT/OAuth Discovery & Control
- Apps Firewall
Architecture, Install and Configure
Cisco Cloudlock’s architecture is 100% cloud-native

Hosted by Cisco Cloudlock on AWS

Comprised of security microservices

Subscription-based

Multi-tenant
Cisco Cloudlock connects without impacting the environment

ZERO Network dependency on monitoring public cloud applications
And connects entirely through a Public API
Cisco Cloudlock – How it works?
Cisco Cloudlock – How it works

CloudLock Cloud Security Fabric
- Content Classification
- Apps Firewall
- Security Analytics
- Encryption Management
- Incident Management
- Central Auditing
- Policy Automation
- User Behavior Analytics
- Configuration Security

PaaS and IaaS
- force.com
- Amazon Web Services

SaaS
- salesforce
- Google Apps
- Dropbox
- ServiceNow
- Box
- Office 365

IDaaS
- okta
- OneLogin

All End - Users
Cisco Cloudlock – How it works

CloudLock Cloud Security Fabric

- Content Classification
- Apps Firewall
- Security Analytics
- Encryption Management
- Incident Management
- Central Auditing
- Policy Automation
- User Behavior Analytics
- Configuration Security

Homegrown Apps
- IT Apps
- ISV Cloud Apps
- Any App

Enterprise
- splunk
- IBM
- HP ArcSight
- serviceNow
- tableau

PaaS and IaaS
- force.com
- Amazon Web Services

SaaS
- Salesforce
- Google Apps
- Dropbox
- ServiceNow
- box
- Office 365

IDaaS
- okta
- OneLogin

All End - Users
Sample Installation
Cloudlock for O365 Installation
Product Demo
Orchestration – NGFW - FirePOWER
Ingest 20MB Log File from Cisco FirePOWER and ASA Series Firewalls to Produce Report

Enrich Log Data with CloudLock Security Intelligence on Over 235,000 Cloud Apps

Leverage the CloudLock Community Trust Rating™ for Efficient Risk Analysis

Launched 8 days after acquisition
Shadow IT App Discovery Report – Export FirePOWER Log

- Select Time Range
- Select Format > Table View
- Select the Maximum Results limit (20MB or less)
- Edit Fields Web Category, Initiator User and Traffic (KB).
- Generate Report (Archived Zip) to be uploaded to Cloudlock
Shadow IT App Discovery Report – Powered by Cisco NGFWs

Top 10 Risky Apps

<table>
<thead>
<tr>
<th>App</th>
<th>Risk</th>
<th>Credential Exposure Risk</th>
<th>Access Scope</th>
<th>Users</th>
<th>Requests</th>
<th>Traffic (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hola Anonymizer</td>
<td>High</td>
<td>High</td>
<td>read basic info</td>
<td>10</td>
<td>22</td>
<td>4.3 MB</td>
</tr>
<tr>
<td>Utorrent P2P File Sharing</td>
<td>High</td>
<td>High</td>
<td></td>
<td>6</td>
<td>14</td>
<td>234.5 KB</td>
</tr>
<tr>
<td>Windows Live Hotmail Email</td>
<td>High</td>
<td>High</td>
<td></td>
<td>4</td>
<td>4</td>
<td>58.2 KB</td>
</tr>
<tr>
<td>Docstoc Web Content Aggregator</td>
<td>High</td>
<td>High</td>
<td></td>
<td>4</td>
<td>4</td>
<td>1.2 MB</td>
</tr>
<tr>
<td>Imesh P2P File Sharing</td>
<td>High</td>
<td>High</td>
<td></td>
<td>3</td>
<td>6</td>
<td>555.8 KB</td>
</tr>
<tr>
<td>BitTorrent Sync P2P File Sharing</td>
<td>High</td>
<td>High</td>
<td></td>
<td>2</td>
<td>7</td>
<td>135.3 KB</td>
</tr>
<tr>
<td>Xunlei P2P File Sharing</td>
<td>High</td>
<td>High</td>
<td></td>
<td>2</td>
<td>3</td>
<td>5.2 KB</td>
</tr>
<tr>
<td>Foxit Reader Business Applications</td>
<td>High</td>
<td>High</td>
<td>read basic info</td>
<td>1</td>
<td>1</td>
<td>949.0 B</td>
</tr>
<tr>
<td>Unknown</td>
<td>High</td>
<td>High</td>
<td>access full data</td>
<td>0</td>
<td>0</td>
<td>0.0</td>
</tr>
<tr>
<td>Facebook Social Networking</td>
<td>Medium</td>
<td>High</td>
<td>access contacts</td>
<td>873</td>
<td>4452</td>
<td>24.2 GB</td>
</tr>
</tbody>
</table>

Generate a new third-party report

Select the third-party vendor that provided the log file.

Cisco FirePOWER

To generate a report, import a FirePOWER eStreamer csv log file.

Browse for a log file

Most Risky Apps Summary

Your environment has 9 very high risk apps and 9 high risk apps out of a total of 224 apps.

<table>
<thead>
<tr>
<th>Apps</th>
<th>Risk</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hola</td>
<td>High</td>
<td>10 users</td>
</tr>
<tr>
<td>Utorrent</td>
<td>High</td>
<td>6 users</td>
</tr>
<tr>
<td>Windows Live Hotmail Email</td>
<td>High</td>
<td>4 users</td>
</tr>
<tr>
<td>Docstoc</td>
<td>High</td>
<td>4 users</td>
</tr>
<tr>
<td>Imesh</td>
<td>High</td>
<td>3 users</td>
</tr>
</tbody>
</table>
Orchestration – Cisco Umbrella (Formerly OpenDNS)
Block Shadow IT Apps Banned with Umbrella

Cisco Umbrella integration enables teams to **block** shadow IT app **access** at the DNS level through Cloudlock.
Cloudlock & Cisco Umbrella Integration - 100% API

• Select **Settings>Integrations>Cloudlock**
• Copy the Cisco Umbrella **URL** provided (Paste into corresponding field in Cloudlock dashboard.)
Block Shadow IT Apps Banned with Umbrella
Orchestration - SIEM
SIEM Usage: An Example

Find incidents via Cloudlock

Updates in Cloudlock Dashboard

Integrate in SIEM tool via API calls

Resolve/Update incidents in SIEM tool

Investigate within SIEM tool
Cisco Cloudlock Splunk App – Available in Splunkbase

Splunk certified App is available to download for free in the splunkbase

Download here - https://splunkbase.splunk.com/app/3043/
Splunk In Action - Cloudlock Dashboard View
IBM QRadar In Action
HP ArcSight Logger In Action
Demo – Dev APIs for your Homegrown Apps
CloudLock CyberDev Platform Options

- Custom Apps
  - Homegrown
  - IT SaaS Apps
  - ISV Cloud Apps

CloudLock CyberDev APIs
- RESTful APIs
- Benefit: Flexibility!

CloudLock CyberDev for IaaS and PaaS Apps
- Codeless Security
  - Benefit: Speed & Automation

CloudLock Cloud Security Fabric
- Compromised Accounts
- Cloud Malware
- Data Breaches
- Compliance
- SecOps & Forensics
Use Case 1
Content Classification Dev API
CloudLock DevAPI’s IM Example: Content Classification

**Application:** Internal Chat App  
**Need:** PII Compliance (No SSN's or ID Nos)  
**Solution:** Cloudlock CCS DevAPI

Hi, Can you please send me Jane’s benefit package? Her social is: 5179811234

Hi, Can you please send me Jane’s benefit package? Her social is: xxxxx1234

Sure! On it’s way

SSN Redacted
Use Case 2
Velocity Detection Dev API
### CloudLock DevAPI’s VPN Log Example: Velocity (UEBA)

<table>
<thead>
<tr>
<th>Application: VPN</th>
<th>Need: Identify employee account is compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solution:</strong> Cloudlock Velocity DevAPI</td>
<td></td>
</tr>
</tbody>
</table>

**Dan.R: Real Employee**

- Login

**Dan.R: Impersonator**

- Login

---

VPN Server

- 2015-11-19T09:00:00, Dan.R, Login, Src: 54.92.67.234

- Violation
  - "distance": 5695.0, "velocity": 6730.0

- Require MFA
Use Case 3
Cloud Migration and Sync Dev API
CloudLock DevAPIs: Cloud Migration & Sync

**Application:** Cloud Migration  
**Need:** Identify and stop files that have sensitive data from being uploaded

**Solution:** Cloudlock CCS DevAPI

1. Look for sensitive data  
2. Only if clear - upload to cloud
CloudLock DevAPIs: Cloud Migration: In Action

All files in the ‘123’ folder are scheduled for upload to Dropbox for Business as part of a cloud migration.

**Use Case:** 3 files: CRM_001, CRM_002 and CRM_003.

1. **CRM_001**
   - 5 credit card numbers:
     - 4539-3428-5183-0420
     - 4929-2282-3733-9301
     - 4929-0752-6208-0965
     - 4916-0461-9386-7239
     - 4556-5491-4543-8277

2. **CRM_002**
   - No credit card numbers:

3. **CRM_003**
   - 1 credit card number:
     - I look like an ordinary file but someone copied this strange looking number: 4539-3428-5183-0420. I wonder what it could be...
CloudLock DevAPIs: Cloud Migration: Demo

- Dropbox folder name: 123
- Local directory: /home/ubuntu/123
- Total elapsed time for list_folder: 0.537

Descending into ...

Upload CRM_003.rtf? [auto] Y
Calling CloudLock CCS Dev API
Found 1 Violations, examples:

an ordinary file but someone copied this strange looking number: XXXX-XXXX-XXXX-0420. I wonder what it could be...

File /home/ubuntu/123/CRM_003.rtf violates corporate PCI policy and will not be uploaded

Upload CRM_002.rtf? [auto] Y
Calling CloudLock CCS Dev API
File is clear to upload
Total elapsed time for upload 729 bytes: 1.160

uploaded as CRM_002.rtf
Upload CRM_001.rtf? [auto] Y
Calling CloudLock CCS Dev API
Found 5 Violations, examples:
XXXX-XXXX-XXXX-0420
XXXX-XXXX-XXXX-9301
XXXX-XXXX-XXXX-0965
XXXX-XXXX-XXXX-7239
XXXX-XXXX-XXXX-8277

File /home/ubuntu/123/CRM_001.rtf violates corporate PCI policy and will not be uploaded

ubuntu@api-integration-01:/opt/cl2splunk$
Conclusion

1 2 3

Simple

Uses the API approach which adds no complexity

Open

Orchestrates security across cloud security platforms

Automated

Enables admins to automate routine decisions and remediation

Cisco Cloudlock aligns to this perfectly
For more information: visit www.cloudlock.com/

Request a Demo or Security Assessment

CASB Buyers Guide
https://www.cloudlock.com/blog/casb-buyers-guide/
Continue Your Cisco Live Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Lunch & Learn
• Meet the Engineer 1:1 meetings
• Related sessions
Call to Action

• Attend the following related sessions
• Extending Your Security Perimeter to Public Cloud - PSOSEC-1903
• Cloud Education Zone & Security Booth Theatre – Cloudlock & Cisco Umbrella
• Visit the World of Solutions for
  • Cisco Campus
  • Walk in Labs
  • Technical Solution Clinics
• Meet the Engineer (Available Feb 18 and Feb 19)
• Lunch and Learn Topics
• DevNet zone related sessions -
Complete Your Online Session Evaluation

• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
The tipping point from the network perimeter to the cloud.
Thank You

yonifine@cisco.com
Appendix
### Splunk In Action - Incident View

#### CloudLock Incident Management

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Severity</th>
<th>Matches</th>
<th>Policy</th>
<th>updated_at</th>
<th>Status</th>
<th>Name</th>
<th>Type</th>
<th>Owner</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>salesforce</td>
<td>ALERT</td>
<td>1</td>
<td>New Unclassified App installs</td>
<td>03/02/16 12:01:46-0500</td>
<td>IN PROGRESS</td>
<td>Conga, Composer, Offline</td>
<td>null</td>
<td>Eric Chaves</td>
<td>Update</td>
</tr>
<tr>
<td>salesforce</td>
<td>ALERT</td>
<td>1</td>
<td>New Unclassified App installs</td>
<td>03/02/16 12:01:46-0500</td>
<td>RESOLVED</td>
<td>Conga, Composer, SFI</td>
<td>null</td>
<td>Eric Chaves</td>
<td>Update</td>
</tr>
<tr>
<td>salesforce</td>
<td>ALERT</td>
<td>1</td>
<td>New Unclassified App installs</td>
<td>03/02/16 12:01:46-0500</td>
<td>RESOLVED</td>
<td>Conga, Composer</td>
<td>null</td>
<td>Eric Chaves</td>
<td>Update</td>
</tr>
<tr>
<td>google</td>
<td>WARNING</td>
<td>1</td>
<td>Risky Access Scopes</td>
<td>03/02/16 12:01:45-0500</td>
<td>RESOLVED</td>
<td>Ganster for Google Drive</td>
<td>null</td>
<td>Jane Morrissey</td>
<td>Update</td>
</tr>
<tr>
<td>google</td>
<td>WARNING</td>
<td>1</td>
<td>Risky Access Scopes</td>
<td>03/02/16 12:01:45-0500</td>
<td>NEW</td>
<td>Cotap</td>
<td>null</td>
<td>Joseph Blanchard</td>
<td>Update</td>
</tr>
<tr>
<td>google</td>
<td>CRITICAL</td>
<td>1</td>
<td>Manually Banned Apps</td>
<td>03/02/16 12:01:45-0500</td>
<td>NEW</td>
<td>Cartwheel by Target</td>
<td>null</td>
<td>Chris Thompson</td>
<td>Update</td>
</tr>
<tr>
<td>google</td>
<td>CRITICAL</td>
<td>1</td>
<td>Manually Banned Apps</td>
<td>03/02/16 12:01:45-0500</td>
<td>NEW</td>
<td>Google APs Explorer</td>
<td>null</td>
<td>Ori Keren</td>
<td>Update</td>
</tr>
<tr>
<td>google</td>
<td>CRITICAL</td>
<td>1</td>
<td>Manually Banned Apps</td>
<td>03/02/16 12:01:45-0500</td>
<td>NEW</td>
<td>Doodle</td>
<td>null</td>
<td>Joseph Blanchard</td>
<td>Update</td>
</tr>
</tbody>
</table>
Splunk In Action - Incident Forensics View
Cloudlock API View – Suspicious User Behaviour

User Login
Username
Origin – SSO Provider
Cloudlock Policy
Browser
OS Version
Cloudlock API View – Geo-location

```
{
    "event_id": "66:okta:okta:teyS04eb7dmt42qo",
    "client_ip": "64.104.125.232",
    "event_type": "user login",
    "name": "User login",
    "created_at": "2017-02-06T21:22:26+00:00",
    "client_location": {
        "lat": 31.0456,
        "lng": 121.3997,
        "country": {
            "code": "CN",
            "name": "China"
        },
        "region": {
            "code": "31",
            "name": "Shanghai"
        },
        "city": "Shanghai"
    }
}
```
Cloudlock API View – DLP – Publicly Shared Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>File Owner</th>
<th>SaaS Application</th>
<th>Policy Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;id&quot;: &quot;0d2y1eddax&quot;, &quot;name&quot;: &quot;Logins for EC2 Instances.xlsx&quot;, &quot;mime_type&quot;: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet&quot;, &quot;owner_name&quot;: &quot;Jimmy Jones&quot;, &quot;origin_id&quot;: 132509136328, &quot;origin_type&quot;: &quot;document&quot;, &quot;direct_url&quot;: &quot;<a href="https://box.com/master/content/993638687/0/0/132509136328">https://box.com/master/content/993638687/0/0/132509136328</a>&quot;, &quot;vendor&quot;: { &quot;name&quot;: &quot;box&quot; }</td>
<td>&quot;policy&quot;: { &quot;name&quot;: &quot;Publicly Shared files&quot;, &quot;id&quot;: null</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public
Cloudlock API View – DLP – PCI Compliance

File Owner

SaaS Application

Policy Violation

Redacted CCN Excerpt
Cloudlock API View – Shadow IT – Connected Apps

Application Name
User
Sanctioned Application
Cloudlock Policy
Cloudlock API View – Shadow IT – Connected Apps

- **Install Type**: "user"
- **Client Type**: null
- **Is Revocable**: true
- **Risk Level**: 4
- **Scope Categories**: ["BEHAF", "BINFO", "FDATA", "INBOX", "UACTV"]
- **Classification**: {
  "reason_id": 7,
  "reason": "Excessive access scopes",
  "updated_at": "2017-02-07T16:24:11.391224+00:00",
  "method": "auto",
  "type": "banned",
  "other_reason": null
}
- **Detected At**: "2017-02-07T16:19:20.661182+00:00",
- **Users Count**: 0

- **Category**: {
  "id": "INBOX",
  "title": "Access inbox or contacts information"
}
- **ID**: "AGM46QZ30b"
- **Description**: "Access directory as the signed in user"
- **Friendly Name**: "(Microsoft Graph) Access directory as the signed in user"
- **URL**: "MicrosoftGraph.openid"

- **Category**: {
  "id": "BEHAF",
  "title": "Act on behalf of a user"
}
- **ID**: "ZRBzXSM32Y"
- **Description**: "Allows the app to edit or delete current signed-in user's files"
- **Friendly Name**: "(Microsoft Graph) Edit or delete user files"
- **URL**: "MicrosoftGraph.Files.ReadWrite"

- **Category**: {
  "id": "FDATA",
  "title": "Full Data Access"}
Your Time Is Now