Integrated Enterprise Inline and Out-of-Band CASB

Pooja Deshmukh, Sr. Product Manager, Zscaler
Four key areas of CASB

Policy Enforcement
Visibility
Data Security
DLP
"Shadow IT"
Unapproved
Sensitive Data
Encryption
Threat Prevention
Anti-malware
Cloud applications
Access governance
Threat Intelligence
SWG Integration
Adaptive access control

Data Security
DLP
Sensitive Data
Encryption
Threat Prevention
Anti-malware

Reporting
Auditing
Risk Management
Data Security
DLP
Sensitive Data
Policy Enforcement
Compliance
Encryption

User Entity Behavior
Analysis
Policy Enforcement
Reporting
Auditing
Risk Management

Inline & API

Data & Users
Where is your data today?

Data has moved to the cloud
- Office 365
- Cloud data sharing applications
- Public cloud

How do users access it?
- From within and outside the traditional perimeter
- Direct access cloud-to-cloud
- Collaboration
Who is responsible for securing your data?

- Users
- Data Owners
- Organizations
- Security solutions
- Hosting service provider
CASB focus areas

Gartner  4 pillars of CASB

- Visibility
- Data protection
- Threat prevention
- Compliance
- User experience
CASB architecture
What’s the best option for you?

<table>
<thead>
<tr>
<th>Inline</th>
<th>Forward proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reverse proxy</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td></td>
</tr>
<tr>
<td>Out-of-band</td>
<td>API</td>
</tr>
<tr>
<td>Logs</td>
<td></td>
</tr>
</tbody>
</table>
CASB vendors partner with Zscaler

1. Traffic forwarding
2. App discovery
3. App classification
4. List unsanctioned applications
5. Unsanctioned cloud app policy
6. Access to apps blocked inline

Inline inspection is necessary for CASBs!
How do these integrations add value?

- Centralized policy
- Better security
- Better user experience
- Reduced complexity & cost
- Improved staff productivity
Industry analysts agree

Reduce complexity now on the network security side by moving to ideally one vendor for secure web gateway (SWG), cloud access security broker (CASB), DNS, zero trust network access (ZTNA), and remote browser isolation capabilities.

Gartner, Inc.: The Future of Network Security Is in the Cloud, August 2019
Zscaler Internet Access Today

Platform Services

Access Control
- Cloud Firewall
- URL Filtering
- Bandwidth Control
- DNS Resolution

Threat Prevention
- Cloud Sandbox
- DNS Security
- Native SSL
- Advance Threat Prevention

Data Protection
- Cloud DLP
- Exact Data Match
- CASB
- File Type Controls

Sanctioned

Unsanctioned
The Zscaler platform is your integrated Inline CASB

<table>
<thead>
<tr>
<th>Inline controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visibility</strong></td>
</tr>
<tr>
<td>App Classification</td>
</tr>
<tr>
<td>Risk Scores</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data Protection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud DLP</td>
</tr>
<tr>
<td>Exact Data Match</td>
</tr>
<tr>
<td>Multi-criteria Policy</td>
</tr>
<tr>
<td>File Type Controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Threat Prevention</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Native SSL</td>
</tr>
<tr>
<td>Cloud Firewall</td>
</tr>
<tr>
<td>Cloud Sandbox</td>
</tr>
<tr>
<td>Advanced Threat Prevention</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Compliance</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only Controls</td>
</tr>
<tr>
<td>Domain Restrictions</td>
</tr>
<tr>
<td>Identity Broker</td>
</tr>
<tr>
<td>Device Posture (Z App)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>User Experience</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth Control</td>
</tr>
<tr>
<td>Service Edge</td>
</tr>
<tr>
<td>Peering with Content Providers</td>
</tr>
</tbody>
</table>

What about my data at rest?
Zscaler extends CASB functionality with APIs

**Inline use cases**
- Visibility
- Data Protection
- Threat Prevention
- Access Control
- App risk scoring

**Out-of-band use cases**
- Discover Sensitive Data
- Discover Threats
- Remediate Risks
- Collaboration Controls
- Reporting

API

SharePoint, box, OneDrive
What’s New?
Tenant onboarding

Add Cloud App Tenant

Last modified at 12:02 PM, August 1, 2019 by admin@zenithlive.org.com

1. Choose Cloud App Provider for Authorization
   - OneDrive
   - SharePoint
   - box

2. Name the Cloud App Tenant

3. Authorize Cloud App Permission
Tenant onboarding

Add Cloud App Tenant

Last modified at 12:02 PM, August 1, 2019 by admin@zenithliveorg.com

Choose Cloud App Provider for Authorization

- box

Name the Cloud App Tenant

Enter Tenant Name
San Jose-HQ-Box

The Tenant Name must be unique.

Authorize Cloud App Permission

To give Zscaler the permission to Box, add the ID below to the authorized app list in Box setting. How to enable application in Box?

Zscaler Application ID

Kiewht29Avhuahda4f1vbf

Copy  Go to Box setting
Name the Cloud App Tenant

Enter Tenant Name
San Jose-HQ-Box
The Tenant Name must be unique.

Authorize Cloud App Permission

To give Zscaler the permission to Box, add the ID below to the authorized app list in Box setting. How to enable application in Box?

Zscaler Application ID
Kiewht294whuhaad7vbf
Copy
Go to Box setting

Enter Box Enterprise ID

Copy the Box Enterprise ID and paste here, which will be used to identify this unique Tenant. Where can I find the Box Enterprise ID?

Box Enterprise ID
myEnterpriseID

Save  Cancel
## Policy-driven controls

### Data Loss Prevention

Configure CASB Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match. Cloud app control policies take priority over URL policy. Default policy which is not visible is to allow all.

<table>
<thead>
<tr>
<th>Rule Order</th>
<th>Rule Name</th>
<th>Severity</th>
<th>Criteria</th>
<th>Action</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Intellectual Property</td>
<td>High</td>
<td>CLOUD APP TENANT</td>
<td>Revoke External Sharing</td>
<td>Restrict IP from being shared externally.</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ZBC-Corporate-OneDrive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GROUP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Engineering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DEPARTMENT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Engineering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DLP ENGINE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Source Code, Patents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>COLLABORATION SCOPE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>External</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>PII</td>
<td>Medium</td>
<td>DLP ENGINE</td>
<td>Revoke Sharing</td>
<td>Do not share employee PII information internally or externally.</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Employee-PII</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Discover sensitive data

CASB Report

Report generated: 9:12 AM, September 18, 2019

ALL INCIDENTS

547
9193 files scanned

APPLICATIONS GENERATING THE INCIDENTS

box
316
Last scanned: 9:12 AM, September 18, 2019

OneDrive
173
Last scanned: 9:12 AM, September 18, 2019

SharePoint
58
Last scanned: 9:12 AM, September 18, 2019

INCIDENTS BY POLICY TYPE

472
DLP

75
Malware

Incident Trend over the Last 30 Days

06/04/2019
All Incidents: 65
DLP Incidents: 46
Malware Incidents: 21
Discover threats

What is the Distribution of Incidents within Policy Types?

**Sensitive Data**
- Customer List: 246
- Source Code: 98
- PCI: 72
- PII: 53
- Others: 3
  - Total Incidents: 472

**Malware**
- Virus: 36
- Spyware: 19
- Trojans: 10
- Adware: 5
- Others: 5
  - Total Incidents: 75

**Departments with Most Incidents**

- Finance: 98
- Human Resource: 89
- Marketing: 72
- Sales: 55

**Users with Most Incidents**

- user@samplecompany.com: 98
- admin@samplecompany.com: 89
- client@samplecompany.com: 72
- user@samplecompany.com: 55
<table>
<thead>
<tr>
<th>Application</th>
<th>Category</th>
<th>Threat Index</th>
<th>Upload</th>
<th>Download</th>
<th>Recommended Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileDropper</td>
<td>File Sharing</td>
<td>2</td>
<td>112MB</td>
<td>209MB</td>
<td>Caution</td>
</tr>
<tr>
<td>Tumblr</td>
<td>Social Networking &amp; Blogging</td>
<td>8</td>
<td>129MB</td>
<td>342MB</td>
<td>Block</td>
</tr>
<tr>
<td>Coupons</td>
<td>Consumer</td>
<td>15</td>
<td>383MB</td>
<td>108MB</td>
<td>Caution</td>
</tr>
<tr>
<td>Groupon</td>
<td>Consumer</td>
<td>3</td>
<td>176MB</td>
<td>245MB</td>
<td>Block</td>
</tr>
<tr>
<td>PDF Converter</td>
<td>File Sharing</td>
<td>2</td>
<td>263MB</td>
<td>365MB</td>
<td>Block</td>
</tr>
<tr>
<td>Pinterest</td>
<td>Social Networking &amp; Blogging</td>
<td>8</td>
<td>402MB</td>
<td>225MB</td>
<td>Caution</td>
</tr>
</tbody>
</table>
Focused incident triage and automated remediation
## Control over historic data scans

### CASB

#### Data Loss Prevention

<table>
<thead>
<tr>
<th>Tenant</th>
<th>Scheduling</th>
<th>Description</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZBC-Corporate-Boxshare</td>
<td>POLICY</td>
<td>Discover sensitive data from older repositories</td>
<td>Running</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Loss Prevention</td>
<td></td>
<td>Last scan: 9/17/2019</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DATA TO BE SCANNED</td>
<td></td>
<td>4:30 PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Generated &amp; Modified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Starting on Jan 01, 2018</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZBC-Corporate-OneDrive</td>
<td>POLICY</td>
<td></td>
<td>Running</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Loss Prevention</td>
<td></td>
<td>Last scan: 9/17/2019</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DATA TO BE SCANNED</td>
<td></td>
<td>8:42 PM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Generated &amp; Modified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Starting on Dec 05, 2017</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com
Thank You