The Evolution of CASB

Now is the Time to Rock the CASB
Executive Summary
As the enterprise continues to adopt cloud services, the evolution of the Cloud Access Security Broker (CASB), also known as Cloud Security Gateway, has undergone a mirrored transition. Over the past five years, CASB offerings have matured through a steady stream of feature introductions, a widening number of use cases, and recently a spate of mergers and acquisitions. Unfortunately, this has created a myriad of misconceptions about what a CASB is, what value a CASB can deliver, and what CASB will become.

Report Scope
This report examines the evolution of the CASB space from its inception through the development of today’s table stake features, a set of predictions of how CASB will evolve in the foreseeable future, and a set of recommendations. This report also compares a selection of today’s CASB offerings against the most relevant and common features demanded by enterprises.

Research Method
This Trace3 Research trend report’s scope was based on research requests received from Trace3 customers and field engineers. From these requests, relevant areas of the technical landscape were mapped out, including the identification of affected 360 View use cases and the primary players in these use cases. From these use cases, mandatory and desirable feature sets were defined and key vendors were then given the opportunity to present, describe and demonstrate their current product offerings. After detailed analysis, comparison matrices were compiled and refined and predictions and recommendations drawn.
The Evolution of CASB

Now is the Time to Rock the CASB

Analysis

Did You Know...

- By 2020, 85% of large enterprises will use a CASB solution for their cloud services, up from less than 5% today. [1]
- $500 million in total VC funding has gone into the CASB market. [1]
- Out of the 14 CASB startups founded since 2011, eight have been acquired. [1]
- By 2018, 58% of all cloud workloads will be SaaS. [2]
- By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources. [3]
- The CASB market is one of the hottest growing areas in cloud security, expected to reach $7.51 billion by 2020, which is up from $3.34 billion in 2015. [4]
- The CASB market is expected to advance at a CAGR of 16.7% from 2016 to 2024, resulting in a market size of $13.2B in 2024. [5]
- 41% of respondents had heard of CASB, however only 21% reported using the technology. [6]

CASB Explained

A CASB is a software tool or service that sits between an organization’s on-premise infrastructure and a cloud provider’s infrastructure. A CASB acts as gatekeeper, allowing the organization to extend the reach of their security policies beyond their own infrastructure.

CASB solutions allow enterprises to extend their security policies to Software as a Service (SaaS) applications such as Office 365, Dropbox, and SalesForce, as well as Infrastructure as a Service (IaaS) platforms such as AWS, Azure, or GCP. In short, CASB helps companies ensure corporate data is secured end-to-end, from cloud to device and vice-versa, regardless if the device is managed or unmanaged, where it is located, or who is using it.

The CASB market can be divided into two offerings: Pure Play and Platform solutions. This is an important factor to consider when approaching the market as the Platform solutions provide a rich set of features when using the entire product suite, whereas Pure Play vendors offer a full featured CASB without relying on underlying products to support their offering. Unfortunately, some solutions marketed as CASB only deliver a subset of the table stake features established CASB solutions deliver, creating confusion in the market. As such, this study has defined the four required capabilities a CASB must deliver:

- Visibility - A CASB must provide enterprises with visibility into users, services, data, and devices, allowing different business units to view cloud applications with the same visibility as if hosted on-premise.

- Compliance - A CASB must provide file content monitoring to find and report on regulated data residing or moving into or out of the cloud. This allows the enterprise to impose controls on cloud usage and ensure compliance with specific industry regulations.

- Data Security - A CASB must provide data protection including encryption. By using data classification and User and Entity Behavior Analytics (UEBA), CASB solutions enforce security policies and monitor sensitive data access and usage across all user devices and locations.

- Threat Protection - A CASB must analyze traffic patterns to identify compromised accounts and malicious usage to prevent unauthorized devices or suspicious users from accessing critical data and/or cloud services.

© 2017 Trace3, Inc. All Rights Reserved
As enterprise data is dispersed into the cloud, it becomes difficult to ascertain where data is stored and whether it is secure and compliant. To combat this, CASB solutions provide both shadow and sanctioned IT discovery, present a consolidated view of an organization's cloud service usage, and can identify users who access data from any device or location. Leading CASB solutions take this a step further by embedding a cloud service security posture assessment database, which provides visibility into the "trustability" of the cloud service provider. CASB vendors also give enterprises visibility into authorized and unauthorized cloud usage and can intercept and monitor data traffic between the corporate network and cloud platform.

CASB solutions can monitor and control user cloud activities from a mobile, desktop, or sync client. A CASB can also monitor and control access to cloud services, privileged accounts, and unauthorized cloud activity in real time.

There are two primary methods for integrating CASB into enterprises to control cloud access and apply corporate security policies, namely as a forward or reverse proxy or via a cloud provider's API. More CASB solutions are becoming "mixed mode" or "multi-mode," using both proxy and API techniques to leverage the benefits of both methods. By way of comparison, each technique presents a unique set of pros and cons:

- **Forward proxy can be used for all types of cloud applications by forcing all data to pass through the proxy. However, using a forward proxy requires the user to install self-signed certificates on every device that accesses the proxy, which can be difficult to deploy in a distributed environment or in one with a large number of employee-owned mobile devices.**
- **A reverse proxy system is easier to deploy because it is accessible from any device, anywhere, without the need for special configuration or certificate installation. The drawback is a reverse proxy can not work with client-server type applications that have hard-coded hostnames.**
- **Like reverse proxy solutions, API-based systems are also easy to deploy. However, the range of cloud applications they can fully integrate with is more limited since not all cloud applications provide API support.**

Today's leading CASB solutions provide five key Visibility features:

- **Forward and Reverse Proxy Support - provides proxy support for both reverse and forward methods.**
- **API Support - provides API support to various SaaS applications (e.g., Office365, Salesforce, Box).**
- **Agent Dependent - requires an endpoint agent in order to achieve optimal protection.**
- **Consolidated Dashboard Views - provides a consolidated dashboard view of data, device, user, application, and administrative activities.**
- **Segregates Corporate Data from Personal Data - provides visibility of corporate data and assets while giving no visibility into personal data.**
Compliance
Compliance is a critical business concern and today's burgeoning adoption of cloud services presents one of the fastest growing challenges enterprise IT compliance teams face. CASB solutions help ensure compliance in the cloud to a variety of regulation regimes such as HIPAA or HITECH (for health-care organizations), PCI compliance (for retail companies), and FFIEC and FINRA (for financial related organizations).

Cloud service providers have dedicated staff and resources to protect data from theft, loss, and corruption since their business depends on delivering and maintaining the trust of customers. Today's major cloud players are equally or more secure than most internal enterprise systems. However, a more serious issue is how to control what information is moving, to which location it is moving, and is this location firmly in compliance with corporate regulations with clear controls for risk management, access policies, and usage controls.

Today's leading CASB solutions provide five key Compliance features:

- **Access for Managed versus Unmanaged Devices** - provides different levels of access to applications based on whether the device is managed or unmanaged by enterprise policies.
- **Role Based Access** - provides different levels of access to applications based on users and/or groups (e.g., sync via Active Directory).
- **Native Single Sign-On** - provides native single sign-on services as opposed to requiring a manual integration by enterprise IT teams.
- **Track Downloaded Data** - identifies and reports on data downloaded from enterprise systems.
- **FIPS 140-2 Compliance** - provides encryption compliant with the federal standards.

Data Security

Data security, whether located on-premise, on a mobile device, or in the cloud, is a primary focus for all IT shops. For most companies, data is their greatest asset. So, as they disperse this data across a growing portfolio of cloud destinations, data security becomes a major concern.

Today's leading CASB solutions can effectively secure data residing outside an enterprise's network perimeter, especially in cloud applications or mobile devices. CASB solutions monitor and control the movements of sensitive data outside the corporate firewall without compromising the end-user experience.

Originally, CASB solutions acted only as security services sitting between a corporation's on-premise infrastructure and cloud services and were primarily focused on visibility and auditing. Now, leading solutions typically also incorporate a growing set of Data Security features and this continues to evolve. CASB solutions have become increasingly adept at protecting data that travels between an organization's perimeter and cloud services. This shield of protection was initially cast around SaaS services but has recently been expanded to protect IaaS and PaaS deployments.

Leading CASB solutions can effectively enforce data-centric security policies that prevent unwanted activity based on data classification, discovery, variations in user access to sensitive data, and privilege escalation. These policies are applied through controls such as audit, alert, block, quarantine, and delete. Several CASB solutions provide the ability to encrypt, tokenize, and redact content at the field or file level. Encryption key management may be integrated with any on...
The Evolution of CASB

Now is the Time to Rock the CASB

premise products. Data Loss Prevention (DLP) features are both natively included in CASB products and available from on-premise network DLP products via Internet Content Adaptation Protocol (ICAP) integration. Data-Centric Audit and Protection (DCAP) features are also native to a handful of CASB solutions but are also found in traditional on-premise DCAP providers who now cover cloud use cases.

Today's leading CASB solutions provide six key Data Security features:
• Encrypt Structured/Unstructured Data
• Simple and Advanced Data Patterns
• Prebuilt Library - Common Data Types
• In-Line Protection
• Mask/Block Data before Download
• Integration with On-Premise DLP via ICAP

Threat Protection
CASB solutions prevent unwanted devices, users, and applications from accessing cloud services by providing adaptive access controls. By adding Threat Intelligence, Malware Identification, and UEBA features, CASB solutions are becoming very adept at determining anomalous user and application behavior. Several vendors have even developed their own analyst teams who research cloud-specific and cloud-native attacks.

CASB solutions help to fill many of the security gaps created when data-center focused enterprises extend operations beyond their perimeter into cloud services and across cloud service providers. Using CASB features, enterprise security professionals are able to monitor and respond to security issues across cloud services, including IaaS and/or PaaS providers by allowing security operations teams to set policy, monitor behavior, and manage risk across all cloud services.

Many CASB solutions can now consolidate multiple security policy enforcement types, including authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, and malware detection and prevention. More progressive CASB solutions also provide advanced control and monitoring, risk and compliance management, threat protection, cloud data security, and data leakage prevention features.

Today's leading CASB solutions provide five key Threat Protection features:
• Advanced Threat Protection - provides security features that defend against sophisticated malware or hacking-based attacks targeting sensitive data.
• Scan Data at Rest - scans data at rest for malware.
• Prevent Upload of Malware - prevents upload of malicious files from unmanaged devices.
• UEBA Lite - provides a subset of UEBA functionality such as suspicious user locations, consecutive login failures, and user risk scoring.
• Detect Compromised Credentials - detects and reports when credentials have been compromised.
The Evolution of CASB

Now is the Time to Rock the CASB

Trace3's Take

Predictions

1. SaaS and IaaS providers will start to offer CASB services for an additional subscription fee within the next 12 months.

2. API functionality will continue to become more robust through the extension of protection and security use cases.

3. Enterprise integration will continue to mature as IT leaders demand single pane of glass visibility across all of their security solutions including CASB.

4. CASB DLP functionality will rapidly mature and expand until it is on par with traditional on-premise DLP solutions.

5. CASB UEBA functionality will become ubiquitous and develop with network-centric, identity-centric, and log-centric UEBA capabilities.

6. CASB will integrate machine learning as an underpinning to its security functionality, allowing it to protect the ever-increasing "fuzzy" attack surface.

7. Unlike most other enterprise IT use cases, it is highly unlikely a full featured CASB will be offered as an open-source variant.

Recommendations

1. CASB solutions require a significant understanding of an organization's use cases to be effective. In particular, for a CASB integration to be successful an enterprise must have an in-depth understanding of their overall detection and prevention strategy.

2. When choosing a CASB solution, place great emphasis on the protection features provided by the product for a given application and not just the list of applications protected since not all capabilities are provided for all applications.

3. When selecting a CASB, a Pure Play solution containing a focused feature set should be the first consideration, unless the enterprise has an existing footprint with a CASB Platform vendor.

4. CASB solutions fall into the OpEx side of the IT budget, therefore enterprises with a CapEx focus should evaluate the financial impact before defining their CASB strategy.

5. CASB intersects multiple disciplines within IT (e.g., IAM, MDM, DLP), therefore enterprise integration of both technology and people should be a primary concern.

6. The various permutations of CASB implementation strategies (proxy or API mode), device locations (internal or external), and device types (managed or unmanaged) will result in variances in visibility, compliance, data security, and data protection functionality within the same solution and therefore should be a key consideration in vendor selection.
The Evolution of CASB

Now is the Time to Rock the CASB

CASB solutions are on-premise or cloud-based security policy enforcement points placed between cloud service consumers and providers to enforce enterprise security policies as the cloud-based resources are accessed. Security policies under CASB control include authentication, single sign-on, authorization, credentials, device profiling, encryption, tokenization, logging, alerting, malware detection, and prevention.

Appendix

Featured Use Cases

Cloud Access Security Broker

CASB solutions are on-premise or cloud-based security policy enforcement points placed between cloud service consumers and providers to enforce enterprise security policies as the cloud-based resources are accessed. Security policies under CASB control include authentication, single sign-on, authorization, credentials, device profiling, encryption, tokenization, logging, alerting, malware detection, and prevention.

Sources


© 2017 Trace3, Inc. All Rights Reserved
The Evolution of CASB

Now is the Time to Rock the CASB

CASB Explained

### CASB Landscape

#### Pure Play

- bitglass
- CENSORTNET
- CipherCloud
- netskope
- FIRELAYS
- skyhigh
- ORACLE

#### Platform

- Cisco Cloudlock
- FORCEPOINT
- Microsoft
- FORTINET
- Symantec

Visibility

### CASB Visibility Comparison

<table>
<thead>
<tr>
<th></th>
<th>Forward &amp; Reverse Proxy</th>
<th>API Support</th>
<th>Agent Dependent</th>
<th>Consolidated Dashboard Views</th>
<th>Segregate Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>bitglass</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CipherCloud</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Cisco</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>FORCEPOINT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>netskope</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>paloalto Networks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>skyhigh</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Symantec</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

© 2017 Trace3, Inc. All Rights Reserved

- ✓ - Supported
- ✗ - Not Supported
- ○ - Partial Support or 3rd Party Reliance
### CASB Compliance Comparison

<table>
<thead>
<tr>
<th>Product</th>
<th>Managed vs Unmanaged Devices</th>
<th>Role Based Access</th>
<th>Native Single Sign-On</th>
<th>Track Downloaded Data</th>
<th>FIPS 140-2 Compliant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitglass</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>CipherCloud</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forcepoint</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netskope</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Palo Alto</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skyhigh</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2017 Trace3, Inc. All Rights Reserved

- Supported
- Partial Support or 3rd Party Reliance
- Not Supported

### CASB Data Security Comparison

<table>
<thead>
<tr>
<th>Product</th>
<th>Encrypt Structured/Unstructured Data</th>
<th>Simple &amp; Advanced Data Pattern</th>
<th>Prebuilt Data Types</th>
<th>In-Line Protection</th>
<th>Mask/Block Download</th>
<th>Integration with DLP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitglass</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CipherCloud</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cisco</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forcepoint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netskope</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Palo Alto</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skyhigh</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2017 Trace3, Inc. All Rights Reserved

- Supported
- Partial Support or 3rd Party Reliance
- Not Supported
About Trace3 Research

To solve the IT problems of tomorrow, our research engineers leverage Trace3’s unique access across the technology landscape to derive impartial insights. By identifying and analyzing technology and market trends, we enable our customers to prepare for and master tomorrow’s challenges before they arrive. Trace3 Research leverages our partnerships with 500 established and emerging technology companies, the real-world experience of over 250 engineers, a 3000-client ecosystem and deep relationships with dozens of the top Silicon Valley venture capital firms to spot trends ahead of most industry pundits. This allows you to take advantage of Trace3’s Research unique access to gain an inside advantage on tomorrow’s trends and reduce your technical and business risk.

(end of report)