Definitive Guide™

to

Cloud Access Security Brokers

Visibility, Security, and Compliance for Applications and Data in the Cloud

Jon Friedman
Mark Bouchard, CISSP

FOREWORD BY:
Assaf Rappaport, CEO and Co-Founder of Adallom

Compliments of:

ADALLOM

Hewlett Packard Enterprise

About Adallom

Founded in 2012 by cyber defense veterans, Adallom is a 2014 Gartner Cool Vendor. Adallom's cloud access security broker delivers visibility, governance and protection for cloud applications. Its innovative platform is simple to deploy, seamless to users, and is available as a SaaS-based or on-premises solution. Powered by SmartEngine™ advanced heuristics and backed by an elite cybersecurity research team, Adallom makes it easy to protect data in the cloud.

For more information, visit www.adallom.com or follow @adallom.

About HPE SECURITY — Data Security

HPE SECURITY — Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise we protect the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use and in motion. Our solutions provide advanced encryption, tokenization and key management that protect sensitive data across enterprise applications, data processing IT, cloud, payments ecosystems, mission critical transactions, storage, and big data platforms. HPE SECURITY - Data Security solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

For more information, visit www. hpe.com/go/DataSecurity and www.voltage.com

Definitive Guide™
to
Cloud Access Security Brokers

Jon Friedman
Mark Bouchard, CISSP

Foreword by Assaf Rappaport

CYBEREDGE
PRESS

Definitive Guide™ to Cloud Access Security Brokers

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9961827-0-6 (paperback); ISBN: 978-0-9961827-1-3 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Designer: Debbi Stocco
Production Coordinator: Valerie Lowery
Adallom Subject Matter Experts: Chris Westphal and Danelle Au

Table of Contents

Foreword

There is a commercial that always seems to come on when I sit down to watch one of my favorite TV shows. A guy on the screen says "the hardest part about going to the gym is going to the gym." That seems silly, but he has a point. People hesitate to purchase a gym membership because they are afraid they will never be able to get to the gym to take advantage of it. (The pitchman is of course pushing a home workout solution that eliminates that problem.)

It's the same issue with cloud security. Just like the commercial, the hardest part about moving to cloud applications is that people are not confident they can get results without struggling forever with the trials, tribulations and complexity of security. I hear from customers all the time who are overwhelmed with options and don't know where to start.

Just like any new technology, cloud security can get in the way of customers realizing the benefits of software-as-a-service. The promises of cost savings and user productivity are hidden behind nebulous layers of unknown security risk. IT departments and CISOs have quickly realized that the security perimeters they've built up over the years are no longer relevant. They're not sure what to do next. This uncertainty either paralyzes them or causes them to make a very uncomfortable leap of faith into the unknown cloud.

At Adallom, we set out to make it easy to secure your data in the cloud. We focus on flexible deployments, comprehensive controls, and proven threat protection. Our goal is to solve "the hardest part about securing the cloud" so that customers can get to what they really want: using cloud applications and taking advantage of their benefits.

We've built a cloud access security broker (CASB) solution that helps you take that first step of discovering what's being used across your organization so you can move to identifying, sanctioning and securing the right cloud applications for your business. We give you tools for visibility into cloud activities, for control over access to apps, for protection over data, and

for threat prevention. We even help you leverage your existing security infrastructure by extending it to the cloud.

As you start out on your journey to secure your cloud applications it's important to understand the full extent of features that can be delivered by CASBs. As with many security solutions, there are many capabilities, benefits and deployment options. We've sponsored this guide to provide you with a better understanding of CASBs.

And of course, when you're ready to embrace cloud applications, we're here to help.

Assaf Rappaport
CEO and Co-Founder
Adallom

Introduction

We hope you will find this *Definitive Guide to Cloud Access Security Brokers* alarming, reassuring, and informative.

Alarming, because we highlight the many challenges enterprises face with cloud applications: lost visibility, unmanaged devices, users who share too many files, and attackers who find your weakest links.

Reassuring, because we describe how cloud access security brokers (CASBs) strengthen security in more ways than the name implies. Certainly they help you control *access* to cloud applications. But they also provide *visibility* into how people and devices interact with applications and data. They improve *threat protection* by alerting you to risky behaviors, policy violations, and deviations from normal usage of cloud applications. They help you enforce *compliance* with industry regulations. They can even remove vulnerabilities and stop threats in their tracks.

Informative, because we review issues related to selecting and implementing a CASB, including deployment modes (API, proxy, and hybrid), and integration with other security technologies. Also, we describe how to extend into the cloud your existing policies for access control, data loss prevention (DLP), compliance, and encryption.

After you read this guide we think you will agree that no enterprise can afford to move to cloud applications without a CASB.

Chapters at a Glance

Chapter 1, "How Cloud Applications Change the Game for Security," examines the challenges facing security teams when enterprises move to cloud applications.

Chapter 2, "Understanding Cloud Access Security Brokers," presents an overview of CASBs and how they provide value in four areas of cybersecurity.

Chapter 3, "Visibility," outlines the types of data that can be monitored by a CASB and the insights that can be derived from that data.

Chapter 4, "Threat Protection," explores how a CASB can generate alerts for security teams and how heuristics can identify threats invisible to other security technologies.

Chapter 5, "Access Control, Data Protection, and Compliance," describes adaptive access control and explains how DLP, encryption, and compliance policies can be enforced for cloud applications.

Chapter 6, "Implementing a Cloud Access Security Broker," reviews integration with other security solutions as well as architecture issues that affect the benefits a CASB can provide.

Chapter 7, "Selecting the Right Cloud Access Security Broker," enumerates criteria for choosing the CASB that best fits your organization.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

How Cloud Applications Change the Game for Security

In this chapter

- Learn why cloud application providers address only some of your cybersecurity issues
- Review security challenges facing cloud application customers

*"**Student**: Dr. Einstein, aren't these the same questions as last year's [physics] final exam?*

***Einstein**: Yes, but this year the answers are different."*

The questions in cybersecurity haven't changed: Can you detect malicious activities, protect critical information assets, and enforce security and compliance policies?

But you need new answers. In the emerging world of cloud-based applications and software-as-a-service (SaaS), you face challenges like applications you don't manage, mobile devices you don't control, and end users who happily share files with "anyone with the link."

To set the stage for our discussion of cloud access security brokers (CASBs), this chapter outlines the distinctive cybersecurity issues that must be addressed by enterprises using cloud-based software like Office 365, Google Apps, Salesforce, Box, and Dropbox, as well as internally developed applications hosted in private clouds.

The Cloud Application Tsunami

It is clear that enterprises of all sizes are moving rapidly to take advantage of cloud-based applications, platforms, and services. According to industry analyst firm IDC:

- ☑ Worldwide spending on SaaS enterprise applications is growing by 18% a year and will reach almost $51 billion in 2018.
- ☑ The overall market for cloud-based solutions and platforms will grow from about $57 billion in 2014 to $127.5 billion in 2018.

The trend is being driven by enterprises seeking to reduce costs, improve productivity and collaboration, offload server and software management, increase application availability, and scale by adding services and users on demand. By increasing business agility, cloud applications can also increase competitiveness and help enterprises bring products and services to market faster.

For background on the adoption of cloud computing, obtain *The Cloud Grows Up* by connecting to: http://www.oxfordeconomics.com/cloudgrowsup, and *Preparing for the next-generation cloud* by connecting to: http://www.economistinsights.com/technology-innovation/analysis/preparing-next-generation-cloud-lessons-learned-and-insights-shared.

Shared Responsibility: Why You Can't Outsource Security

Unfortunately, you can't outsource cybersecurity by going to the cloud. Cloud application vendors are committed to protecting the integrity of their applications and infrastructure. However, they can't control your employees, and they don't know enough about your users or your business to detect abnormal behaviors or to apply your policies for security and regulatory compliance.

Your enterprise is still responsible for:

- ☑ Protecting user credentials and access to cloud applications
- ☑ Deciding what information is sensitive, and enforcing policies for accessing and sharing it
- ☑ Monitoring events and behaviors to detect malicious activities
- ☑ Documenting compliance with regulations and industry standards

Review the license agreements of your SaaS vendors. How do they define their responsibilities and yours? Here is an example from the Google Apps terms of service: "Customer will use commercially reasonable efforts to prevent unauthorized use of the Services and to terminate any unauthorized use. Customer will promptly notify Google of any unauthorized use of or access to the Services…"

Now let's look at the issues that make your part of the security equation so difficult.

Who watches grandma's necklace?

You want to celebrate the college graduation of your favorite niece by giving her the use of your late grandmother's heirloom emerald necklace. You prudently rent a safe deposit box at the nearest bank and give her the key.

The bank will ensure that nobody steals the necklace by tunneling into the vault or by forcing their way in with a gun.

But you are out of luck if someone obtains the key and passes herself off as your niece. Nor is the bank responsible if your niece leaves the necklace in her car and a criminal steals it.

Moreover, it isn't the bank's job to monitor your niece's behavior and determine if she is acting responsibly. The bank can't stop her from taking the emeralds to parties every weekend or leaving them in an unlocked drawer in the apartment she shares with three roommates.

In short, whether the vault is in the bank or in the cloud, you share responsibility for security, especially aspects such as safeguarding credentials, protecting assets in motion and at rest, and monitoring behavior.

Security Challenges for Cloud Applications

Most of today's cybersecurity processes and tools were developed when applications ran in local datacenters, when endpoint devices were owned and managed by the enterprise, and when administrators could control how files were stored, accessed, and shared. With cloud applications, we can't assume any of those conditions still hold.

Lost visibility

When applications reside in corporate datacenters, enterprises can monitor all events and actions related to access and activity.

But for applications hosted in the cloud, enterprises have only as much visibility as the cloud application vendors are willing to provide. In addition, every cloud application vendor has its own mechanisms for authentication and access control, its own activity monitoring capabilities, its own alerting system, and its own audit trails.

As a result:

- ☑ Security organizations often are unable to detect policy violations or indicators of potential attacks.
- ☑ Even when attacks are detected, it is difficult and time-consuming to pull together and correlate threat indicators and security data from multiple applications.

Unmanaged and non-compliant devices

When a laptop or mobile device is owned and managed by the enterprise, administrators can ensure that it meets security requirements such as a patched operating system, secure browsers, and up-to-date antivirus files. They can usually limit the installation of non-approved software, and enforce the use of secure virtual private network (VPN) connections by remote users.

In a world of BYOD (bring your own device), users who supply their own laptops, tablets, and smartphones feel entitled to treat them as personal devices. They often:

- ☑ Ignore patches and security updates
- ☑ Install whatever apps catch their fancy, no matter how sketchy the source
- ☑ Share the devices with friends and family members
- ☑ Connect to cloud applications through unsecure WiFi hotspots and public networks

The consequences include:

- ☑ Continual violations of corporate policies, such as those that prohibit the download of files containing sensitive information, or require downloaded files to be encrypted
- ☑ Increased risk of data leakage from compromised endpoints
- ☑ More opportunities for attackers to compromise endpoints and capture credentials there
- ☑ Mobile employees connecting to cloud applications directly through public networks, bypassing monitoring and security controls

You may need to update your corporate and compliance policies to reflect cloud computing conditions. Educate your users on those policies and the harm they can cause by violating them.

Hidden data, over-sharing, and rogue admins

In conventional client-server applications, most data is stored in one or two places within the application, and administrators can control access. But in our current world of global collaboration:

- ☑ A single application might have separate repositories for office documents, structured data, video files, chat sessions, social media feeds, design documents, and software files.

- ☑ Users storing files in cloud applications and collaboration services like Box and Dropbox share sensitive data with people outside the organization, and give permission to share data with "connected apps" in the application vendor's ecosystem.
- ☑ To help manage cloud applications like Salesforce and Google Apps, departments designate "administrators" who make bad security choices.

Not only is it much harder to monitor access to data, but information sharing decisions that were once made by IT staff have now been ceded to users and untrained administrators. These conditions give cybercriminals and hackers an incredibly rich set of targets for compromise.

For quantified descriptions of risks related to cloud applications and data sharing, connect to Adallom's *Cloud Usage Risk Report*: https://learn.adallom.com/Adallom-Cloud-Usage-Risk-Report.html, and the *Cloud Security Alliance's Cloud Usage: Risks and Opportunities Report*: https://cloudsecurityalliance.org/download/cloud-usage-risks-and-opportunities-survey-report/.

The weakest links

Attackers trying to steal your organization's information assets will find your cloud application vendors a hard target. It is easier for them to:

1. Launch a phishing attack to capture credentials. According to the Verizon 2015 Data Breach Investigation Report, 23 percent of recipients open phishing messages and 11 percent open attachments. The attacker can use phishing to acquire user credentials to access your cloud services. (See *Amazon EC2 control panel hack submarines hosting provider* at: http://searchsecurity.techtarget.com/news/2240222992/Amazon-EC2-control-panel-hack-submarines-hosting-provider.)

2. Compromise a home computer. An attacker can find the identities of your employees on social media, break into computers at their homes (some of which will be poorly defended), and try a "landmine" attack. That means planting malware on the PCs that steal data when employees log into their cloud applications. (See *New Zeus Variant Found Targeting Salesforce.com Accounts* at: http://www.securityweek.com/new-zeus-variant-found-targeting-salesforcecom-accounts.) The attacker also might find on the PCs sensitive files that were downloaded against policy.

Chapter 2

Understanding Cloud Access Security Brokers

In this chapter

- Examine a conceptual view of a cloud access security broker
- Understand four categories of security where CASBs provide value

"Necessity is the mother of invention."

— Plato

A new class of product has emerged to address the challenges faced by enterprises moving to cloud applications. The analyst firm Gartner has named these solutions *cloud access security brokers* (CASBs). In this chapter we provide a high-level conceptual view of CASBs, and discuss how they extend existing cybersecurity concepts to cloud application environments.

What is a Cloud Access Security Broker?

We define a cloud access security broker as:

A platform that provides visibility into cloud applications, monitors application access and usage across multiple cloud-based applications, and enforces policies for access control, data protection, and compliance.

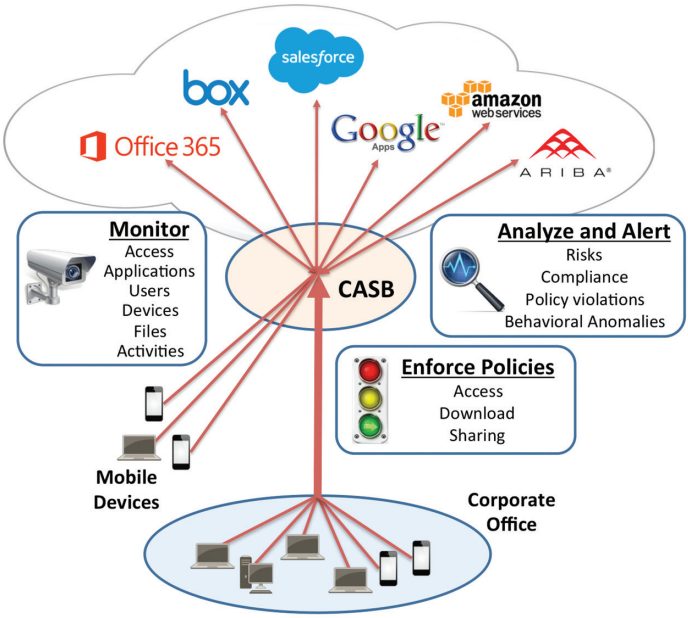

Figure 2-1: Conceptual view of a cloud access security broker

One of the primary functions of a CASB, as illustrated in Figure 2-1, is to monitor the access of all users, from all managed and unmanaged devices, to all cloud applications. The CASB collects data related to:

- ☑ **Cloud-based applications**
- ☑ **Users** accessing the applications
- ☑ **Devices** used to access the applications
- ☑ **Files and data** being created and stored in the applications
- ☑ **Activities** related to accessing applications and files (such as logins and session duration), related to working with applications and files, and related to managing permissions for access and sharing

But a CASB is much more than a passive monitoring tool. It can correlate and analyze the data it collects in order to:

- ☑ Identify vulnerabilities and risks
- ☑ Detect anomalous behaviors indicating attacks
- ☑ Demonstrate compliance with policies and regulations

A CASB can strengthen threat protection and incident response by generating alerts when it detects risks, policy violations, and anomalous behaviors.

Finally, a CASB can be a platform for enforcing corporate and regulatory policies in order to:

- ☑ Control access to applications and files
- ☑ Control when and how files and data are shared and downloaded

Figure 2-1 is a conceptual view of a CASB, but *not* an architectural representation. CASBs can capture data from firewall and device logs, through application APIs, and with a proxy that scans network traffic. It is important to understand the strengths and limitations of these methods before making deployment and vendor selection decisions. We will discuss architectures and deployment modes in Chapter 6.

How CASBs Strengthen Security

The capabilities of CASBs can be grouped into four categories: *visibility, threat protection, access control*, and *compliance*. We provide a brief overview here, and will examine the categories in depth in Chapters 3, 4, and 5.

Visibility

CASBs can provide very detailed data on which cloud-based applications are used in the enterprise, who is accessing them, and how they are being accessed (from what devices, when, and where). They can also show what files are being stored, who owns them, and how they are being accessed and shared inside and outside the enterprise. This data can be correlated

and analyzed to help enterprises monitor user behaviors, assess risks, manage policies, and improve security practices.

Think of CASBs as a way to restore much of the visibility lost when application activity and data are moved from the datacenter to the cloud. A CASB can identify heavily used applications and files, track trends, and identify risks such as inactive user accounts ("zombies") and confidential data shared with external users. It can also "discover" cloud applications brought into the workplace by business departments without the knowledge and support of IT.

Threat protection

Today, most IT organizations concede that attackers will be able to capture user credentials through spear phishing attacks and social engineering techniques. It is therefore critical to monitor application access and usage and detect anomalous behaviors and indicators of attacks as soon as possible. Yet these areas are exactly where cloud application vendors provide the least help. That is not surprising: how is a cloud application vendor supposed to know what is normal for your organization and your users?

Threat protection is one area where CASBs provide services unavailable from any other source. A CASB can observe the activities of a user across multiple cloud applications and multiple devices, and use that data to create baselines of normal behavior. The CASB can then generate alerts when it detects deviations from those baselines.

The large volumes of data about applications, users, devices, files, and activities that CASBs collect can also be extremely valuable to incident response (IR), forensics, and risk management teams trying to reconstruct advanced, multi-stage attacks and determine the attackers' tactics, techniques and procedures (TTPs).

Some CASBs can be integrated with security information and event management (SIEM) solutions. With that integration, alerts generated by the CASB, together with related information and "context," are available in real time to your security operations center (SOC) and IR teams.

Access control

In the old days, access control was based on a relatively simple question: Is this person entitled to access the corporate network and the applications on it?

In a cloud computing world, the enterprise may want to base access decisions on a more nuanced set of conditions: What resources are safe to expose to this person (or more accurately, to this set of user credentials), when requested from this device, in this location, over this network connection?

Through "adaptive access control," a CASB makes it feasible to create multi-factor, granular access rules and to enforce them consistently across a range of cloud applications.

Compliance and data protection

CASBs provide audit trails so organizations can demonstrate that application activities, access, and file sharing comply with corporate policies and industry standards.

They can also be used to enforce compliance requirements and protect data using technologies such as:

- ☑ Data loss prevention (DLP), to identify and block the download and sharing of files containing sensitive information like intellectual property and personally identifiable information (PII)
- ☑ Encryption, to ensure that files are encoded before they are uploaded to or downloaded from the cloud
- ☑ Information rights management (IRM), to prevent sensitive content in documents from being copied, printed, or otherwise distributed

A CASB can help apply sophisticated data protection rules, for example, enforcing the encryption of files downloaded to unmanaged devices, or blocking the sharing of files with devices that log on from dubious geographical regions.

Extending the Reach of Existing Security Tools

Deploying a CASB does not mean adding a new layer of technology that duplicates your current security solutions. Rather, it can extend your existing security tools and policies into the cloud. For example, some CASBs can:

- ☑ Manage access to cloud applications based on information contained in enterprise directories about users, user groups, and roles
- ☑ Extend existing DLP and encryption solutions to protect files being downloaded from cloud applications
- ☑ Share data with SIEM systems about application access, policy violations, and security incidents outside the corporate network

Phased Implementation

CASB capabilities can be implemented in stages so that:

- ☑ Monitoring of cloud application activities can be started literally in minutes.
- ☑ Detection of behavioral anomalies and security violations can also be enabled out of the box.
- ☑ Access control policies can be gradually customized to support specific use cases.
- ☑ Advanced controls can be put in place over time to enforce compliance policies and automate data protection.

This phased approach allows enterprises to realize major benefits immediately. They can achieve early wins and avoid the risks inherent in monolithic “big bang” implementations, and later deploy advanced features as they are needed.

Chapter 3

Visibility

In this chapter

- Understand the types of activities that can be monitored by a cloud access security broker
- Learn about the insights that can be gained and how they can improve security

"You can observe a lot just by watching."

— Yogi Berra

We have said that one of the main functions of a cloud access security broker is to monitor access and usage across multiple cloud-based applications. But when a CASB is monitoring, exactly what data does it collect, and how can that information be used? What insights can you expect to gain from visibility into user activities?

Data, Sources, and Output

Figure 3-1 shows some of the data collected by a CASB, where it comes from, and how it can be used.

Data about activities

When Jon asks to log into Salesforce.com, or Mark tries to download a file from Box, we generate a lot of data related to the requestor, the "object" of the request, and the requested action. This data can be captured by a CASB.

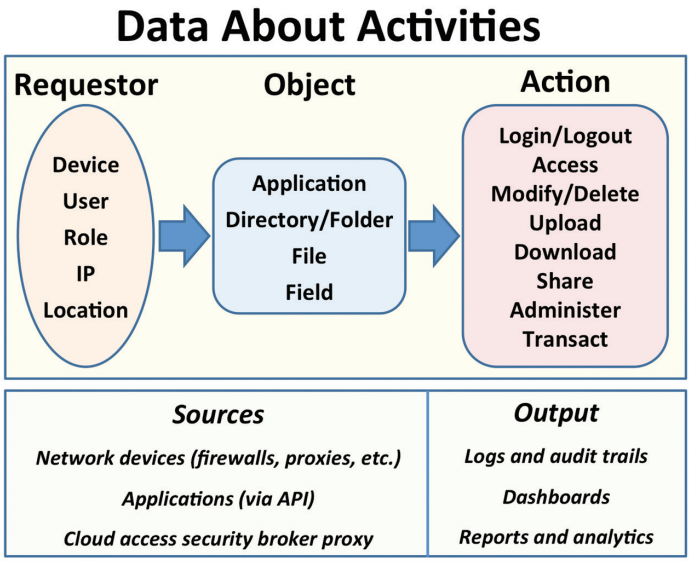

Figure 3-1: Data collected by a cloud access security broker

Information about the requestor might include not only the user (Jon, Mark), but also the user's role (analyst, vice president of research), the device (Jon's laptop, Mark's smartphone), and the IP address and location where the request was made.

The request will relate to an object or entity, in most cases an application, directory, file, or field of data.

The request will involve an action that the user wants to carry out. This might be to:

- ☑ Log into or log out of an application
- ☑ Access a directory or file
- ☑ Create, modify, or delete a directory, file, or data field
- ☑ Upload or download a file
- ☑ Share a directory or file with other users
- ☑ Perform an administrative action, such as changing access permissions for a directory or file
- ☑ Perform a transaction in an application

Sources and output

The primary sources of data for a CASB are:

- ☑ Network devices such as firewalls, next-generation firewalls (NGFWs), secure web gateways (SWGs), and proxies, which provide information on what cloud applications users are accessing
- ☑ Cloud applications, which record data on users, requested actions, and the results of requests (e.g., Did the login request succeed or fail? Was the file edited? Were the file permissions changed?)
- ☑ A CASB proxy, which directly monitors application access and activities (CASB proxies will be discussed in Chapter 6)

A CASB can produce output in many forms, including:

- ☑ Dashboards, which highlight key issues and trends
- ☑ Logs and audit trails, which provide detailed information for compliance audits, incident response, forensics, and risk management
- ☑ Standard and custom reports
- ☑ Databases used for queries and advanced analytics

Dashboards are a good place to start when you are learning about a CASB. The dashboard will give you a quick read on the current status of all cloud applications being monitored and protected.

Visibility at Work

Let's look at some of the insights we can find in this data.

Discovery of unsanctioned applications

A CASB can provide visibility into cloud applications that are unsanctioned by the IT organization. These applications can pose major security risks because they lack security features, or simply because they are unmonitored.

The IT organization can use a CASB to rein in “shadow IT” applications using a three-step process:

1. **Discover** unsanctioned cloud applications, including applications being used, the number of users, and the amount of usage
2. **Categorize** the applications into those that should be banned (because they create significant risks), those that can be ignored (because they are rarely used or pose no risk), and those that should be sanctioned and supported by the IT organization
3. **Protect** the sanctioned cloud applications by monitoring them and enforcing policies with the CASB

Some CASBs provide extensive information on the security features and weaknesses of popular cloud applications. This information can be used to show business managers why their unsanctioned applications are a bad idea, and to help enterprises select more secure cloud application vendors.

A CASB can also discover "connected" third-party applications accessing data in sanctioned cloud applications. For example, a group of Google Apps users might grant an unsanctioned third-party application permission to access their Gmail accounts and the files they store in Google Drive. A CASB could identify the application, the users employing it, and the permissions they granted. If the access created significant risks, the CASB could block the unsanctioned application from accessing data in Google Apps.

When information hides in applications

A CASB can also discover information and files stored in unexpected corners of cloud applications.

Do you manage customer relationships with Salesforce? Sensitive company and customer information is probably stored in customer records and attachments in the CRM system, in Chatter files, and in Knowledgebase articles. That same information might also be distributed on Community Cloud, or shared with apps on Salesforce AppExchange (https://appexchange.salesforce.com/). A CASB can provide visibility into where the information is hiding and how it is being shared.

Users, abusers, and imposters

A CASB can provide detailed information about usage trends for cloud applications, including which applications are being used, who is accessing each application, and how rapidly cloud application usage is growing. This data can help you understand user needs and plan for future requirements.

In addition, a CASB can identify users who indulge in risky practices. Bad behaviors include downloading files with sensitive data to unmanaged devices (such as home PCs), sharing sensitive files publicly, and authenticating directly to cloud applications without going through corporate single sign-on (SSO) tools. Warning and educating these users can curb their risky behaviors.

A CASB can also detect evidence of attackers using stolen credentials. Such evidence might include excessively large downloads, abnormally large numbers of requests in short periods, access requests from new devices or new locations, and repeated attempts to violate corporate policies. In Chapter 4 we will discuss how CASBs can use sophisticated analysis to pinpoint abnormal behaviors, but many types of attacks can be identified based solely on routine monitoring and standard dashboards.

You can reduce risk by monitoring the online activities of critical individuals (such as CXOs, vice presidents, and administrators) and key departments (like finance, legal, engineering, and IT). These are the most common targets of spear phishing attacks. By keeping a close watch for indicators that top-level credentials have been stolen, you will be able to detect and stop advanced attacks sooner.

Oversharing

Information sharing is immensely complicated in today's cloud application world. Users can store and share files in:

- ☑ Business applications (Salesforce, Ariba)
- ☑ Productivity applications (Office 365, Google Apps)
- ☑ Cloud drives and collaboration applications (Box, Dropbox, OneDrive, Google Drive)

Users often make bad decisions when they set sharing permissions for files and directories. A user might invite groups to access a directory without knowing who is a member. Another might select "anyone with the link" as a permission for file access (Figure 3-2), then email that link to colleagues. The user might expect the colleagues to keep the link confidential, but nothing prevents them from forwarding the link to everyone they know.

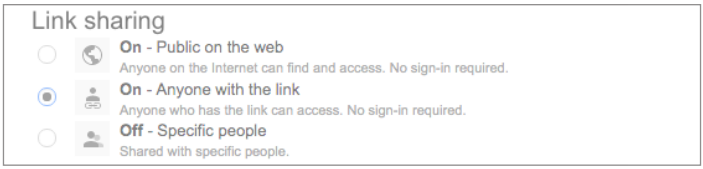

Figure 3-2: Users can share files without knowing the implications.

A CASB can monitor:

- ☑ Which files are being stored in applications and on cloud drives
- ☑ What sharing permissions have been granted for every directory and file
- ☑ Which files have been accessed or downloaded by external (as well as internal) collaborators

Zombies and super admins

CASBs can identify "zombie" admins (privileged users who have been inactive for several months) and unnecessary super admins (users of applications like Salesforce and Google apps who have been granted administrative rights but never perform administrative tasks). Eliminating or downgrading these accounts reduces the potential for damage if users' credentials are stolen or accounts are misused.

Cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure present a special use case for a CASB. Accessing the consoles for these services is equivalent to taking control of the administrative console in a corporate datacenter. Enterprises need to make sure attackers don't alter machine configurations, remove instances, delete backups, or take other steps that interfere with applications running on the cloud platform.

Chapter 4

Threat Protection

In this chapter

- See how a CASB can generate alerts for security teams
- Understand how heuristics can help identify threats
- Learn how cyber threat intelligence can strengthen a CASB

"There is no terror, Cassius, in your threats; For I am armed so strong in honesty/That they pass by me as the idle wind."

— William Shakespeare

Cloud access security brokers can play an important role in today's biggest security sport: detecting cyberthreats in their early stages, before they do serious damage.

How CASBs Generate Alerts

Not only can CASBs provide visibility into risky and suspicious behaviors, they can generate alerts to security operations center (SOC) and incident response (IR) teams. They can call attention to risky actions and policy violations, and also detect anomalous behaviors.

As illustrated in Figure 4-1, a CASB can build a complete profile of how users and applications interact, then use machine-learning heuristics and behavioral analysis to create baselines of normal behavior. When deviations from these baselines occur, the CASB can generate alerts.

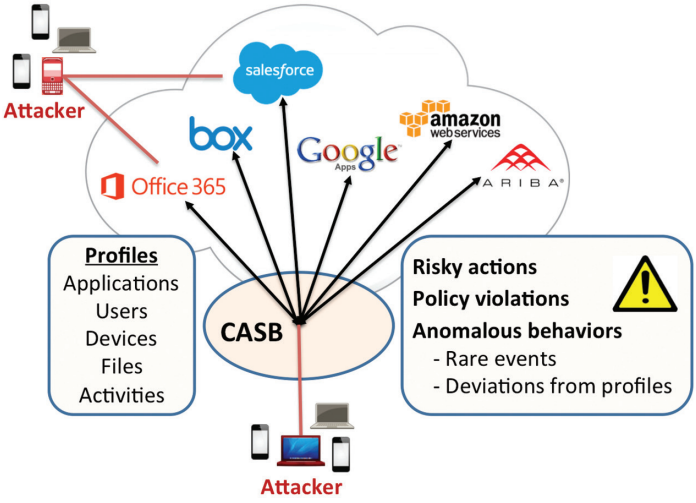

Figure 4-1: Heuristics use profiles of normal activities to detect anomalous behaviors

Heuristics are techniques for reaching approximate solutions to problems very quickly. Heuristic methods include rules of thumb, stereotyping, and profiling. Heuristics allow a CASB to establish norms for every user, application, and organization, and to quickly pinpoint behaviors that might represent the activities of threat actors. False positives are minimized because the norms are based on behaviors observed in real-world production environments. Accuracy improves over time as new data helps the system "learn."

We will now explore some of the ways that CASBs can generate alerts.

Risky actions and policy violations

A CASB can generate alerts when users create unnecessary risks or violate policies, such as:

- ☑ Sharing sensitive files publicly
- ☑ Downloading large numbers of files

- ☑ Attempting to access cloud applications directly, without going through corporate single sign-on (SSO) or identity and access management (IAM) solutions
- ☑ Attempting to download sensitive files to unmanaged devices such as home computers or non-compliant personal smartphones

Suspicious actions and security incidents

CASBs can alert security teams to evidence that an attack is in progress. Alerts might be generated based on:

- ☑ Access requests with the same user credentials coming from two different countries at the same time
- ☑ Access requests from blacklisted IP addresses (such as requests from anonymizing proxy services or from IP addresses belonging to competitors)
- ☑ Access requests from accounts that have been inactive for extended periods ("zombie" accounts)

Integration between a CASB and your security information and event management (SIEM) system can allow you to correlate suspicious activities in the cloud with suspicious events in the datacenter.

High-impact actions

You may decide that some actions have such great impact or potential for damage that someone on the security team should receive an alert every time they occur.

These actions might include:

- ☑ Creation of new privileged administrators and "super users" who have access to applications and data stores with sensitive information
- ☑ Configuration changes to key applications or to the administrative console of AWS, Azure, or other cloud platforms
- ☑ Any action by the CEO or CFO

Conduct a brainstorming session to enumerate the policy violations, risky and suspicious actions, and high-impact actions that should be monitored by a CASB. Enlist not only security analysts, but also database and application administrators, compliance officers, and business managers. You will uncover new ways of identifying threats and speeding up response and remediation.

Anomalous behaviors

A CASB can detect deviations from normal behaviors, as illustrated in Figure 4.1. These anomalies can take several forms:

- ☑ Rare events, such as a request to perform an administrative action from a user who has seldom or never performed an administrative action
- ☑ Unlikely events, such as a request to log into an application from a country from which nobody has ever accessed the application
- ☑ Deviations from profiles, such as an unusual number of failed login attempts in a short period

Dynamic Analysis of Files (Sandboxing)

A CASB can extend to the cloud the use of another key technology for threat protection: dynamic analysis of files, or "sandboxing." Sandboxing detects malware by executing files in an isolated "virtual sandbox" environment, then observing the behavior of the file and detecting suspicious or malicious actions.

A CASB can work with a sandboxing product to test both files-at-rest in cloud applications and files-in-motion being uploaded and downloaded. If the test detects malware, the CASB can send an alert to the security team, and send an analysis report of the malware to the SOC and IR teams.

Enforcement Actions

CASBs can take a number of enforcement actions to immediately eliminate vulnerabilities and block dangerous activities. These include:

- ☑ Blocking all requests from a suspicious user to log into applications
- ☑ Requiring two-step authentication to log into a specific application
- ☑ Changing permissions so a file cannot be shared publicly, or the contents of a directory cannot be downloaded
- ☑ Requiring a user to register his or her device

Supporting Incident Response and Forensics

Today most enterprises assume they will be compromised by advanced attacks. They rely on IR and forensics teams to spot indicators of compromise (IOCs), correlate them with other indicators, reconstruct attack steps, clean up damage, and improve security controls to prevent repeat incidents.

CASBs can play an important role in these activities. For example, if the IR team detects a suspicious download from a cloud application, the CASB can answer questions such as:

- ☑ What user account requested the download, from what device, and from which location?
- ☑ What other applications, directories, and files has this user account accessed recently?
- ☑ What other files has this user account downloaded and shared?
- ☑ Has this user account made any administrative changes to cloud applications to hide suspicious actions?

Answering these questions can help IR and forensics teams obtain a more detailed picture of attacks and move more quickly to stop them.

Cyber Threat Intelligence

Some CASB providers have their own cyber threat intelligence centers. Security experts in these centers look for new application vulnerabilities, scan the web for information about new threats to cloud applications, analyze the techniques of attackers, and identify indicators of probes and ongoing attacks. This intelligence is integrated into the decision rules and heuristics of the CASBs, and also shared with their clients' security teams.

Intelligence vs. the SEA

The Syrian Electronic Army (SEA) uses phishing, malware, web defacement, and denial of service attacks to intimidate enemies of the Syrian regime.

In a 2015 phishing attack, the SEA sent out emails containing a link to what appeared to be a YouTube sign-in form on a web site. Users who completed the form ended up sending their Google credentials to the attackers, who used them to:

- Reset the user's Google password
- Automatically forward copies of all email delivered to the user
- Install a piece of malware on the user's device

One victim brought information about the attack to Adallom, its CASB provider. The security researchers at Adallom Labs were able to reconstruct the steps of the attack, assess its potential impact, and supply the customer with mitigation techniques. They also provided other Adallom customers with guidance on how to thwart the attack.

You can find more detail about the SEA attack and Adallom's analysis at: https://www.adallom.com/blog/phishing-in-the-sea/.

Chapter 5

Access Control, Data Protection, and Compliance

In this chapter

- Learn about adaptive access control
- See how DLP, NAC, encryption, and IRM can be enforced for cloud applications
- Review how CASBs support compliance

"Distrust and caution are the parents of security."

— Benjamin Franklin

Cloud access security brokers not only monitor access to cloud applications, they also provide a central point for controlling access, preventing sensitive information from being downloaded to insecure devices, and enforcing encryption.

In effect, a CASB can extend data loss prevention (DLP), network access control (NAC), and other security technologies to cloud environments. They can also ensure enforcement of data sharing and compliance policies.

Some of the capabilities described in this chapter require a CASB deployed in proxy mode. Others involve integration with third-party products. These caveats are important, but to avoid cluttering our narrative we will hold off discussing them until Chapter 6.

Not Your Father's Access Control

Once upon a time, access control was simple: users on an access control list could log onto applications. But that paradigm provides no protection when cybercriminals manage to obtain legitimate user credentials by using phishing, keystroke loggers, or man-in-the-middle attacks.

How can a CASB minimize potential damage from an attacker with stolen credentials? By applying *adaptive access control*; that is, by restricting access based on real-time conditions. The CASB can factor in not only the permissions granted to the (purported) user, but also context such as whether the request is coming from:

- ☑ An unmanaged device (not very trustworthy)
- ☑ A user in an inappropriate role or department (a sales intern doesn't need to access engineering designs)
- ☑ An unlikely location (we have no employees in Romania right now)

Adaptive access control can provide granular control of user actions. For instance, a CASB could stop users from performing administrative actions, or permit read-only access to files but no editing or downloading.

One of the first things you should look at in a CASB is its access control capabilities. How granular are they? Can you enforce a blacklist (e.g., block access for requests coming from a specific country or range of IP addresses)? Does it offer "device pinning" (allowing administrative actions to be performed only by specific users on specific managed devices)? In what other ways can it help you reduce risk without blocking legitimate users?

Endpoint assessment and cloud NAC

As we discussed in Chapter 1, cybercriminals know that it is much easier to compromise a poorly protected home computer or personal mobile device than to attack a cloud application directly. A CASB, working in conjunction with an endpoint assessment solution, can identify at-risk devices and block their access to cloud applications.

PCs and mobile devices can be checked for factors such as:

- ☑ Malware infections
- ☑ Old, vulnerable operating systems, browsers, and apps
- ☑ Outdated or missing antivirus software
- ☑ The absence of required data protection technologies such as disk encryption

The CASB can function as a cloud NAC solution, preventing at-risk devices from accessing cloud applications, or restricting them to specific functions.

A CASB can also use endpoint assessment data as attributes for access control decisions, and to prevent users from downloading files and data to vulnerable devices.

Data Protection, Cloud Style

Data protection includes preventing sensitive data from leaving the cloud, ensuring that data downloaded to endpoint devices is properly secured, and implementing data sharing controls for files with sensitive content

Cloud DLP

DLP technology is designed to keep sensitive information on trustworthy systems. A DLP solution searches files, emails, and messages for key words, expressions, patterns of characters (xxx-xx-xxxx), and other clues indicating the presences of sensitive data such as credit card and Social Security numbers, personally identifiable information (PII), protected health information (PHI), intellectual property, and corporate legal and financial information. It can prevent files and messages containing such data from being downloaded or distributed outside the corporate network.

A CASB should give you the option of extending to cloud applications DLP rules you have already defined for your on-premises data stores. You shouldn't be forced to re-create and manage separate DLP policies for cloud and on-premises environments.

Encryption and IRM

One of the most important capabilities of a CASB is enforcing your encryption policies. Options include:

- ☑ Forcing the encryption of files uploaded from user devices to cloud applications
- ☑ Forcing the encryption of all files downloaded from cloud applications to devices that are unmanaged, are in unusual locations, or have other risk factors
- ☑ Forcing the encryption of all files with sensitive information downloaded from cloud applications
- ☑ Preventing the download of files to devices that do not have encryption software installed

A CASB, working in conjunction with an information rights management (IRM) solution, can provide even more granular control of sensitive information. This control might include:

- ☑ Requiring encryption based on file type (e.g., xls or exe), file name (e.g., the name includes "finance" or "confidential"), file owner, and other factors
- ☑ Allowing files to be read, but preventing users from printing or exporting the contents, or copying selections to clipboards
- ☑ Setting retention limits, for example, allowing a file downloaded to an unmanaged device to be accessed for only 30 minutes

Data sharing controls

A CASB can ensure that files with sensitive information are shared appropriately. For example, if DLP detects sensitive files being shared publicly on the Web, the CASB can implement controls such as changing permissions on files or removing editor privileges. It can also transfer ownership of files when users leave the organization.

Granular access control, DLP, NAC, encryption, and IRM not only reduce the risk of data leakage from unmanaged and poorly protected devices, they also have major implications for compliance.

Compliance

Many government regulations and industry standards require access audit trails, access controls, and encryption of protected data. You can find these capabilities in most cloud applications, but trying to implement them separately and document compliance across multiple applications can be a nightmare. Here we look briefly at some of the ways a CASB can simplify compliance.

Audit trails and attestation

A CASB can provide a complete audit trail of how cloud applications are being accessed and how data within those applications is being accessed and shared. The audit trail can document your enforcement of access policies and attest to the effectiveness of your controls. The CASB can dramatically reduce the time and effort required to collect and correlate compliance data across multiple cloud applications.

CASBs also provide a record of policy violations: people accessing data they shouldn't, sensitive files shared outside the enterprise, information downloaded to unsecure devices. Don't be dismayed if the numbers are high at first. Instead, be prepared to focus on the biggest issues, make improvements, and use the CASB to document progress.

DLP, eDiscovery, and IRM

Many regulations and standards include requirements to identify and control sensitive information such as PII, PHI, and credit card and Social Security numbers. A CASB with DLP capabilities can ensure that these mandates are addressed consistently across all cloud applications.

In addition, DLP features can help the corporate legal department "discover" documents related to litigation and regulation that are hiding in obscure corners of cloud applications (see the *When information hides in applications* box in Chapter 3). DLP and IRM can also help ensure compliance with data protection and document retention policies.

Encryption

Several of the most important regulations and standards have very strong requirements for encrypting data in the cloud, on endpoint devices, and in transit between the two. In addition, the Health Insurance Portability and Accountability Act (HIPAA) and several US state breach notification laws provide that if enterprises can prove that data on lost or stolen devices was encrypted, they do not need to notify customers or employees of the breach. This safe harbor clause can save millions of dollars in breach notification costs and avoid humiliating publicity. A CASB can ensure that file encryption policies are followed consistently, and quickly produce data that demonstrates compliance.

Sample compliance requirements

HIPAA § 164.312 Technical Safeguards

(a)(1) Standard: **Access control.** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights...

(iv) **Encryption and decryption** (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information...

(b) Standard: **Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

PCI DSS 3.1

3.4 Render [primary account number] unreadable anywhere it is stored...by using any of the following approaches: One-way hashes based on strong cryptography...Truncation... Index tokens and pads...**Strong cryptography**...

7.2 **Establish an access control system** for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

10.1 **Implement audit trails** to link all access to system components to each individual user.

Chapter 6

Implementing a Cloud Access Security Broker

In this chapter

- Examine how a cloud access security broker can interface with cloud applications and existing security solutions
- Understand the basics of API and proxy mode deployments, and review a phased approach to implementation

"God is in the details." — Ludwig Mies van der Rohe

"The Devil is in the details." — Various

Some of the features and benefits we have been discussing depend on how a CASB is deployed, and how it is integrated with other security solutions. Now we review some of those important implementation details.

Interfacing with Cloud Applications

We mentioned in Chapter 3 that one important source of data for CASBs is the applications themselves. Some CASBs interface with cloud applications through application programming interfaces (APIs). Through an API, a CASB can obtain information about an application's users, files stored in the application, permissions and sharing settings of those files, and activities such as logins and logouts, modifications, deletions, uploads and downloads of files, administrative actions, and transactions.

CASBs differ in how many cloud applications they can access via APIs. However, lesser-known SaaS applications and internally developed applications can be submitted to the CASB vendor for integration with their solution.

When you evaluate a CASB, consider both the breadth of its application coverage and how fast the vendor turns around requests to integrate new applications.

Some CASBs have catalogs detailing the security controls and compliance certifications of cloud applications. This information can help you assess the risks of unsanctioned cloud applications and have fact-based discussions with business units about whether specific applications are really enterprise ready. The same information can also help you decide which cloud applications to sanction and support and, if a replacement is needed, help you select a more secure alternative.

Deployment Mode Options

There are two deployment mode options for CASBs to monitor sanctioned applications: API mode and proxy mode (Figure 6-1).

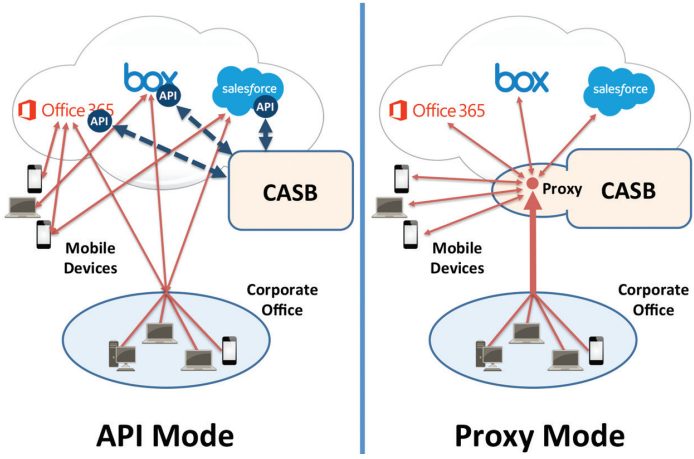

Figure 6-1: CASBs can be deployed in API mode and proxy mode

API mode

A CASB deployed in API mode is "out of band"; users communicate directly with cloud applications, and the CASB obtains data from the applications through their APIs. This approach provides very detailed visibility into data at rest and user activities, including logins and logouts, file uploads and downloads, information sharing, and administrative actions.

CASBs deployed in API mode can also perform administrative tasks and enforce governance policies. For example, if a user violates policies by publicly sharing files containing sensitive information, administrators can use the CASB to change the access permissions on the files, or to take file ownership away from the offending user.

A major advantage of API mode is speed: a CASB can be implemented literally in minutes because no changes to networks, endpoint devices, or applications are needed.

Proxy mode

A CASB deployed in proxy mode is "inline"; network traffic between users and cloud applications flows through the CASB proxy. This is achieved in one of two ways:

- ☑ In a forward proxy, traffic is routed to the CASB proxy by network devices (for office users) or by agents on each endpoint (for external users).
- ☑ In a reverse proxy, cloud applications are configured to guide traffic through the CASB proxy.

Proxy mode allows CASBs to implement very granular access controls.

Proxy mode also gives the CASB visibility into data in motion and allows it to enforce policies in real time. For example, the CASB can ensure that files being uploaded are encrypted, and can block the download of sensitive files to noncompliant devices. It can also generate alerts in real time, allowing security teams to react immediately to security incidents, policy violations, and anomalous behaviors.

However, proxy mode takes longer to implement. To route traffic to the CASB proxy, changes need to be made to network devices and endpoints (for forward proxy), or to applications (for reverse proxy). Also, some implementations of forward proxies require the installation of software agents on endpoint devices, which may be impossible with unmanaged devices. Further, some reverse proxies can break application functionality.

Hybrid mode

Some CASBs offer a hybrid mode that combines API mode and proxy mode. This allows the CASB to support a wide range of use cases with visibility, policy enforcement, and ways to deal with unmanaged devices.

We have only touched on a few of the key issues related to CASB deployment modes. Gartner has a useful report that goes into more depth. To purchase a copy of *Select the Right CASB Deployment for Your SaaS Security Strategy*, connect to: https://www.gartner.com/doc/3004618/select-right-casb-deployment-saas.

Integrating with Existing Security Solutions

Some of the features we have discussed require integration with existing security products. Not all CASBs offer the same integrations, so you should understand the options.

Directories and SSO solutions

Most CASBs integrate with enterprise directories, single sign-on (SSO) products, and other identity and access management (IAM) solutions. These integrations give the CASB access to additional information about users, such as their roles, departments, and business units. They can also help CASBs enforce corporate policies, such as:

- ☑ Requiring users to authenticate to cloud applications through an SSO solution, not directly over the web
- ☑ Blocking access to cloud applications as soon as a user changes roles or is terminated (*deprovisioning*)

Data loss prevention

Cloud DLP features allow a CASB to detect sensitive information in files and prevent those files from being downloaded to unmanaged devices, or from being downloaded at all. Some CASBs integrate with DLP products to leverage existing DLP policies and file classifications, allowing a single set of DLP policies to be enforced across cloud and on-premises datacenters.

Cloud NAC

A CASB can work with third-party cloud network access control (NAC) solutions. Endpoints that are unmanaged or non-compliant with corporate standards can be blocked from accessing cloud applications, or can be given restricted access and limited ability to download or share files.

Sandboxing

A CASB can work with a sandboxing product to test files in motion and files residing in cloud applications for malware.

Encryption and IRM

Integrating a CASB with encryption and information rights management (IRM) solutions can ensure that:

- ☑ Files uploaded to cloud applications are encrypted
- ☑ Files downloaded to unmanaged and other untrusted endpoints are encrypted
- ☑ Sensitive content cannot be printed, exported, copied, or retained for long on endpoints

Experts debate the relative merits of encrypting all data, or encrypting data at the field level or file level. For CASBs, file-level encryption tends to be the best option. Encrypting and decrypting all data creates excessive processing overhead. Encrypting data at the field level often breaks application functionality. For example, using a third-party solution to encrypt Salesforce fields can interfere with searching, as well as disrupting integration with other applications such as Marketo.

SIEM

All alerts generated by a CASB, together with related information (the context for the alert), can be pushed to security information and event management (SIEM) solutions. That allows the security operations center (SOC) and incident response (IR) teams to see CASB-created alerts immediately, correlate them with on-premises activities, prioritize them alongside other alerts, and respond to them using established workflows. It also gives them instant access to the contextual information collected by the CASB.

Phased Implementation

A CASB can be implemented in phases. A phased approach allows the enterprise to begin receiving a return on their investment immediately (usually on the first day) and evolve over time toward a comprehensive set of capabilities. Table 6-1 describes one possible sequence.

Phase	Functionality Added in Each Phase
1	Discovery and assessment of unsanctioned cloud applications
2	Visibility into users, applications, devices, and files; Enforcement of governance policies; Integration with IAM, DLP and SIEM tools; Alerts on security events, policy violations, and anomalous behaviors
3	Real-time enforcement of access control and compliance policies, including cloud NAC
4	Real-time enforcement of high-security use cases, including encryption and IRM policies

Table 6-1: Example of a phased implementation

Chapter 7

Selecting the Right Cloud Access Security Broker

In this chapter

- Review six areas you can use to compare CASBs.
- Learn questions that you should ask vendors.

"The best way to predict the future is to create it."

— Peter Drucker

Cloud access security brokers are a relatively new technology. Products differ widely in capabilities. In this chapter we highlight factors you should use to compare CASBs and select the one that best fits your organization.

Breadth of Application Coverage

Every cloud application is different, so some work is required to fully integrate a CASB with each new one. You should look at a CASB vendor's catalog of applications to:

- ☑ Determine if your current and planned cloud applications are on the list
- ☑ Assess the odds that the next application you want to monitor will be included
- ☑ Understand the vendor's process for supporting new applications

Discuss your special application-related requirements with the CASB vendor. For example, if you are going to put internally developed applications in a private cloud, find out the vendor's practices for integrating your homegrown applications with their CASB.

Depth of Security Controls

How granular are the security controls in the CASB? Factors to consider include:

- ☑ Adaptive access control: can the CASB make access decisions based on multiple criteria, including users, devices, user roles, IP addresses, and locations?
- ☑ Can compliance policies be enforced based on criteria like confidential information in files and the status of the endpoint accessing the application?
- ☑ Are data sharing controls available to ensure files and documents are being shared with external parties appropriately?
- ☑ Can alerts be generated based on a wide range of security incidents and policy violations?

Heuristics for Threat Protection

One of the highest priorities for security teams today is identifying advanced targeted threats before they can damage the enterprise. CASBs contribute to this effort by detecting anomalous behaviors and clues about cybercriminals probing and manipulating cloud applications. Ask CASB vendors about their heuristics engine and alerting capabilities. For example:

- ☑ How many variables are used to define normal usage?
- ☑ Can anomalies be detected at various levels, such as the entire company, groups within the company, and individual users?
- ☑ Can alerts be customized per user or per group (e.g., based on behaviors outside of the norm for the CEO, or for the finance department)?
- ☑ How does the vendor fine-tune heuristics and continue to improve the heuristics engine?

Deployment Modes

As we discussed in Chapter 6, there are trade-offs between deployment modes. Most importantly:

- ☑ API mode can be implemented quickly, requires no changes to infrastructure, and can enforce governance policies for data at rest, but it has limited ability to enforce security policies for data in motion.
- ☑ Forward proxy mode puts the CASB "inline" for access control and real-time policy enforcement, but it requires configuration changes on network equipment and mobile devices.
- ☑ Reverse proxy mode provides access control and real-time policy enforcement, and works with unmanaged devices, but can affect application functionality if it is not implemented properly by the CASB vendor.

Some organizations may find a CASB with one deployment mode that meets their needs. However, most enterprises are better served by a CASB that offers a hybrid architecture combining API mode with at least one of the proxy modes.

Integration with Security Solutions

Throughout this guide we have described how CASBs can be integrated with existing security solutions. However, CASBs differ widely in the type and number of integrations they offer. You should look for integrations that:

- ☑ Add to the access control capabilities of the CASB (e.g., determine if endpoints are managed and in compliance with policies)
- ☑ Protect documents throughout their lifecycle (e.g. use encryption and information rights management)
- ☑ Extend existing security policies and procedures to the cloud (e.g., enforce current DLP and compliance rules with the CASB)
- ☑ Provide existing security tools with insights into activities in the cloud (e.g., share log data and alerts with corporate SIEM systems)

Cyber Intelligence for Cloud Applications

Today's cybercriminals, hacktivists, and state-sponsored hackers are constantly devising new techniques to attack cloud applications and cloud application users. To keep up, a CASB vendor must monitor the web for new attackers, determine their tactics, techniques and procedures (TTPs), and devise new detection methods to counter those threats.

Ask vendors about their intelligence center or research lab: how is it staffed, and how do its experts work with product developers to build intelligence into the CASB?

Talk to reference customers. Has the CASB vendor been a good partner, an extension of the customer's security operations center? Does their intelligence center look for anomalous behaviors in the customer's environment, and accept queries about cloud application threats? Does the vendor provide regular assessments and recommendations on how to update policies and strengthen data protection?

Final Thought: Security Catches Up to the Cloud

There is no question that cloud-based applications multiply the challenges faced by enterprise security teams. They lose visibility into the applications, and lose control over devices and user behaviors. They risk fragmenting their security solutions into separate cloud- and premises-based silos.

Most enterprises are very close to a cross-over point where security will fall hopelessly behind current threats -- unless they find a way to extend visibility, threat protection, and policy enforcement to cloud applications.

Cloud access security brokers are an innovative response to these challenges. We hope you have found this guide an informative introduction to the topic, and will explore how a CASB can be used in your environment.

Protect your most sensitive data from damaging breaches

Make your most sensitive data useless to hackers. Encrypt it—at the moment it's created and throughout its lifecycle. HPE Security—Data Security protects your data at rest, in motion, and in use. On your site, in the cloud, and on mobile devices. Our continuous data-centric security keeps your business out of the headlines, and it helps you assure PCI compliance, data de-identification, and protection of personally identifiable information, personal health information, and intellectual property. HPE Security—Data Security encryption, key management and security solutions keep you ahead of hackers. Learn more at: HPE.com/go/DataSecurity

Hewlett Packard Enterprise

Cloud applications reduce costs and improve productivity.

But how do you monitor and protect your data in a cloud environment? How do you deal with lost visibility, unmanaged devices, and careless users? This guide explains how cloud access security brokers (CASBs) extend security to cloud applications, providing visibility, threat protection, access control, and compliance. See why you can't afford to move to cloud applications without a CASB.

- Cloud access security brokers — learn key characteristics and benefits of cloud access security brokers (CASBs)
- Visibility — review the types of data monitored by CASBs and the insights you can obtain from that data
- Threat protection — discover why CASBs can identify threats invisible to other security technologies
- Access control and compliance — examine how CASBs employ "adaptive access control" and enforce security policies
- Implementation — explore deployment modes and a phased approach to implementing a CASB
- Selection — find out how to choose the CASB that best fits your organization

About the Authors

Jon Friedman has more than 20 years of experience in industry analysis and marketing at software and IT services companies. He has explained the technologies of more than 40 high-tech companies. Jon has a BA from Yale and an MBA from Harvard. Mark Bouchard is a cybersecurity veteran with nearly 20 years of IT experience. A former industry analyst, Mark is also a proud veteran of the U.S. Navy.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9961827-1-3