Secure Cloud Services by Integrating CASB Based Approach

P. Arul Selvam

Department of CSE

Hindusthan College of Engineering and Technology

Coimbatore

ABSTRACT

In the last decades, cloud computing has attracted much attention in business, as it provides numerous computing functions (e.g., Software-as-a-Service (SaaS), Platform as-a-Service (PaaS) and Infrastructure-as-a-service (IaaS). Shadow IT refers to the use of cloud apps and services without the explicit approval of IT. Early on, the practice was one of the main drivers of Cloud Access Security Broker (CASB) adoption. There are two risks we found, they are i.) Users typically use unapproved software-as-a-service (SaaS) applications for file sharing, social media, collaboration and web conferencing. Ii.) Another growing challenge, third-party apps and scripts with OAuth permissions. OAuth-connected third-party apps access IT-approved cloud services, such as Microsoft 365 and Google G Suite. Some of these pose risks because of poor design, giving them broader than necessary data permissions. The danger of OAuth is once a token is authorized, access to enterprise data and applications continues until it's revoked—even if the user's password is changed. Integrating CASB solution into broader web security infrastructure can provide deeper visibility into all unapproved web apps.

Keywords: cloud computing, insider threats, web security, CASB, OAuth

1. INTRODUCTION

CASBs can help you address the complexities of cloud security—especially if they take a people-centric approach. They can help you strengthen your security posture by safeguarding your people and your data from advanced threats, prevent data loss and maintain compliance, and control access to SaaS apps. Let's explore three critical CASB use cases: i) Cloud thread protection, such as such as ransomware, intelligent brute force attacks and advanced phishing campaigns. ii) Cloud data security and compliance, such as insider risks and accidental data leakage. iii) Cloud app governance, such as third-party OAuth applications and shadow IT.

Today's attacks target people, not technology. This is just as true for the cloud as it is on premises. As businesses move their messaging and collaboration platforms from the corporate network to the cloud, they become vulnerable to attack. A CASB with a broad complement of security solutions with robust detection, remediation and risk-based authentication capabilities offers the best defense against today's people-centric threats, including brute-force attacks, phishing attacks, malicious file shares and malicious OAuth apps or OAuth abuse.

Automated tools are used to come up with multiple combinations of usernames with passwords exposed in large credential dumps. These are lists of email addresses, passwords and other information published online after a breach. Attackers can even bypass multi-factor authentication by leveraging legacy email protocols, such as Internet Message Access Protocol (IMAP). This common protocol is used to access email on different devices from the email server and is especially susceptible to cloud attacks.

Ransomware is one of today's most disruptive forms of cyber-attack. With just a single username and password—especially for cloud apps such as Microsoft 365 or Google Workplace—a ransomware operator can launch attacks inside and outside of your organization. CASB controls can be a key defense by: i) Monitoring and detecting compromised cloud accounts ii) Monitoring for malicious file uploads to cloud accounts iii) Protecting from command and control with web security iv) Limiting network access with zero-trust access controls.

Research shows that more than 31% of organizations or groups using cloud services experienced account compromise that started with phishing campaigns. To cover their tracks, attackers sometimes leverage virtual private networks (VPNs) or TOR nodes, which preserve a user's privacy and identity. Email account compromise (EAC) and business email compromise (BEC) are forms of phishing that target businesses and people who perform wire transfer payments or have access to confidential employee data, such as W-2 tax forms. Cyber criminals typically pose as executives or business partners to prey on victims' trust.

Threat actors also distribute malware via cloud services like Dropbox. They leverage these platforms mainly because they are unlikely to be blocked by IT security because nearly everyone uses them. Customer support teams are especially at risk, as they may open malicious files shared by threat actors who impersonate customers.

As people share and store more of your corporate data in the cloud, the possibility of a breach increases. Malicious activity and even well-intentioned oversharing of content by users can put data at risk. To prevent data loss and breaches, it's critical to monitor and govern how people use data across cloud apps and multiple channels.

Half of all reported data breaches result from malicious attacks caused by attackers or criminal insiders (employees, contractors or other third parties). About 19% were due to compromised credentials and another 19% stemmed from cloud misconfigurations. When you move data to the cloud, compliance with government regulations and industry mandates becomes more difficult than ever before. Compliance requirements are constantly changing, with a growing emphasis on data security, privacy and sovereignty.

A robust, advanced CASB solution can help you define and implement policies that govern how, when and where your people can access your vital corporate data. CASB policy parameters should include user roles, risks associated with the login and contextual information such as user location, device health and others. To get started, study how data is handled by cloud apps and understand organization's specific data security objectives and use cases for data identification, file remediation, forensics and reporting. The right CASB solution should allow you to deploy cloud Data Loss Prevention (DLP) policies consistent with those for email and on-premises file repositories. It should also be able to integrate with other DLP solutions and enable you to unify incident management.

In today's cloud-first world, governing your users' access to both IT-authorized and unauthorized apps (shadow IT) has never been more important. The average enterprise has an estimated 1,000 cloud apps in use. And some of these have serious security gaps that can potentially put organizations at risk and violate compliance regulations and mandates. An example is users granting broad OAuth permissions to third-party apps. This inadvertently violates data residency regulations, such as General Data Protection Regulation (GDPR). In addition, attackers often use third-party add-ons and social engineering to trick people into granting broad access to your approved SaaS apps.

A CASB solution helps you govern the cloud apps and services your people use by offering a centralized view of your cloud environment. It allows you to get insights into who is accessing what apps and data in the cloud from where and from which device. CASB catalog cloud services (including third-party OAuth apps) rate the risk level and overall trustworthiness of cloud services and assign them a score. CASBs even provide automated access controls to and from cloud services based on cloud service risk scores and other parameters, such as app category and data permissions.

An OAuth app is an application that integrates with a cloud service and may be provided by a vendor other than the cloud service provider. These apps add business features and user-interface enhancements to cloud services such as Microsoft 365 and Google Workspace. Most OAuth apps request permission to access and manage user information and data and sign into other cloud apps on the user's behalf. For example, they can access users' files, read their calendars, send emails on their behalf and more. These add-on apps use OAuth authentication to obtain limited access to cloud services. Unfortunately, OAuth apps can easily be exploited. Attackers can use OAuth access to compromise and take over cloud accounts. Until the token is explicitly revoked, the attacker has persistent access to the user's account and data.

2. WORK FLOW

In this paper, we discuss in detail three critical CASB use cases: i) Cloud thread protection, such as such as ransomware, intelligent brute force attacks and advanced phishing campaigns. ii) Cloud data security and compliance, such as insider risks and accidental data leakage. iii) Cloud app governance, such as third-party OAuth applications and shadow IT.

2.1 Cloud Threat Protection

The CASB model identifies risky users who are highly targeted or have access to critical systems or data and it provides accurate detection of cloud account compromise through machine learning and threat intelligence. The proposed model sends alerts when account compromise or post-compromise activity is detected. Deletes or quarantines malicious files automatically upon detection. Reverts file sharing permissions and removes malicious files. Removes delegates and email forwarding rules. Removes OAuth tokens.

The CASB model Controls access via conditional access rules, such as safe listing and/or block listing countries, networks or IP reputation (example: TOR nodes).

Controls access based on users and groups, such as privileged users with access to critical systems or sensitive data (example: IT administrators), highly targeted persons (example: HR managers) and VIPs (example: board members). Prevents risky access based on known threat actor footprints such as IP addresses, user agents and other indicators of compromise. Enforces step-up authentication policies and limits access levels for off-network devices or based on device health.

2.2 Cloud Data Security and Compliance

Here's a list of data-protection and compliance capabilities to look for when considering a CASB solution. CASB based approach, discovers sensitive data in both SaaS and IaaS services. Detects sharing permissions for public, external, internal and private files and folders. Identifies regulated data (PCI, PII, FINRA, HIPAA and GDPR) to assess compliance risks using out-of-the-box and advanced data loss prevention technologies. Pinpoints who in your organization has access to sensitive cloud data.

CASB based approach, alerts security teams when data exfiltration after account compromises, malicious insiders activity and other data security violations occur. Integrates current DLP policies across email, endpoint, on-premises file shares, cloud and web. Identifies users sharing sensitive data too widely. Applies adaptive prevention controls around file sharing and data exfiltration, such as blocking data exfiltration and quarantining, deleting or revoking broad share permissions for sensitive files. Automates policy enforcement for file uploads, downloads, collaboration, and messaging in the cloud through rules based on context: user, user group, location, device, IP, file properties and DLP policies. Identifies malicious user activity in the through user behaviour analytics. Integrates with insider threat management and enterprise DLP solutions to protect from malicious and negligent insiders across cloud, email and endpoint.

CASB based solution, prevents access to block-listed cloud apps while allowing access to those that meet your security guidelines. Monitors and limits access to tolerated cloud apps using contextual policies (example: allow only the HR department to access HR applications or limit VAPs access to tolerated apps based on risk). Integrates cloud DLP incident triage and reporting with those capabilities for other DLP channels, such as email, endpoint and on-premises data stores. Integrates with security information and event management and IT service management platforms like ServiceNow to capture alerts for file-handling policies, DLP violations and response actions.

2.3 Cloud App Governance

Here's a list of cloud-app governance capabilities to look for when considering a CASB solution. CASB based approach, discovers cloud services in use and catalogs them by ingesting network traffic logs automatically from firewalls, and secure web gateways such as Zscaler, Palo Alto Networks, Checkpoint and others. Detecting and assessing OAuth permissions for third-party apps that access cloud apps like Microsoft 365 and Google Workspace. Detects the number of users and data traffic for cloud services. Identifies who in your organization is accessing which cloud services. Assesses cloud service security risks and compliance gaps and assigns a risk score to each service. Identifies files uploads and downloads and the user involved.

In CASB based approach after detecting malicious activities, provides alerting and coaching capabilities for end users. Provides compliance reporting capabilities. Applies cloud governance policies and automates controls for cloud access such as "allow," "read-only" or "block" based on app risk score and app category. Revokes OAuth permissions for third-party apps based on severity of risk, app scope, category and other characteristics, such as user/groups. Controls file uploads to and downloads from unapproved cloud applications by leveraging web isolation and DLP technologies to protect users from threats and data loss.

Gets visibility and control over shadow IT and web apps with security service edge (SSE) integrations. Offers added data protection by integrating Proofpoint Enterprise DLP, Proofpoint Insider Threat Management.

3. IMPLEMENTATION

CASBs can be deployed in a number of configurations, such as forward proxy, reverse proxy or using API mode. In this paper, deployment of CASB uses out-of-band application programming interfaces (APIs) to receive and analyze cloud traffic data such as log events, data files, user activity and more. The CASB enforces security policy and remediates access issues with features such as revoking user sessions, revoking OAuth tokens, suspending user accounts, forcing users to change their password, reducing file sharing permissions.

4. CONCLUSIONS

Security is a key part of cloud-first business transformation. To fully defend organization in the cloud, we need to address threat protection, data security, and app governance. A people-centric CASB solution accounts for who is most attacked, who is vulnerable to attacks, and who has privileged access to sensitive corporate data.

This level of visibility and control enables you to keep threats at bay, protect your information assets and stay compliant. Proofpoint provides the only CASB to meet the needs of security people serious about cloud threats, data loss and time-to-value. Proofpoint CASB is built on an agentless cloud security architecture. It protects your most valuable cloud assets and accelerates your migration to the cloud.

With Proofpoint CASB, you can extend people-centric threat visibility and adaptive controls to cloud apps.

REFERENCES

[1] “Getting Started with CASB\ E-BOOK”, Gartner. “2020 Gartner Magic Quadrant for CASB.” October 2020.