# CASB's New Data Protection Role in a SaaS World

## Securing data, blocking threats, and reducing misconfiguration risk

*By Toph Whitmore, Industry Director, Cybersecurity*

FROST & SULLIVAN VISUAL WHITEPAPER

# CONTENTS




# INTRODUCTION

**Conceived over a decade ago, Cloud Access Security Broker (CASB) technology was originally envisioned as the security enforcement point for data exiting the protective perimeter of an enterprise's internal network.**

How times change: The cloud, once a novelty exploited for specialized use, is now where enterprise work gets done, a platform enabling organizational growth. **Changes in platform, connectivity, and workplace have stretched CASB technology to the limits of its security efficacy.**

Today, CASB still delivers security indispensable to the modern enterprise. For one, it serves as a management window into how employees use the cloud. But many CASB solutions lack comprehensive functionality to support the new way of work. CASB and enterprise security must continue to evolve to secure the hybrid workplace.[1]

Modern work is done in the cloud. **Enterprise Software-as-a-Service (SaaS) application adoption has, in particular, raised CASB's profile.** It has highlighted the risk and cost associated with SaaS platform misconfiguration. And it has also formalized CASB's role in an integrated Secure Access Service Edge (SASE) enterprise platform.

1 Frost & Sullivan. (2022, June 9). *Insights for CISOs—Cloud Access Security Broker (CASB).*

# The Enterprise Shift to the Cloud Demands New Security, Connectivity Approaches

Whether for data or applications, cloud is the present and future of enterprise work.

**Enterprise IT leaders and strategic decision makers view cloud as a cost of doing business, as a platform necessary to enable growth:**

*Importance of Technologies to Achieve Business Priorities, Global, 2022*

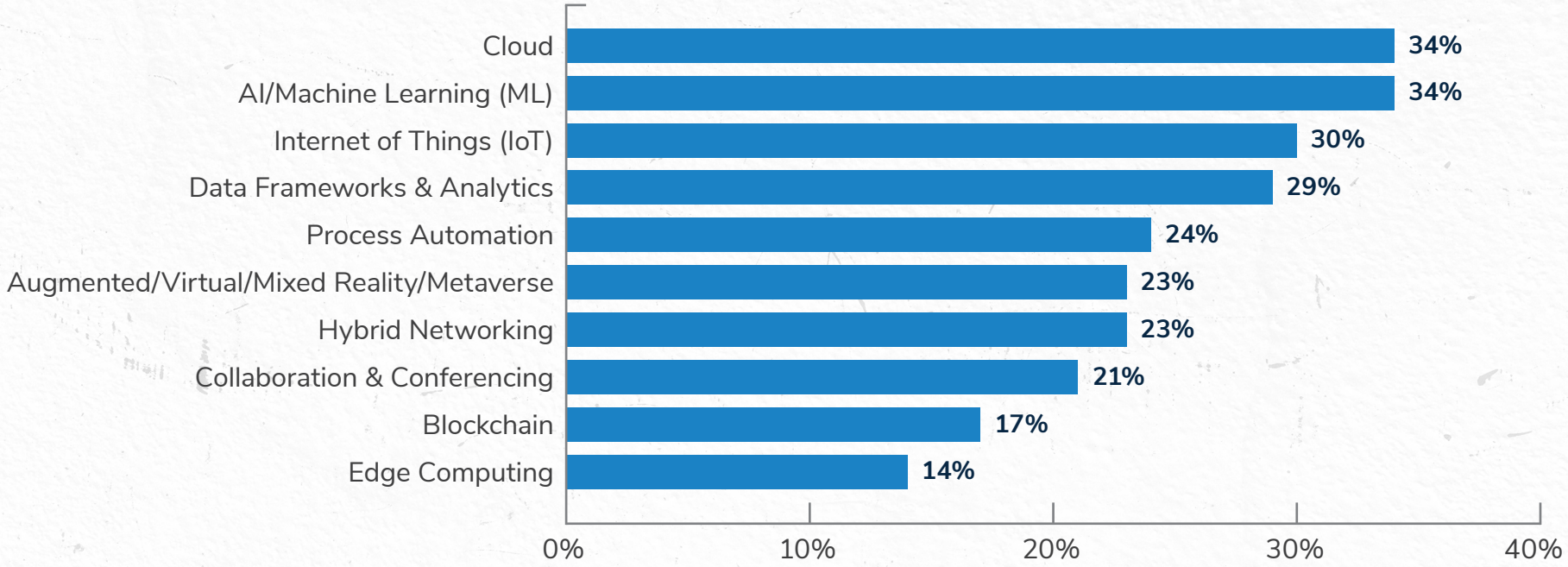


*Exhibit 1: In a recent survey, 894 enterprise IT leaders and decision makers were asked what technologies they would be investing in during the coming 12 months. They prioritized cloud as critical to business success.*

Source: Frost & Sullivan. (2022, November 29). The State of the Cloud: The Importance of Hybrid and Multicloud Environments for Business Success.

# The New Way of Work, Brought to You by the Cloud

The modern enterprise has committed to cloud (and hybrid cloud, and multicloud) environments. Some key findings from a recent survey of enterprise IT leaders:

- Nearly three-quarters polled say "a successful, competitive business requires a strategic, seamless hybrid or multicloud environment."
- Some enterprises keep *some* apps on premises because of "security, resiliency, or sustainability concerns," but legacy infrastructure usage is dropping.
- Seventy percent of those surveyed have adopted a cloud-first approach for all new applications.
- SaaS adoption continues to supplant traditional infrastructure. "Replace the app with a cloud-native application" is the second-most popular strategy for upgrading legacy applications.[2]

The way of work has changed: It's cloud-first, device-agnostic, and remote. Employees work at branch offices, while traveling, or in a Starbucks. They connect to corporate resources from business-issued laptops, shared operational systems, or their own smartphones. They are inside the network perimeter, on the open internet, or in the cloud. It's hard to envision a scenario dictating a return to the 1980s-like office, yet many enterprises continue to try to protect employee work with decades-old security models.[3]

With work environments so extended, **the center of enterprise data gravity has shifted from the data center to the cloud.** Users need to connect to get their work done. To them, whether a resource is private or public is unimportant. They just need to use it. Employees should not have to care where an app resides, whether it's hosted on the open internet or housed in the corporate data center.[4]

With work environments so extended, the center of enterprise data gravity has shifted from the data center to the cloud.

2 Frost & Sullivan. (2022, November 29). The State of the Cloud: The Importance of Hybrid and Multicloud Environments for Business Success.
3 Frost & Sullivan. (2023, publication pending). Global Security Service Edge (SSE) Market, 2023.
4 Frost & Sullivan. (2022, October 31). Insights for CISOs —The Big 12 Business Considerations for Cloud Zero Trust Architecture Adoption.

# It's 10 P.M. Do You Know Where Your Employees Are... in the Cloud?

Extending the enterprise work environment into the cloud introduces new security risks:

- Data is more difficult to track, let alone protect. It lives everywhere—on devices, in the data center, on the internet.
- Security leaders may have little to no influence over third-party SaaS application use within the company. App usage, visibility, and management now typically lie outside enterprise control.

In traditional managed application environments, CISOs oversaw application use within the confines of the enterprise and, specifically, within the enterprise's data centers. **Security priorities haven't changed with the advent of the cloud, but** where **security must be applied has.** CISOs must secure both cloud data and SaaS apps. They must understand employee SaaS app usage—what apps employees are using and how. And they have to do all that across a working environment that extends from the corporate network out to the cloud.

Security priorities haven't changed with the advent of the cloud, but where security must be applied has. CISOs must secure both cloud data and SaaS apps.

# Meanwhile, Threat Actors Seize the Day

In February 2023, Canadian retailer Indigo Books & Music's website went down. What at first seemed like a minor outage was soon confirmed to be a highly effective cyberattack. Across Canada, Indigo stores switched to cash-only transactions. The company's eCommerce site went down … and stayed down. A group taking credit for the attack threatened to release employee data to the dark web. Indigo frantically built a new website and was able to restore limited online sales … three weeks after the hack, missing out completely on the lucrative Valentine's Day holiday selling period.

Indigo's experience is just one example of a rather obvious truism: **Cyberthreats are more ominous and attacks are more damaging.** Recent Frost & Sullivan research examining threats to industrial targets highlighted the extent to which threat actors are identifying and then capitalizing on enterprise blind spots. Attacks are more frequent, more sophisticated, more damaging, and better subsidized.[5]

**Extending the enterprise work environment makes it easier for employees to do their work. But it also extends the attack surface into the cloud (or clouds), making it harder for security leaders to protect their employees' work.** Current solutions—including CASB—were never designed for such complex environments. They cannot effectively protect against new threats, particularly those that target vulnerabilities introduced by SaaS use and data in the cloud.

5 Frost & Sullivan. (2022, January 18). *Increasing Sophistication of Attacks and Evolving Threat Landscape Powering Global Industrial Cybersecurity, Outlook 2022.*

# From Enforcement Point to Posture Management: Understanding the Past and Future of CASB

CASB functionality has traditionally acted as a policy enforcement point between cloud service users. As SaaS adoption has increased, CASB's importance (and prominence) has only grown.

CASB was originally created to address the challenge of shadow IT use. Companies adopted it to gain visibility into the cloud applications and services used in the organization without explicit approval.

CASB has evolved over the years and vendors have added many features to their products. Besides the frequently offered functions such as Single Sign-On (SSO), credential mapping, device profiling, encryption, and tokenization, some vendors may also include next-generation Data Loss Prevention (DLP), Cloud Security Posture Management (CSPM), User Behavior Analytics (UBA), adaptive access control, and other features. These functionalities can improve the efficacy of CASB offerings by enhancing its primary functions:[6]

6 Frost & Sullivan. (2022, June 9). *Insights for CISOs—Cloud Access Security Broker (CASB).*

## VISIBILITY

CASB can discover all cloud services that users are accessing, including shadow IT. As it monitors data flows, it can provide useful information about cloud spending and risks, as well as management capabilities.

## COMPLIANCE

CASB enforces policies that comply with both internal and external regulations (government and/or industry-specific). This protects companies from costly data breaches.

## THREAT PROTECTION

CASB offers protection against attacks that start in cloud services—or that can be spread by them. It can identify, mitigate, and remediate threats in real time.

## DATA SECURITY

CASB enforces data-centric security policies. Features such as encryption, tokenization, and DLP are essential to understand whether data is being shared outside the organization and how it is being handled.

## ACCESS CONTROL

CASB controls access for authorized and unauthorized users based on identity, activity, and application accessed. Organizations can then avoid banning all services with a one-size-fits-all approach.

**PERFORMANCE**
CASB cannot introduce latency nor impact user experience.

*Exhibit 2. The five pillars—and performance mandate—of CASB.*

Source: Frost & Sullivan. (2022, June 9). Insights for CISOs—Cloud Access Security Broker (CASB).

# SaaS Application Adoption Raises Misconfiguration Risk, Elevates SSPM Need

Cloud-based SaaS application adoption changes the nature of both enterprise security and risk.

- The enterprise work environment extends beyond the data center and into the cloud.
- It introduces a different control dynamic: To at least some extent, and with virtually every application, the enterprise cedes some level of security control to the SaaS vendor.
- The more SaaS applications in use, the higher the risk of misconfiguration.

Cloud apps and services allow employees to get their jobs done quicker, easier, and with greater flexibility than traditional computing tools. But **when data is taken outside of an organization's security perimeter, it exposes the organization to risk**.[7]

In the modern enterprise, security must be built into every strategic workflow. That includes cloud application management. But gauging threat posture in a cloud, hybrid cloud, or multicloud environment requires security leaders to understand SaaS app configuration risks, including unauthorized application access, weakened identity management, and even security policy bypass. Those responsible for SaaS app configuration must be knowledgeable about security specific to the enterprise work environment. Misconfiguration is both an enterprise risk and potential liability: It's like locking the front door but forgetting to close the windows.

Application security configuration management is difficult enough as it is. But when those apps are distributed in, served from, and used in the cloud, identifying and rectifying misconfiguration gets complicated. For that reason, ensuring that enterprise SaaS use remains secure is within the (new) realm of CASB.

**CASB is evolving to include SaaS Security Posture Management (SSPM).** SSPM is the catch-all term for management configuration functionality associated with securing SaaS application use in an enterprise.

Beyond brokering connections and enforcing policy, CASB must now be entrusted with preventing misconfiguration (and reducing risk associated with it). In that way, CASB automates and simplifies SaaS app configuration, providing greater administrative visibility into enterprise SaaS app usage. Beyond that functionality, assessing SSPM can come down to a straightforward equation: the more SaaS applications a CASB solution supports, the better the security management outlook for an enterprise CISO.

7 Frost & Sullivan. (2020, October 5). Accelerating Migration to the Cloud Transforming the Global Cloud Access Security Broker (CASB) Market, 2024.

# Modern Enterprise Work Requires Modern CASB in a Modern SASE/SSE Platform

The new way of work is in the cloud. But "SaaS sprawl" introduces new threats to enterprise security, complicates day-to-day application management, moves data from on premises to the cloud, and cedes security control to third parties. CASB—that is, next-generation CASB (NG-CASB) equipped with robust SSPM capabilities—is integral to enterprise security, particularly within a comprehensive security suite.

**CASB is most effective when integrated into a platform or comprehensive security architecture.**[8] Security Service Edge (SSE) solutions (standardized by the US National Institute for Standards and Technology [NIST] as Cloud Zero Trust Architecture [ZTA] solutions) offer a combination of cloud-edge-delivered cybersecurity services and cloud-brokered connectivity. CASB is one of the cornerstone features of SSE and SASE architectures, so CISOs should have a clear understanding of this solution. A ZTA-compliant (SSE) solution includes CASB, Zero Trust Network Access (ZTNA), and Secure Web Gateway (SWG) features as fundamental security components, protecting user connectivity to the cloud, to private resources, and to the open internet. (SASE adds SD-WAN capability.)[9] CASB's inclusion in SASE/SSE platforms is due in part to customers who demand the simplified administration of integrated cybersecurity solutions.[10]

CASB is most effective when integrated into a platform or comprehensive security architecture.

8 Frost & Sullivan. (2020, October 5). *Accelerating Migration to the Cloud Transforming the Global Cloud Access Security Broker (CASB) Market, 2024.*
9 Source: Frost & Sullivan. (2023, publication pending). *Global Security Service Edge (SSE) Market, 2023.*
10 Frost & Sullivan. (2022, June 9). *Insights for CISOs—Cloud Access Security Broker (CASB).*

# The Modern Workplace Requires NG-CASB for Securing SaaS, Enabling Growth


In a cloud-first world dominated by SaaS applications and cloud data storage, data protection in the form of **CASB functionality must evolve**.

Effective CASB solutions provide enterprise visibility into cloud application use, support regulatory compliance, offer threat protection, enforce data security policies, and control cloud application access, ideally without introducing performance latency.

Cloud platform and application adoption stretches the enterprise security landscape. New hybrid ways of work further complicate cloud security management.

**"CASB 1.0" may be the present, but the (rather immediate) future is next-gen CASB that supports SSPM and integrates into SSE/SASE platforms.**

# THE GROWTH PIPELINE COMPANY

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion

FROST & SULLIVAN