

LEARNING MADE EASY

Palo Alto Networks Special Edition

# Next-Generation CASB

for  
**dummies**<sup>®</sup>  
A Wiley Brand



Discover shadow  
IT apps

Mitigate SaaS app  
security risks

Prevent sensitive  
data loss

Brought to you  
by



Lawrence Miller, CISSP

# About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2022, 2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit [www.paloaltonetworks.com](http://www.paloaltonetworks.com).

# Next-Generation CASB

**for  
dummies®**  
A Wiley Brand



# Next-Generation CASB

Palo Alto Networks Special Edition

**by Lawrence Miller, CISSP**

for  
**dummies**<sup>®</sup>  
A Wiley Brand

# Next-Generation CASB For Dummies®, Palo Alto Networks Special Edition

Published by  
**John Wiley & Sons, Inc.**  
111 River St.  
Hoboken, NJ 07030-5774  
[www.wiley.com](http://www.wiley.com)

Copyright © 2024 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

ISBN 978-1-119-93368-7 (pbk); ISBN 978-1-119-93369-4 (ebk)

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact [info@dummies.biz](mailto:info@dummies.biz), or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For information about licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com).

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Editor:** Elizabeth Kuball  
**Acquisitions Editor:** Traci Martin  
**Editorial Manager:** Rev Mengle

**Client Account Manager:**  
Cynthia Tweed  
**Production Editor:**  
Tamilmani Varadharaj

# Table of Contents

**INTRODUCTION** ..... 1

- About This Book ..... 1
- Foolish Assumptions ..... 2
- Icons Used in This Book..... 2
- Beyond the Book..... 3

**CHAPTER 1: Looking at the Modern Cybersecurity Landscape**..... 5

- Recognizing Current Trends..... 5
  - Cloud-driven enterprise digital transformation ..... 5
  - Work from home and remote/hybrid workforces ..... 6
  - The explosive rise and adoption of SaaS ..... 6
- Conventional CASBs Can't Keep Up with New SaaS Challenges..... 8
  - The shadow IT conundrum..... 8
  - Uncontrolled access from anywhere on any device..... 9
  - Data protection issues for structured/unstructured data ..... 10
  - Lack of automation in incident management and remediation ..... 11
  - Misconfiguration issues ..... 11
  - Suspicious user activity ..... 12

**CHAPTER 2: Understanding the CASB Solution Architecture**..... 13

- What Is a CASB? ..... 13
- Comparing Past and Present CASB Solutions..... 14
- Looking at the Next-Generation CASB Architecture ..... 16
  - Multimode ..... 16
  - API-based ..... 16
  - In-line controls ..... 16
  - Data loss prevention ..... 17

**CHAPTER 3: Exploring Must-Have Capabilities and Features in Next-Generation CASBs** ..... 19

- Visibility of Sanctioned and Unsanctioned SaaS Apps..... 20
- SaaS Data Protection ..... 21
- Incident Response..... 22
- Threat Prevention..... 22

	Granular In-Line Controls.....	23
	Suspicious User Activity.....	23
	SaaS Security Posture Management.....	24
<b>CHAPTER 4:</b>	<b>Mitigating SaaS App Risks.....</b>	<b>25</b>
	Starting with Discovery and Control .....	25
	Getting Visibility into Data Flows .....	26
	Educating Users on Risky Data Usage .....	28
	Preventing Threats in SaaS Apps.....	28
	Controlling Tolerated Apps versus Unsanctioned Apps.....	29
	Monitoring and Preventing Risky User Behavior.....	29
	Ensuring the Best Security Posture on Corporate SaaS Apps .....	30
<b>CHAPTER 5:</b>	<b>Ten (or So) Things to Look for in a Next-Generation CASB.....</b>	<b>31</b>
	Cloud Scale.....	31
	Simple Deployment.....	32
	Detection of Known and Unknown Threats.....	34
	Comprehensive Data Protection and Compliance.....	34
	Integrated and Consistent Security across All Locations .....	36
	<b>Glossary.....</b>	<b>37</b>

# Introduction

The hybrid workforce — where employees can now work seamlessly from corporate offices, branch offices, home offices, or on the road — has dramatically changed how and where business is done. To enable this new work environment, modern businesses have rapidly increased their adoption of software as a service (SaaS) applications to bolster productivity and increase agility. Employers and employees have become increasingly dependent on a host of mission-critical collaboration SaaS applications, like Confluence, Jira, Microsoft Teams, Slack, and Zoom.

SaaS applications provide tremendous convenience to end users and are key enablers in driving business continuity and productivity. But SaaS applications continue to change the way organizations do business; their exploding numbers create security concerns that organizations must address.

Reducing security risks in SaaS applications, where organizations' most sensitive data often resides, is key to securing the cloud-led enterprise IT of the future. A next-generation cloud access security broker (CASB) can help address modern enterprise requirements to keep your mission-critical SaaS applications and sensitive data secure.

## About This Book

*Next-Generation CASB For Dummies*, Palo Alto Networks Special Edition, consists of five chapters that explore the following:

- » The modern cybersecurity landscape and the limitations of conventional CASB solutions (Chapter 1)
- » The key components of a next-generation CASB solution architecture (Chapter 2)
- » The essential capabilities and features of next-generation CASB (Chapter 3)



- » How next-generation CASB mitigates SaaS application and data risks (Chapter 4)
- » Important things to look for in a next-generation CASB (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest, feel free to jump ahead to that chapter. You can read this book in any order that suits you (though we don't recommend upside down or backward).

There's also a helpful glossary in case you get stumped by any terms or acronyms used in this book.

## Foolish Assumptions

It has been said that most assumptions have outlived their usefulness, but I assume a few things nonetheless!

Mainly, I assume that you're a decision-maker or a security practitioner and you're looking for an innovative solution to secure SaaS applications and data for your hybrid workforce. Whether you're a chief information security officer (CISO), an IT manager, or a cloud architect, this book shows you how next-generation CASB can help you address the challenges of modern SaaS and the hybrid workforce.

If any of these assumptions describes you, then this is the book for you! If none of these assumptions describes you, keep reading anyway. It's a great book and after reading it, you'll know quite a bit about SaaS security and next-generation CASB.

## Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:



REMEMBER

The Remember icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin.



TECHNICAL  
STUFF

The Technical Stuff icon explains the jargon beneath the jargon and is the stuff legends — well, legendary nerds — are made of.



TIP

Tips are appreciated, but never expected, and I sure hope you'll appreciate these useful nuggets of information.



WARNING

The Warning icon points out the stuff your mother warned you about. (Well, probably not, but it does point out practical advice.)

## Beyond the Book

There's only so much I can cover in this short book, so if you find yourself at the end of this book wondering, "Where can I learn more?," go to <https://paloaltonetworks.com/network-security/next-gen-casb>.

- » Exploring digital transformation, work-from-home, and SaaS trends
- » Understanding the limitations of conventional CASBs

# Chapter 1

# Looking at the Modern Cybersecurity Landscape

In this chapter, you explore modern trends, including enterprise digital transformation, work from home and work from anywhere, and software as a service (SaaS) adoption and how these trends are evolving the cybersecurity landscape. You'll also learn why traditional cloud access security broker (CASB) products are unable to keep up with this rapidly changing landscape.

## Recognizing Current Trends

The modern cybersecurity landscape is being reshaped by fast-paced changes that enable business agility and competitive advantage, but introduce significant challenges for IT and security that can no longer be effectively managed with traditional processes and technologies.

### Cloud-driven enterprise digital transformation

Modern enterprises are focused on digital transformation initiatives that maximize efficiency and business productivity while

reducing time to market to maintain their competitive edge and remain relevant in their respective industries.

Many enterprises leverage cloud-based technologies, including SaaS applications, to help them achieve their digital transformation objectives by enabling simplified management and consumption, ubiquitous availability, and ease of use, among other advantages of cloud services.

## **Work from home and remote/hybrid workforces**

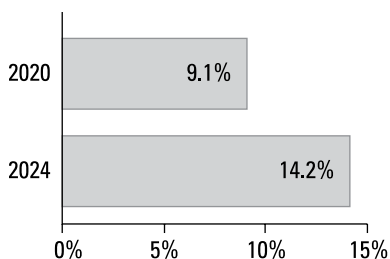
The emergence of the *hybrid workforce* — where employees can now work fluidly from corporate offices, branch offices, home offices, or on the road — has dramatically changed how and where business is done. The COVID-19 pandemic accelerated this hybrid workforce trend and intensified SaaS adoption worldwide. In 2020, the overall spend per company on SaaS applications increased by 50 percent, and the number of unique sanctioned SaaS apps in use per company went up by 30 percent year over year.

To adapt to this new environment, businesses have increased their appetite for SaaS apps to bolster productivity and increase agility. As a result, employers and employees have become increasingly dependent on a host of mission-critical SaaS-based collaboration apps, like Confluence, Jira, Microsoft Teams, Slack, and Zoom, among others.

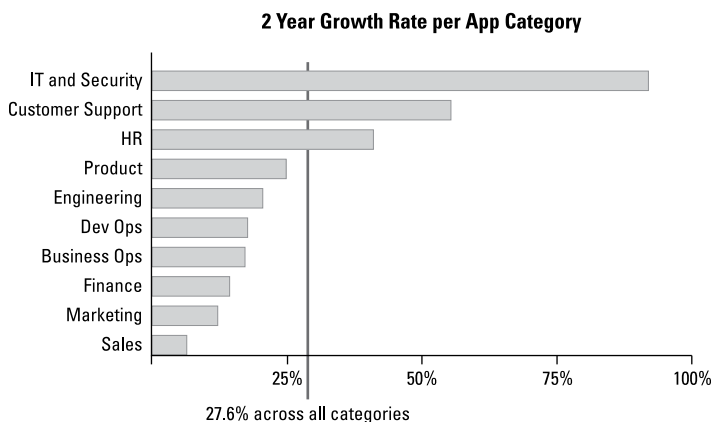
## **The explosive rise and adoption of SaaS**

Widespread adoption of cloud-delivered SaaS products such as Google Workspace, Microsoft 365, Salesforce, Zoom, and many others continues to grow. As the first cloud-based service to truly take off and proliferate the enterprise, SaaS has a significant lead on infrastructure as a service (IaaS), platform as a service (PaaS), and other cloud offerings. According to Gartner, SaaS is expected to maintain its dominance as the largest market segment in worldwide IT spending through 2024 (see Figure 1-1).

According to Blissfully's 2020 SaaS Trends report, SaaS applications are also increasingly being used by nearly every business function across the organization including IT and security, customer support, human resources, product engineering, DevOps, finance, marketing, and sales (see Figure 1-2).




**FIGURE 1-1:** Projected increase in cloud spend in the global enterprise IT spending market by 2024.



**FIGURE 1-2:** SaaS applications span many departments across the enterprise.

As SaaS proliferates across all these business functions, it also means that its ownership and management are becoming increasingly distributed. The often decentralized nature of enterprise SaaS adoption is causing IT teams to struggle with tracking, evaluating, maintaining, and protecting all SaaS apps in use by the organization. According to Blissfully’s 2019 SaaS Trends report, the typical enterprise uses hundreds of sanctioned SaaS apps that lead to thousands of app-to-people connections — all of which need to be secured (see Figure 1-3).



SaaS Statistic (per company)	Overall	Enterprises	Medium-level companies	Small-level companies
Spend	Up by 50%	\$4.16M	\$2.47M	\$202K
Unique SaaS apps	137	288	185	182
App to person connections	—	21,580	4,406	624
SaaS app churn	30%	46%	29%	35%
# of duplicate apps	3.6	7.6	5.8	2.3
# abandoned app subscriptions	2.6 (up by 100%)	7.1	4.3	1.4
# of billing owners per company	—	98	32	10

**FIGURE 1-3:** SaaS spend and usage statistics by market segment in 2020.

## Conventional CASBs Can't Keep Up with New SaaS Challenges

The cloud offers tremendous advantages, but the explosive growth in the number and types of SaaS apps now in use, as well as the reliance on modern collaboration tools, poses significant security risks to companies.

CASBs are vital to modern enterprise security for securing cloud-based applications and the sensitive data that flows through them. However, current first-generation CASB solutions present significant limitations.

### The shadow IT conundrum

Employees can directly access a myriad of SaaS applications without having to go through their company's network — often without the IT department knowing — leading to a lack of visibility into, or control over, application usage and risk.

The risks of shadow IT have increased substantially with remote employees working from home on unsecured networks. Many employees circumvent the corporate virtual private network (VPN) to access these apps directly. If personal, unmanaged devices are used to access company resources, shadow IT becomes significantly more challenging to detect and prevent.



WARNING

Shadow IT creates many hurdles for IT and security organizations, including the following:

- » **Shadow IT doesn't allow IT teams to administer centralized control over data security.** IT has no centralized control over what sensitive and proprietary business data gets dispersed across thousands of unvetted and unsanctioned cloud services and applications. The unmanaged repositories of data residing outside the organization's established security boundaries results in explosive growth of the enterprise attack surface.
- » **Shadow IT goes against an organization's data compliance requirements.** Shadow IT is not managed by the IT team, so they have little to no visibility into the compliance ramifications of these unapproved apps and the data being processed, transferred, or stored in these apps. Shadow IT creates the burden of additional regulatory audit points, where proof of compliance must be expanded.
- » **Shadow IT leads employees away from prescribed security best practices.** Most of the time, employees' motivations for using shadow IT apps are not malicious or negligent, but despite employees' best intentions, shadow IT poses serious risks to enterprise cybersecurity by exposing the organization to risks such as data breaches, insider threats, regulatory noncompliance, and malware (including ransomware).

## Uncontrolled access from anywhere on any device

In a cloud environment, an enterprise no longer has a single network perimeter to protect. Company data and applications have expanded beyond the corporate premises, and users require access from anywhere on any device.

At the same time, users create and use massive amounts of data, ranging from highly confidential and sensitive to mundane, and this data is now literally everywhere — in SaaS applications, in the public cloud, in the data center, and on users' devices.

As a result of all this, companies are losing visibility into and control over their networks, including users' web activities, what resources users are accessing, where and how sensitive data is protected, and their overall corporate security.

## Data protection issues for structured/unstructured data

Maintaining visibility of all sensitive data, wherever it is and moves, is fundamental to enabling an effective data protection strategy. But automatic discovery and categorization of sensitive data is not an easy task for any classification tool. In addition to broadly categorizing data as sensitive or nonsensitive, data also needs to be classified as structured or unstructured:

- » **Structured:** Structured data is clearly defined and searchable because it is stored and exists in predefined structures such as databases, consisting of cells with columns and rows with names, addresses, phone numbers, Social Security numbers, credit card numbers, and so on.
- » **Unstructured:** Unstructured data is available in a variety of formats. As an example, a Social Security number is a nine-digit number, often separated by two dashes, and it can be found in any construct such as a message among other words, in a Microsoft Word file, in a PDF, and so on.

Data protection technologies in first-generation CASB solutions struggle to keep pace with the volume and sprawl of both structured and unstructured sensitive data. Their data loss prevention (DLP) capability relies mainly on regex-based and traditional data fingerprinting methods, resulting in slow and inaccurate protection. Most important, they haven't evolved to detect data leakage through modern collaboration apps like Slack, Teams, and Zoom, which use new ways of communicating through short, unstructured messages.





A *regular expression* (*regex* for short) is a string of characters that specifies a search pattern in text. For example, you might search for credit card numbers using a regex that specifies 16 numeric digits.

## Lack of automation in incident management and remediation

The speed and scale of modern cyberthreats requires organizations to leverage automation for effective incident management and remediation. Unfortunately, far too many organizations still rely heavily on manual, error-prone processes, which slows incident response and gives cybercriminals more dwell time in the target environment to establish persistence, move laterally, and do damage.

## Misconfiguration issues

New cloud technologies and service offerings are constantly being introduced — which is not only a great benefit of the cloud but also a serious challenge of it. Keeping pace with and understanding the innovations and changes in the cloud is a never-ending quest.

Misconfiguration issues in the cloud are a major source of security risk for organizations. Many organizations have only a limited understanding of the *shared responsibility model*, in which both the customer and the cloud service provider are responsible for different aspects of security and compliance. This is particularly true of SaaS offerings, where many customers mistakenly believe the cloud provider is responsible for the entire stack, including data protection. The opportunities for misconfiguring sharing permissions in Slack or Teams, for example, can result in a serious data breach for the organization.



Regardless of whether you're using IaaS, PaaS, or SaaS solutions, you — not the cloud provider — are *always* responsible for the security of your data.

## Suspicious user activity

Finally, detecting and recognizing suspicious user activity has also become more challenging as a result of the hybrid workforce and rapidly changing patterns of what can be considered normal user behavior.

As the workforce becomes more dispersed and applications, data, and security tools and services become more decentralized, getting complete end-to-end visibility of network activity becomes more difficult. Without this full picture, baselining user activity and identifying insider threats (including negligent, accidental, or malicious behavior) using first-generation CASB solutions and other traditional technologies becomes a futile activity.

- » Defining CASBs
- » Looking at first-generation and other legacy CASBs
- » Architecting the next-generation CASB solution

## Chapter 2

# Understanding the CASB Solution Architecture

**T**his chapter introduces cloud access security broker (CASB) solutions — what they are and how current first-generation CASB solutions compare to next-generation CASB solutions.

## What Is a CASB?

A CASB is a security policy enforcement point that sits between a cloud services provider and its users.

CASBs help organizations discover their sensitive data across software as a service (SaaS) applications, cloud services environments, on-premises data centers, and mobile devices. A CASB also enforces an organization's security, governance, and compliance policies, allowing authorized users to access and consume cloud applications while enabling organizations to protect their sensitive data effectively and consistently across multiple locations.

# Comparing Past and Present CASB Solutions

The first CASB solutions were introduced in 2013. In a cloud-driven world, they have become vital to enterprise security. CASBs help enterprises protect and govern the usage of the SaaS applications in use by the organization.

However, the rapid adoption of SaaS apps is radically changing user access patterns and levels of security risk for cloud-driven enterprises. Today, first-generation (and other legacy) CASB solutions struggle to provide holistic visibility and effective security policy enforcement for the enterprise.

Traditional CASBs can't discover and control new cloud applications quickly because they rely on static application libraries that must be manually populated. Additionally, the application programming interface (API) protections in traditional CASBs typically don't cover modern collaboration apps — like Confluence, Jira, Slack, Zoom, and so on — where users spend much of their time working with sensitive data.

Traditional CASBs offer basic cloud security capabilities that are limited in scope and depth. For example, the data loss prevention (DLP) capabilities in traditional CASBs are quite basic and inaccurate, covering only data security in the cloud, and are not integrated with enterprise DLP policies and solutions. Traditional CASBs also lack the essential threat protection mechanisms that detect endless threat variations that cybercriminals constantly create to target SaaS applications.

Traditional CASBs were designed as stand-alone proxy-based point solutions that were disjointed from the rest of the enterprise security infrastructure. These proxy-based CASBs require complex traffic redirection from the network firewall with Proxy Auto-Configuration (PAC) agents and log collectors, causing significant architectural and operational complexity, as well as high cost of ownership.



REMEMBER

Furthermore, traditional CASBs can't keep up with the rapid growth of SaaS applications and shadow IT, the ubiquitous growth of data, or the increasing numbers of hybrid and remote workers in the enterprise. To keep pace, enterprises need a next-generation CASB solution.

Table 2-1 compares first-generation (legacy) CASB and next-generation CASB capabilities.

**TABLE 2-1    Comparing Legacy and Next-Gen CASBs**

Legacy CASBs	Next-Gen CASBs	Description
Protect only apps that use HTTP/HTTPS.  Limited to productivity apps with files and databases.  Manual; no intelligence to automatically identify new apps.	Protect any app using any protocol.  Protect all collaboration apps with conversations and images.  Automated discovery of new SaaS apps via crowdsourcing and machine learning (ML).	Legacy CASBs limit what you can see; a next-gen CASB lets you see and secure all apps in your hybrid enterprise.
Complex and require changes to network architecture.  Separate tools for HQ, branch, and remote users.  Siloed approach with disjointed controls and security gaps.  Users are not protected in a single-unified solution.	Activate in one click and integrate into the existing network architecture.  CASB, secure access service edge (SASE), and enterprise DLP integrated in a unified cloud console.  Consistent policies for HQ, branch, and remote users.	Legacy CASBs are complex and disjointed; a next-gen CASB simply and consistently protects all users everywhere.
Protect only data that goes through proxy and limited APIs.  Inaccurate pattern-based detection requires a lot of manual tuning.  Separate tools and policies for SaaS and other control points.	Comprehensive cloud-based enterprise DLP for all control points.  More accurate detection with ML and natural language processing (NLP).  Consistent policies for HQ, branch, and remote users.	Legacy CASBs offer inaccurate data protection; a next-gen CASB accurately protects all sensitive data in real time.
Lack important capabilities and use an ineffective third-party sandbox.  Inaccurate and limited; can only protect from threats through HTTP/HTTPS.  Siloed approach; disjointed and separate from the network.	Rely on innovation and proactive threat analysis.  Show effectiveness with 100 percent of blocked evasions.  Consistent across SaaS, infrastructure as a service (IaaS), network, branch, and remote workforces.	Legacy CASBs offer poor security.  Next-generation CASB delivers integrated and consistent security.

# Looking at the Next-Generation CASB Architecture

To address modern enterprise security requirements, a next-generation CASB natively promotes the convergence of cloud and enterprise security to close operational gaps between the two. By integrating with existing security infrastructure and leveraging ML and crowdsourced threat intelligence from the global community, next-generation CASB automatically discovers and controls all SaaS apps and data risks across all users from every location on any device.

## Multimode

Next-generation CASB incorporates both in-line and API-based SaaS controls for governance, access controls, and data protection. Also called a *multimode* CASB, the combination of in-line and API-based SaaS security capabilities provides superior visibility, management, security, and zero-day protection against emerging threats.

## API-based

Using out-of-band API-based security mechanisms, next-generation CASB connects directly to sanctioned SaaS apps and scans them for sensitive data, endless variants of malware, and policy violations, while maintaining compliance and ensuring threat protection in real time without dependence on third-party tools.

In addition to protecting the sensitive data in your SaaS apps, next-generation CASB protects the app itself via API to detect misconfigurations that could potentially leak sensitive data.

## In-line controls

In-line controls provide security for data in motion. Next-generation CASB works in conjunction with SASE to monitor access to SaaS applications and evaluate the data being sent or retrieved. Next-generation CASB uses cloud-based ML in order

to discover SaaS applications. It also provides advanced analytics and reporting, so your organization has the insight into the data security risks of sanctioned and unsanctioned SaaS application used, or shadow IT, on your network.

## Data loss prevention

DLP solutions help organizations automatically locate all their sensitive information and protect it from intentional or unintentional loss and from theft. However, traditional DLP solutions weren't designed with workforce mobility and the cloud landscape in mind. As enterprises continue on the path to digital transformation, problems with complexity, administrative effort, and partial protection of sensitive data will only become more common.

In DLP, automatic discovery of sensitive data drives response actions on policy violations — so it needs to be accurate. Inaccurate detection produces false positives, unsustainable incident triaging work, and disruption of normal business processes. Content similarities need advanced detection techniques that account for context as well.

A modern DLP approach also needs to adapt to data flowing through modern collaboration apps like Slack, Microsoft Teams, and Zoom, where users communicate with short and unstructured messages leveraging more screen captures rather than traditional files to quickly convey ideas and information.



REMEMBER

DLP starts with automatic data discovery and classification. After data is discovered, it can be protected. DLP can discover where data is stored in the organization's sanctioned SaaS apps, in their public cloud storage resources, traversing their networks, or shared across their employees' devices. It can then enable automatic or manual protective actions.

A modern cloud-delivered DLP solution enables a more comprehensive and effective data protection approach. When natively integrated with next-generation CASB, it enables organizations to protect all sensitive data continuously and consistently across network, cloud, and users regardless of location or device.

## WHY THE NEXT-GENERATION CASB IS AN INTEGRAL PART OF A ZERO TRUST SASE SOLUTION

CASBs are one of the key cloud security capabilities that make up a comprehensive SASE (pronounced “sassy”) solution. SASE solutions converge software-defined wide-area networking (SD-WAN) and network security services such as firewall as a service (FWaaS), Zero Trust, and CASB in a single, cloud-delivered service model.

CASB security functionality is integrated into SASE, providing SaaS application and data security in a single platform. A SASE solution helps you understand which SaaS apps are being used and where data is going, no matter where users are located. Specific capabilities should include the following:

- **SaaS visibility:** Discovery of shadow IT, app discovery, app usage reporting, app risk assessment, and configuration assessment
- **Control and compliance:** App access control, data discovery and classification, compliance reporting and remediation, and unmanaged device access control
- **SaaS protection:** Threat protection, data protection, encryption, rights management, suspicious user activity, and workflow integration



#### IN THIS CHAPTER

- » Enabling complete visibility of sanctioned and unsanctioned SaaS apps
- » Leveraging enterprise data loss prevention
- » Automating incident response
- » Protecting your apps and data from threats in real time
- » Delivering granular and adaptive access management
- » Discovering and preventing suspicious user activity
- » Managing your SaaS security posture

## Chapter 3

# Exploring Must-Have Capabilities and Features in Next-Generation CASBs

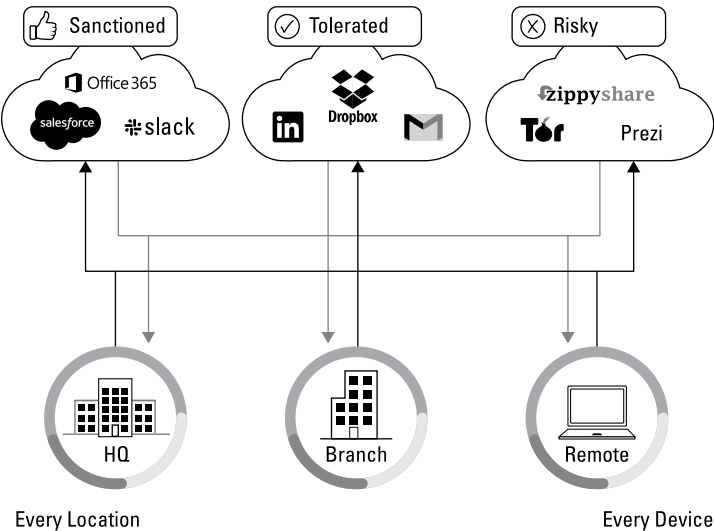
**T**his chapter outlines the key capabilities and features to look for in a next-generation cloud access security broker (CASB) solution.

# Visibility of Sanctioned and Unsanctioned SaaS Apps

First and foremost, a next-generation CASB must automatically discover and prevent risks for tens of thousands of new software as a service (SaaS) applications before they become a problem for your enterprise.

A comprehensive next-generation CASB solution scans all traffic, ports, and protocols in addition to Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS), including Tor, File Transfer Protocol (FTP), and virtual private networks (VPNs), in order to detect all types of applications.

As shown in Figure 3-1, a next-generation CASB solution must provide visibility into and control of all SaaS apps (including unsanctioned, tolerated, and sanctioned apps) across every location and every device.



**FIGURE 3-1:** Next-generation CASB provides visibility into and control of all enterprise SaaS apps and data across every location and every device.

The application identification technology in next-generation CASB leverages the power of the broad global community and machine learning (ML) models to automatically provide continuous

identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

A SaaS Security catalog delivers granular visibility into applications, their usage within the organization, and their risks. Applications are classified across hundreds of different categories in the catalog. Default risk scores can also be customized based on the risk attributes that matter most to your organization. Risk mitigation controls and policy recommendations can be automated for existing and future applications, eliminating time-consuming manual policy definitions.

## SaaS Data Protection

Next-generation CASB helps enterprises achieve unparalleled protection of all their sensitive data with more automated detection engines, more control points, and content-aware technologies. The solution provides data protection and compliance controls consistently across all SaaS applications, and comprehensively throughout the enterprise across clouds, on-premises networks, and users, with cloud-delivered enterprise data loss prevention (DLP).

Enterprise DLP leverages a single cloud engine to deliver unified policies for sensitive data everywhere, both at rest and in transit. It scans, classifies, and protects all data stored within SaaS applications while it's in motion to make sure policy violations, exposures, and regulatory compliance are properly addressed.

Enterprise DLP ensures the highest levels of accuracy. It automatically detects sensitive content via ML-based data classification and an extensive number of described data identifiers using regular expressions (regex) or keywords — for example, credit card or ID numbers, financial records, General Data Protection Regulation (GDPR), and other data privacy- and compliance-related information — and applies customizable data profiles and Boolean logic to scan for collective types of data. Type of exposure (for example, public or internal), confidence levels, and precise context criteria (for example, number of occurrences and pattern logic) reduce incidents and inaccurate detection.



Exact data matching (EDM) is an advanced data fingerprinting method to detect specific sensitive data, and protect it from malicious exfiltration or loss.

Most important, a next-generation CASB is able to automatically identify sensitive information even within the context of unstructured users' conversations on collaboration apps like Slack through deep learning, natural language processing (NLP), artificial intelligence (AI) models, and advanced optical character recognition (OCR), ensuring high accuracy and fewer false positives.

Automated incident workflows with policy-based response actions include user alerts and auto-remediation. Detection of flexible document properties, such as third-party data tagging, augments the identification of sensitive data.



Next-generation CASB also includes file-blocking profiles that can be used to prevent files from being downloaded, which is an important part of a cloud data protection strategy.

## Incident Response

Next-generation CASB has DLP end-user alerting with security orchestration, automation, and response (SOAR) capabilities. SOAR allows your team members to understand why a file upload was blocked by enterprise DLP and enables self-service temporary exemptions for file uploads that match your enterprise DLP data profiles.

The enterprise DLP end-user alerting with SOAR provides an audit trail to better understand the upload and response history for every file scanned by the DLP cloud service. Additionally, enabling end-user alerting with SOAR prevents malware-triggered uploads because an affirmative action is required to request an exemption.

## Threat Prevention

Next-generation CASB protects sanctioned SaaS apps by consistently applying enterprise DLP, ML-powered threat prevention, and ongoing monitoring of user activity and administrative configurations. This deployment model works across any access

point, regardless of the user's location or device. It preserves the user experience with corporate SaaS apps because it's nonintrusive and doesn't interfere with standard business processes.

These threat prevention capabilities in next-generation CASB help you accurately protect all sensitive data stored in cloud applications, maintain compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and GDPR, and stop all unknown and known threats in real time, without requiring third-party security tools.

## Granular In-Line Controls

Granular in-line controls allow for fine-tuned monitoring and control of SaaS application usage within your organization. These controls provide a level of granularity that allows administrators to create specific policies and rules for different types of cloud applications and user groups. Clientless capabilities are also supported to secure access from unmanaged devices accessing SaaS applications.

## Suspicious User Activity

Next-generation CASB provides user and entity behavior analytics (UEBA), which is a user behavior analytics tool that leverages ML and advanced analytics to identify and detect suspicious user activities. This feature can detect and prevent security threats, such as compromised accounts, data exfiltration, and insider threats. UEBA monitors user activity by collecting data from various sources, such as cloud application logs and network traffic. It then uses ML algorithms to analyze the data and identify abnormal or suspicious activity. This includes identifying unusual patterns in user behavior, such as an unusual increase in file uploads, or an unusual number of failed login attempts.

Overall, UEBA allows the security team to detect and prevent security threats from compromised accounts, data exfiltration, and insider threats, by providing a detailed view of user activity, allowing security teams to investigate and understand the context of suspicious activity, and take automated actions according to the severity of the threat.

# SaaS Security Posture Management

Next-generation CASB addresses an attack vector that traditional CASBs have overlooked: the app itself. A strong security posture for sanctioned SaaS apps consists of proper configurations and protection from misconfigurations that could leak sensitive data.

Although the explosion of SaaS apps has dramatically improved productivity and business agility, it has opened up new avenues for data breaches and exposures, making SaaS Security Posture Management (SSPM) fundamental to every organization's SaaS security strategy.

Securely configuring thousands of settings across hundreds of sanctioned SaaS apps is not an easy task. What's more, finding security misconfigurations — and keeping them fixed — is even harder. Next-generation CASB should address the gap that legacy CASBs have neglected.

#### IN THIS CHAPTER

- » Mapping your attack surface
- » Understanding where your sensitive data is used and stored
- » Protecting users from themselves — and SaaS app risks
- » Enabling real-time threat prevention
- » Implementing granular controls for sanctioned, tolerated, and risky apps
- » Monitoring risky user behavior
- » Improving your security posture

# Chapter 4

## Mitigating SaaS App Risks

In this chapter, you learn how to put the key capabilities of a next-generation cloud access security broker (CASB) to work in your organization to mitigate software as a service (SaaS) app risks.

### Starting with Discovery and Control

Addressing your SaaS app risks begins like many other strategic security efforts: with knowing what you have to protect. More specifically, with regard to SaaS apps, you need to discover shadow IT across your entire organization. Map your attack surface by taking an inventory of all SaaS apps that are in use, whether they're sanctioned by the organization or not, and the data that these apps use.

Next, you need to categorize the SaaS apps that you discover as either sanctioned, tolerated, or unsanctioned:

- » **Sanctioned:** Sanctioned apps are generally core enterprise apps that have been formally adopted by your organization and are fully supported.
- » **Tolerated:** Tolerated apps are apps that may have come into your organization through shadow IT but are nonetheless necessary for your users to perform their job functions or are otherwise permitted. These apps may have additional security requirements or policies enforced to mitigate any associated risks. For example, you may increase monitoring of user activity within the app, implement specific data loss prevention (DLP) policies to restrict the transfer of sensitive data, and/or enforce multifactor authentication (MFA) for identity and access management (IAM).
- » **Unsanctioned:** Unsanctioned apps have no legitimate business need and could present unnecessary risk to an organization. These apps could include ones like unknown file-sharing apps, gambling apps, certain social media apps or streaming services, or even apps that are capable of evading proxies.

Undertaking this effort manually is practically impossible in any large organization. The number and types of SaaS apps that your employees download, install, and use every day can be overwhelming. Discovering these apps with siloed tools or through manual processes will lead to a never-ending race for IT to keep up with your users.



REMEMBER

Automated and accurate SaaS app and data discovery and classification for sensitive and regulated data transferred to and stored in the cloud is a key capability in next-generation CASB.

## Getting Visibility into Data Flows

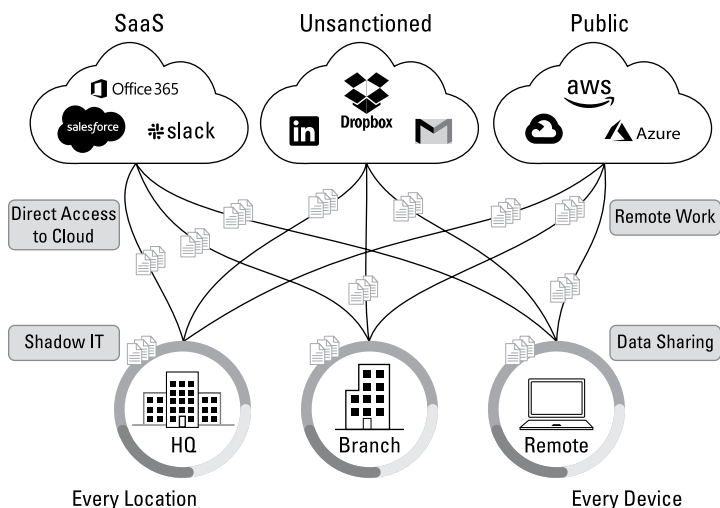
Organizations are responsible for ensuring compliance and data privacy throughout the entire enterprise, including in sanctioned SaaS applications, in cloud environments, and across remote user devices and locations.





Sensitive data that is subject to regulatory mandates, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) may be — and probably is — stored and shared outside your on-premises data center in SaaS collaboration apps and file storage services (such as Dropbox, Google Drive, and OneDrive).

It is incumbent upon organizations to make sure sensitive data is not overshared, is not overexposed in the cloud, and is not transferred through unsanctioned SaaS apps (see Figure 4-1). But the growing reliance on cloud apps, whether sanctioned or unsanctioned, makes it harder for IT teams to monitor noncompliant data transfers made by employees working remotely. A good example of this is when an employee tries to edit a confidential document containing payment card data using a document editing app in the public cloud, and unwittingly transfers a file containing private information that is subject to GDPR.



**FIGURE 4-1:** Sensitive data may be processed and stored anywhere, including in sanctioned and unsanctioned SaaS apps, public clouds, and user devices.

As SaaS adoption continues to rise, so does the uploading, storing, and sharing of business information — including sensitive or confidential data — through these apps. SaaS apps do make information easy to share between users and apps, but their exploding numbers create a complex web of interactions that puts

data security at extreme risk. The transfer of business data on unsanctioned apps is even more difficult for IT teams to monitor, given the lack of visibility into the apps in use across the enterprise.

## Educating Users on Risky Data Usage

Any security initiative, regardless of how innovative the technology may be, requires the right mix of people, processes, and technology to succeed. Determined users can be very resourceful and come up with creative ways to circumvent controls that they don't understand and perceive to be nothing more than a nuisance.

Educating your users about the risks associated with various SaaS apps and user behaviors is critical. With even just a basic understanding of why certain security controls exist and what the associated risks of a specific app or behavior means to the organization — as well as to the individual user (for example, a SaaS app downloaded to a user's personal device may expose their banking information, personal photos, or private messages) — can go a long way toward promoting a collaborative and secure culture in which users, IT, and security work together to achieve their desired outcomes.

## Preventing Threats in SaaS Apps

A next-generation CASB incorporates real-time global threat intelligence and other threat prevention capabilities to protect your critical SaaS apps and sensitive data from known, unknown, and emerging threats. This capability goes beyond malware protection and allow or block policy enforcement to include granular controls, automated incident response (for example, via security orchestration, automation, and response [SOAR]), playbooks for specific scenarios, and analytics to identify anomalous network activity and risky user behavior.

# Controlling Tolerated Apps versus Unsanctioned Apps

Beyond sanctioned apps, well-intentioned employees often end up circumventing security policies and controls to use various unapproved apps, including tolerated apps and unsanctioned apps, to meet a legitimate business need. The practice of accessing unapproved apps creates a shadow IT environment in which the unapproved apps are managed by the employees themselves without the explicit knowledge, approval, and support of the IT department.

In practically every enterprise, employees use more SaaS apps than assumed — the unapproved apps serve to further complicate the problem by tacking on hidden risks of data loss, widening the threat landscape, and expanding SaaS governance problems. A significant challenge today is that employees can often access any SaaS app — sanctioned, tolerated, or unsanctioned — from their remote work-from-home offices without connecting to the corporate virtual private network (VPN).

Another case in point is that all SaaS apps — whether sanctioned, tolerated, or unsanctioned — run in the cloud, are delivered from the cloud, and are, by definition, highly distributed in countless cloud provider environments. The clutter created by these apps is responsible for bringing every organization's cloud-shift transformation to a critical crossroads. On the one hand, employees are unavoidably dependent on SaaS apps to get their work done; on the other, organizations at the cusp of transformation are finding themselves caught in a metaphorical storm of hundreds of apps “raining down” from different cloud provider environments.



TIP

Use the capabilities in a next-generation CASB to enforce granular controls for sanctioned, tolerated, and unsanctioned apps in your environment.

## Monitoring and Preventing Risky User Behavior

As organizations increasingly adopt SaaS applications such as Box, Microsoft 365, Salesforce, Slack, Workday, and others, more and more data is uploaded, stored, and shared in the cloud. In this

scenario, monitoring remote employee behavior that can pose a risk to sensitive data is difficult.

Moreover, managing employees' authorized IT devices is not always enough because often remote employees don't connect to their employer's VPN and instead choose to connect directly to both corporate applications and various unsanctioned SaaS applications. Without application programming interface (API) security support, an even bigger challenge occurs if the devices used by remote users to access corporate SaaS applications happen to be their unmanaged personal devices that IT has no knowledge of. In such instances, organizations have little to no visibility or control over what sensitive data is transferred by the employees through SaaS applications.



**WARNING**

Malicious actors are not the only source of data loss in organizations. Well-meaning employees often engage in behaviors that inadvertently put sensitive data at risk — for example, sharing confidential documents openly in cloud applications or transmitting private information via personal email accounts.

## Ensuring the Best Security Posture on Corporate SaaS Apps

A single, consistent next-generation CASB must protect users, apps, and data in a manner that is clear, comprehensive, and easy. It should alleviate the IT team's shadow IT burdens by automatically allowing them full visibility and thorough control over all their shadow IT risks. Providing the broadest API support to control a large number of sanctioned SaaS apps, next-generation CASB should maintain compliance consistently in the cloud while preventing ever-evolving threats to critical apps, as well as the exposure of sensitive data.



**TIP**

To secure SaaS apps today, you need visibility into configurations. Performing continuous, comprehensive monitoring of all security-impacting configurations in SaaS apps and aligning them to security-oriented best-practice recommendations is a must.

#### IN THIS CHAPTER

- » Enabling rapid growth at cloud scale
- » Keeping deployment simple
- » Detecting all threats
- » Extending data protection and compliance across the enterprise
- » Delivering integrated and consistent security

# Chapter 5

## Ten (or So) Things to Look for in a Next-Generation CASB

**H**ere are some important capabilities and features that you need to look for in a next-generation cloud access security broker (CASB) solution for your enterprise.

### Cloud Scale

Complete visibility into your software as a service (SaaS) environment is essential in determining the true state of your cloud and data security. When cloud-based solutions are used outside the purview of IT, your company's data is no longer under the influence and oversight of the company's governance and risk policies. A next-generation CASB solution should continuously and automatically see and secure all sanctioned and unsanctioned apps, including modern collaboration SaaS apps, to keep pace with the exponential growth of SaaS.

A next-generation CASB solution should be able to scan all traffic, ports, and protocols, automatically discover new apps, and leverage the largest set of application programming interfaces (APIs) of SaaS apps, including APIs for modern collaboration apps like Microsoft Teams and Slack. It should provide accurate and customizable risk scores and risk attributes against all apps to monitor and prevent risky user activity — before the apps come into question and become carriers of threats. Comprehensive real-time SaaS visibility and risk scores will enable your IT teams to keep up with SaaS growth, help ascertain granular risk-based controls of both known and previously unknown SaaS apps, and intelligently prevent them from becoming conduits of data loss.



**TIP**

Look for these capabilities to make sure your next-generation CASB solution supports cloud scale:

- » Broad security coverage for all SaaS apps, including API-based security coverage to provide additional control for sanctioned SaaS applications
- » Continuous app discovery powered by an application ID-based cloud engine for shadow IT apps
- » Automated risk classification with numerous attributes to help determine each organization's risk
- » Bulk tagging capabilities to help classify apps by adding their sanctioned status and customized tagging for detailed classification
- » Integrated in-line controls and enforcement that can be deployed easily across all devices and users
- » Strong SaaS Security Posture Management (SSPM) capabilities with continuous visibility into configurations
- » Continuous, comprehensive monitoring of all security-impacting configurations in SaaS apps and alignment to security-oriented best-practice recommendations

## Simple Deployment

In highly distributed modern enterprises with multiple sites and mobile users, the middleman approach of legacy CASB solutions becomes difficult to scale, costly, and unsustainable. Legacy

CASBs are cumbersome to deploy because they add an unnecessary cloud gateway (typically, a proxy) and require complex traffic redirection from log collectors like the network firewall and Proxy Auto-Configuration (PAC) agents. On top of that, they need an active directory (AD) connector to enforce policies by user ID or the AD group. With multiple sites, this infrastructure has to be duplicated over and over again. Beyond that, due to users working from remote locations today, extra endpoints with PAC file installations or additional VPN agents to route remote user traffic through the cloud-based proxy are also required. Proxy architecture is a must for those who depend on it, but it's a burden for everyone else to set up and it definitely shouldn't be the only way.

A next-generation CASB solution should eliminate all the middleman components and unburden your IT teams from additional infrastructure investments. It should allow your IT security teams to simplify operations by leveraging secure access service edge (SASE) and CASB together in a unified platform for security, networking, and data protection across all environments. Lastly, it should be capable of leveraging your existing next-generation firewall investment for comprehensive and integrated SaaS security posturing and monitoring.



**TIP**

Look for these capabilities to make sure your next-generation CASB solution is simple and easy to deploy:

- » A 100 percent cloud managed solution with flexible deployment options to easily enable a hybrid workforce
- » A single dashboard for visibility applied throughout all cloud application policies
- » Simplified configuration using optimized workflows and machine learning (ML)-based automation
- » Automatic up-to-date shadow IT visibility powered by native integrations
- » Out-of-the-box integration with enterprise data loss prevention (DLP), threat protection, and in-line controls for enforcement
- » No added PAC files or proxies to complete deployment

# Detection of Known and Unknown Threats

The diverse nature of SaaS apps means a highly distributed environment where hundreds of apps “rain down” from different cloud provider environments to generate numerous points of compromise. Successful outcomes of your SaaS security posturing require actionable insights into detection and prevention of threats arising from your SaaS landscape.

A next-generation CASB solution should be a proven solution that prevents zero-day threats with natively integrated in-line ML models that don’t require you to rely on third-party tools. It should stop new and unknown threats instantly with evasion-resistant signatures, and then distribute updates globally within seconds, ensuring protection is distributed more quickly than the rate of infection.

Going beyond traditional malware analysis, a next-generation CASB should draw from a crowdsourced threat intelligence engine that leverages the largest data sets to stop threats quickly and easily with in-line, real-time, zero-day protections. This new approach to threat prevention will ensure the most up-to-date security posture and defense against anomalous SaaS-based threats across your network — saving your IT teams valuable time and effort.



TIP

Look for these capabilities to make sure your next-generation CASB solution provides best-in-class threat prevention:

- » Continuous malware and threat protection powered by a cloud-based malware analysis and prevention engine to help detect and prevent new unknown file-based threats
- » An incident remediation workflow with automated remediation
- » User activity monitoring and response

## Comprehensive Data Protection and Compliance

Most legacy CASB solutions offer basic security with regards to data protection and compliance that is limited to cloud environments. Enterprise DLP solutions deployed on-premises



rely on advanced techniques and superior capabilities, but they create an unbalanced approach between on-premises and cloud environments.

A next-generation CASB solution should provide data protection and compliance controls reliably, consistently, and comprehensively throughout the entire enterprise, across clouds, in on-premises networks — basically wherever your users and data reside. It should discover, classify, and protect all data stored within and transmitted across SaaS that is in-line and SaaS that is out of band via APIs to make sure policy violations, exposures, and regulatory compliance are properly addressed.

A next-generation CASB also needs to adapt to new data models of modern collaboration apps like Microsoft Teams, Slack, and Zoom, where users communicate with short and unstructured messages and screen captures. Leveraging a powerful cloud detection engine, descriptive data profiles, exact data matching (EDM), image recognition, natural language processing (NLP), and artificial intelligence (AI) models, it should accurately detect sensitive data — including structured and unstructured data — both at rest and in motion.



**TIP**

Look for these capabilities to make sure your next-generation CASB solution offers comprehensive data protection and compliance:

- » Enterprise DLP for data at rest and data in motion, including discovery of sensitive data in SaaS applications, data exposure detection through out-of-the-box EDM, optical character recognition (OCR) and data profiles, and prevention of data exfiltration
- » Data protection for mission-critical collaboration applications like Confluence, Jira, Microsoft Teams, Slack, and Zoom, with the ability to automatically identify sensitive information in real time within the context of unstructured users' conversations through deep learning, NLP, and AI models
- » Out-of-the-box reporting for compliance including a real-time General Data Protection Regulation (GDPR) report for data at rest, an on-demand risk assessment report for data at rest, and an on-demand SaaS Security report for shadow IT applications

# Integrated and Consistent Security across All Locations

Detached from an enterprise's core infrastructure, legacy CASBs are limited in their ability to provide consistent security controls across all environments — the cloud, on-premises, remote. This limitation has a downstream effect on security teams who must synchronize risks, policies, and controls across multiple environments.

A next-generation CASB solution should function as an integrated solution that securely enables a company's hybrid workforce across all locations — whether remote or in the office — in addition to all the applications in use and all data stored or transmitted through them. Circumventing the complexity of point products, such a solution consistently protects data stored and in motion not only via cloud-based apps but also through the physical network. Being multimode, the next-generation CASB secures both unsanctioned and sanctioned SaaS apps and protects all traffic — web and non-web — from a single unified cloud-delivered console. It should discover unsanctioned SaaS apps and manage risks while providing broad API-based security to connect and scan sanctioned apps running out of band in the cloud for at-rest detection, inspection, and remediation across all users, folders, and file activity.



**TIP**

Look for these capabilities to make sure your next-generation CASB solution is integrated and multimode:

- » Granular in-line controls across all applications for all users and devices
- » Data security controls and compliance across all SaaS apps, networks, and users, without requiring any third-party tools
- » Threat prevention across all apps, networks, and devices, without requiring any third-party tools
- » The reuse of existing security infrastructure — no architectural changes, PAC files, or additional virtual private network (VPN) agents required

# Glossary

**AI:** *See* artificial intelligence (AI).

**API:** *See* application programming interface (API).

**application programming interface (API):** A set of protocols, routines, and tools used to develop and integrate applications.

**artificial intelligence (AI):** The ability of a computer to interact with and learn from its environment and to automatically perform actions without being explicitly programmed.

**BitTorrent:** *See* torrent.

**CASB:** *See* cloud access security broker (CASB).

**cloud access security broker (CASB):** A security policy enforcement point that sits between a cloud services provider and its users, allowing authorized users to access and consume cloud applications while enabling organizations to protect their sensitive data effectively and consistently across multiple locations.

**data loss prevention (DLP):** An application or device used to detect the unauthorized storage or transmission of sensitive data.

**denial of service (DoS):** An attack on a system or network with the intention of making the system or network unavailable for use.

**DLP:** *See* data loss prevention (DLP).

**DoS:** *See* denial of service (DoS).

**EDM:** *See* exact data matching (EDM).

**exact data matching (EDM):** An advanced data fingerprinting method to detect specific sensitive data and protect it from malicious exfiltration or loss.

**File Transfer Protocol (FTP):** A standard network protocol used to transfer computer files from one host to another over TCP ports 20 and 21. *See also* Transmission Control Protocol (TCP).

**firewall as a service (FWaaS):** A firewall platform provided as a service offering in a cloud environment.

**FTP:** *See* File Transfer Protocol (FTP).

**FWaaS:** *See* firewall as a service (FWaaS).

**GDPR:** *See* General Data Protection Regulation (GDPR).

**General Data Protection Regulation (GDPR):** A law that strengthens data protection for European Union (EU) residents and addresses the export of personal data outside the EU.

**HTTPS:** *See* Hypertext Transfer Protocol Secure (HTTPS).

**Hypertext Transfer Protocol Secure (HTTPS):** HTTP is an application protocol used to transfer data between web servers and web browsers, typically on TCP port 80. HTTPS is an encrypted version of HTTP that uses SSL or TLS encryption to secure data in transit. *See also* Transmission Control Protocol (TCP), Secure Sockets Layer (SSL), *and* Transport Layer Security (TLS).

**IaaS:** *See* infrastructure as a service (IaaS).

**IAM:** *See* identity and access management (IAM).

**identity and access management (IAM):** The processes and procedures that support the life cycle of identities and access privileges.

**infrastructure as a service (IaaS):** A cloud-based service model in which the customer manages operating systems, applications, compute, storage, and networking, but the underlying physical cloud infrastructure is maintained by the service provider.

**machine learning (ML):** A method of data analysis that enables computers to analyze a data set and automatically perform actions based on the results without being explicitly programmed. Also, a subset of AI. *See also* artificial intelligence (AI).

**MFA:** *See* multifactor authentication (MFA).

**ML:** *See* machine learning (ML).

**multifactor authentication (MFA):** Any authentication mechanism that requires two or more of the following factors: something you know, something you have, or something you are. MFA is commonly implemented with a combination of username and password (something you know) and a one-time passcode sent to a user's device via text message, email, or phone call (something you have).

**natural language processing (NLP):** A branch of AI that helps computers understand, interpret, and manipulate human language. *See also* artificial intelligence (AI).

**NLP:** *See* natural language processing (NLP).

**OCR:** *See* optical character recognition (OCR).

**optical character recognition (OCR):** A process that converts printed or handwritten text to machine-readable characters.

**P2P:** *See* peer-to-peer (P2P).

**PaaS:** *See* platform as a service (PaaS).

**PAC:** *See* Proxy Auto-Configuration (PAC) file.

**Payment Card Industry Data Security Standard (PCI DSS):** An industry standard that mandates compliance for businesses that handle payment card transactions (such as debit cards and credit cards) and is enforced by the payment card brands (American Express, MasterCard, Visa, and so on).

**PCI DSS:** *See* Payment Card Industry Data Security Standard (PCI DSS).

**peer-to-peer (P2P):** A distributed application architecture that enables sharing between nodes.

**platform as a service (PaaS):** A cloud-based service model in which the customer is provided access to a platform for deploying applications and can manage limited configuration settings, but the operating system, compute, storage, networking, and underlying physical cloud infrastructure are maintained by the service provider.

**PrivateVPN:** A torrent-friendly VPN that supports unlimited P2P file sharing. *See also* torrent, virtual private network (VPN), *and* peer-to-peer (P2P).

**Proxy Auto-Configuration (PAC) file:** A web-based ruleset written in JavaScript that advises your endpoint on how to direct its traffic for a given URL: either via a web proxy or directly to the internet. It can contain information including the Internet Protocol (IP) address of the

website, the IP address of the user, and the host that requested the website. *See also* Uniform Resource Locator (URL).

**RaaS:** *See* ransomware as a service (RaaS).

**ransomware as a service (RaaS):** A business model that lowers the technical barrier for ransomware attacks. Instead of having to learn the skills necessary to code ransomware or access a network, cybercriminals can buy or lease access to ransomware with a broad range of offerings such as collection services and technical support.

**regex:** *See* regular expression (regex).

**regular expression (regex):** A string of characters that specifies a search pattern in text.

**SaaS:** *See* software as a service (SaaS).

**SASE:** *See* secure access service edge (SASE).

**SD-WAN:** *See* software-defined wide-area network (SD-WAN).

**secure access service edge (SASE):** Pronounced “sassy,” SASE solutions converge SD-WAN and network security services such as CASB, FWaaS, SWG, and ZTNA in a single, cloud-delivered service model. *See also* cloud access security broker (CASB), firewall as a service (FWaaS), secure web gateway (SWG), software-defined wide-area network (SD-WAN), and Zero Trust Network Access (ZTNA).

**Secure Sockets Layer (SSL):** A deprecated transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the internet. *See also* Transport Layer Security (TLS).

**secure web gateway (SWG):** A security platform or service that is designed to maintain visibility into all types of traffic, while stopping evasions that can mask threats. Additional functionality may include web content filtering and credential theft prevention.

**shadow IT:** IT applications and services that are acquired and operated by end users without explicit organizational approval and often without organizational IT knowledge or support.

**software as a service (SaaS):** A cloud-based software distribution model in which a third-party provider hosts applications that it makes available to customers over the internet. The software vendor hosts and maintains the servers, databases, and code that constitute an application.

**software-defined wide-area network (SD-WAN):** A newer approach to wide area networking that separates the network control and management processes from the underlying hardware, and makes them available as software. *See also* wide area network (WAN).

**SSL:** *See* Secure Sockets Layer (SSL).

**SWG:** *See* secure web gateway (SWG).

**tactics, techniques, and procedures (TTP):** The behaviors, methods, strategies, and tools used by threat actors to attack a target.

**TCP:** *See* Transmission Control Protocol (TCP).

**TLS:** *See* Transport Layer Security (TLS).

**Tor:** An open-source browser and network that enables users to communicate anonymously over the internet, often for nefarious and/or illegal purposes.

**torrent:** A P2P file-sharing communications protocol that distributes large amounts of data widely without the original distributor incurring the costs of hardware, hosting, and bandwidth resources. Instead, each user supplies pieces of the data to newer recipients, reducing the cost and burden on any given individual source. Also known as BitTorrent. *See also* peer-to-peer (P2P).

**Transmission Control Protocol (TCP):** A connection-oriented protocol responsible for establishing a connection between two hosts and guaranteeing the delivery of data and packets in the correct order.

**Transport Layer Security (TLS):** A transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers on the internet.

**TTP:** *See* tactics, techniques, and procedures (TTP).

**Uniform Resource Locator (URL):** Commonly known as a *web address*. The unique identifier for any resource connected to the web.

**URL:** *See* Uniform Resource Locator (URL).

**virtual private network (VPN):** A VPN creates a private connection, known as a *tunnel*, to the internet. All information traveling from a device connected to a VPN will be encrypted and go through this tunnel. When connected to a VPN, a device will behave as if it's on the same local network as the VPN. The VPN will forward device traffic to and from the intended website or network through its secure connection.

**VPN:** *See* virtual private network (VPN).

**WAN:** See wide-area network (WAN).

**wide-area network (WAN):** A computer network that spans a wide geographical area and may connect multiple local-area networks.

**Zero Trust Network Access (ZTNA):** A “never trust, always verify” security approach that ensures proper user context through authentication and attribute verification before allowing access to apps and data in the cloud or data center.

**ZTNA:** See Zero Trust Network Access (ZTNA).



## Explore key capabilities in next-generation CASB

When it comes to securing cloud-based applications and the sensitive data that flows through them, security teams have typically turned to cloud access security brokers (CASBs). However, current first-generation CASB solutions are broken due to numerous architectural and operational inefficiencies. Organizations often deploy multiple siloed tools to try to achieve a holistic defense, thereby increasing operational complexity and reducing security efficacy. Next-generation CASB offers a better path forward.

### Inside...

- Protect your hybrid workforce
- Control sanctioned and unsanctioned SaaS apps
- Prevent data loss
- Improve your security posture
- Automate incident handling
- Identify risky user behavior



**Lawrence Miller** served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 250 *For Dummies* books on numerous technology and security topics.

Go to **Dummies.com™**  
for videos, step-by-step photos,  
how-to articles, or to shop!

ISBN: 978-1-119-93368-7

Not For Resale

**for  
dummies®**  
A Wiley Brand



# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.