CASB 2.0

Symantec

The Next Generation of Cloud App Security

CASB 2.0

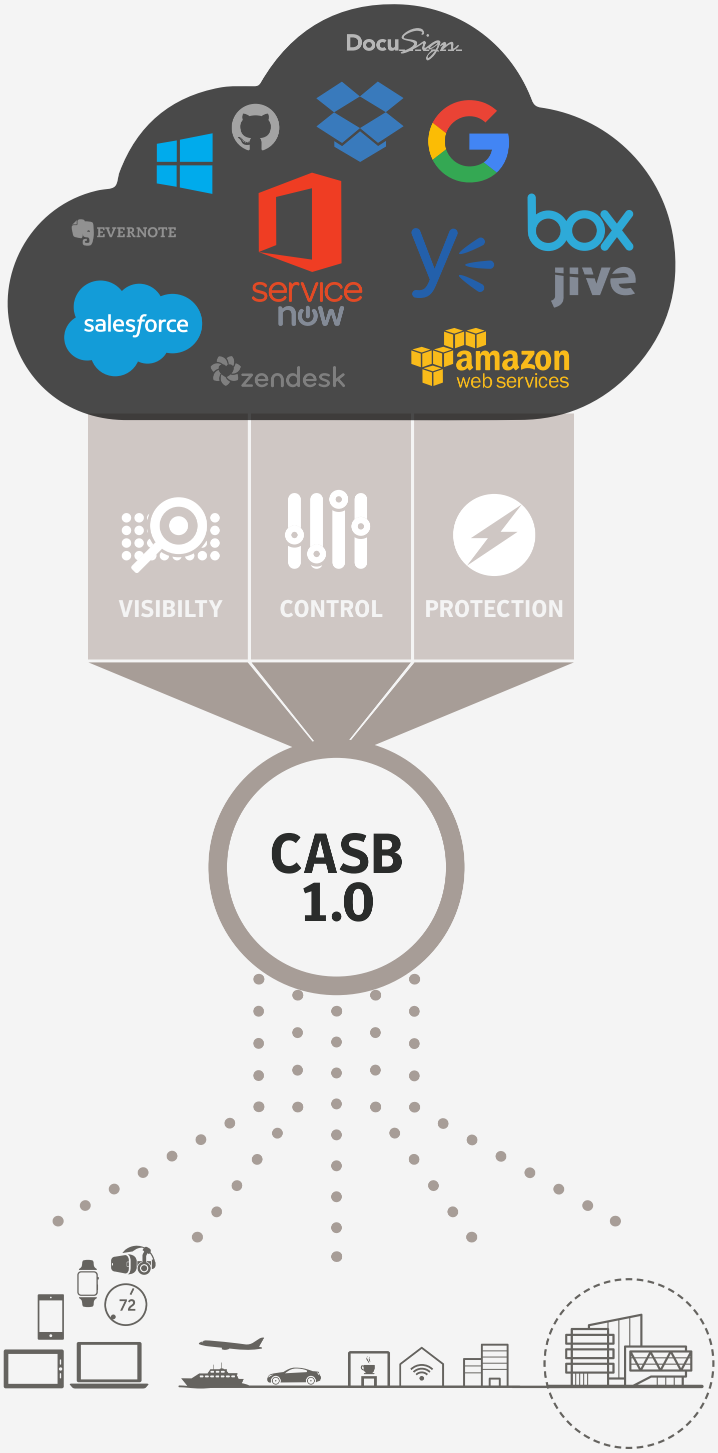
The Next Generation of Cloud App Security

Introduction

Cloud Access Security Broker (CASB) solutions have emerged over the past few years to address new security requirements related to the fast-growing cloud app and services market. As you have undoubtedly already seen in your own organization, cloud apps like G Suite, Office 365, and Salesforce provide tremendous benefits in terms of increased collaboration and employee productivity, but they also substantially increase your organization's attack surface.

Organizations are often blind to what cloud apps and services their users are accessing (known as Shadow IT). More importantly they are also blind to what users are doing inside cloud apps, for example what sensitive content they may be uploading and sharing (known as Shadow Data). Finally, the prospect of placing valuable corporate data in third party services raises the concern of data exfiltration by malicious actors. Most cloud app providers support a "shared responsibility" model for security—they will secure their back-end infrastructure, but they will not take responsibility for how users use the service or what data they upload. Thus a compromised account can lead to significant damage, which is outside the liability of the cloud app provider.

> "By 2020, 85% of large enterprises will use a cloud access security broker platform for their cloud services, which is up from less than 5% today."
>
> —Gartner, 'Market Guide for Cloud Access Security Brokers', 10/24/2016



CASB 1.0 to the Rescue

First generation CASBs stepped in to help cloud app customers address these new challenges. A typical CASB 1.0 solution provides:

Visibility into cloud app usage, including unsanctioned cloud apps, known as Shadow IT.

Granular control of sensitive data, including Cloud DLP and tokenization/encryption policy enforcement.

Protection against malicious attacks, leveraging user behavior analytics or anomaly detection to identify suspicious account activity.

Limitation of CASB 1.0

While these initial CASB solutions have helped to solve these new challenges, they also have limitations. The primary limitation of CASB 1.0 solutions is that they create a separate island of security in the cloud, disconnected from your existing core security investments. This complicates deployment, increases costs, and limits security efficacy.

Having separate security silos, where the CASB solution is isolated and separate from Data Loss Prevention (DLP), Secure Web Gateways (SWGs), endpoint security, encryption, and authentication services leaves gaps in functionality where data can be leaked, accounts can be compromised, and hackers can infiltrate your network. For example, how do you ensure that your core DLP policies are enforced consistently between on-prem and the cloud? Or how do you go beyond identifying risky apps, to actually restricting users in real time? Or how do you ensure your best-of-breed advanced malware protection can effectively examine content flowing in and out of your cloud app accounts?

The Emerging Need for CASB 2.0

In order to effectively protect your cloud apps and data no matter the user, location, or access device, your CASB needs to seamlessly integrate with core security infrastructure, including DLP, endpoint management, web security, encryption, user authentication, and advanced malware protection. Ultimately you want to leverage all of your security assets and investments to deliver the most effective security for the cloud. CASB 2.0 is about intelligently integrating CASB functionality with all of these core security technologies to provide comprehensive coverage of your cloud activity.

A CASB 2.0 solution delivers the following benefits:

1. **Improved security efficacy**
2. **Reduced operational overhead and expense**
3. **Better user experience**

A comprehensive CASB 2.0 solution cannot be achieved through simplistic arm's length interoperability, but instead requires deep integration to gain real value. Such a solution should:

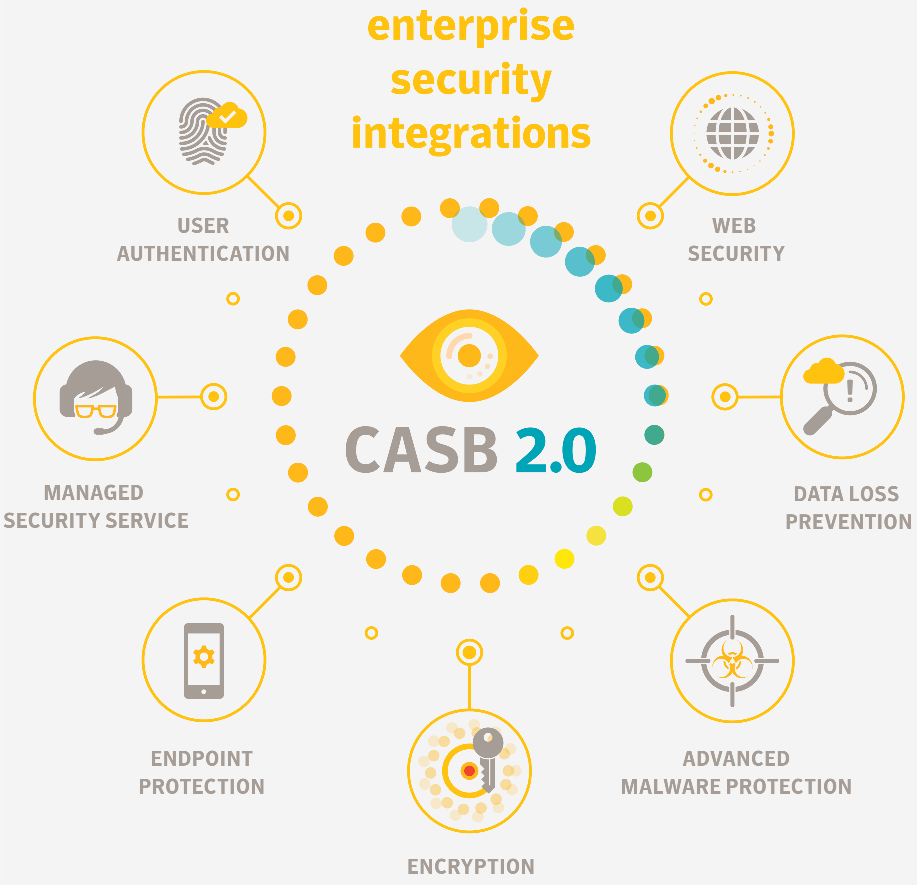
Share critical information between systems through native APIs

Enable consistent policies to be enforced across cloud and other channels

Integrate user interfaces to enrich management consoles for various personas

Reduce deployment complexity related to multiple security solutions

A full featured CASB 2.0 solution delivers significant advantages to enterprise organizations that want to fully embrace the cloud without compromising security.

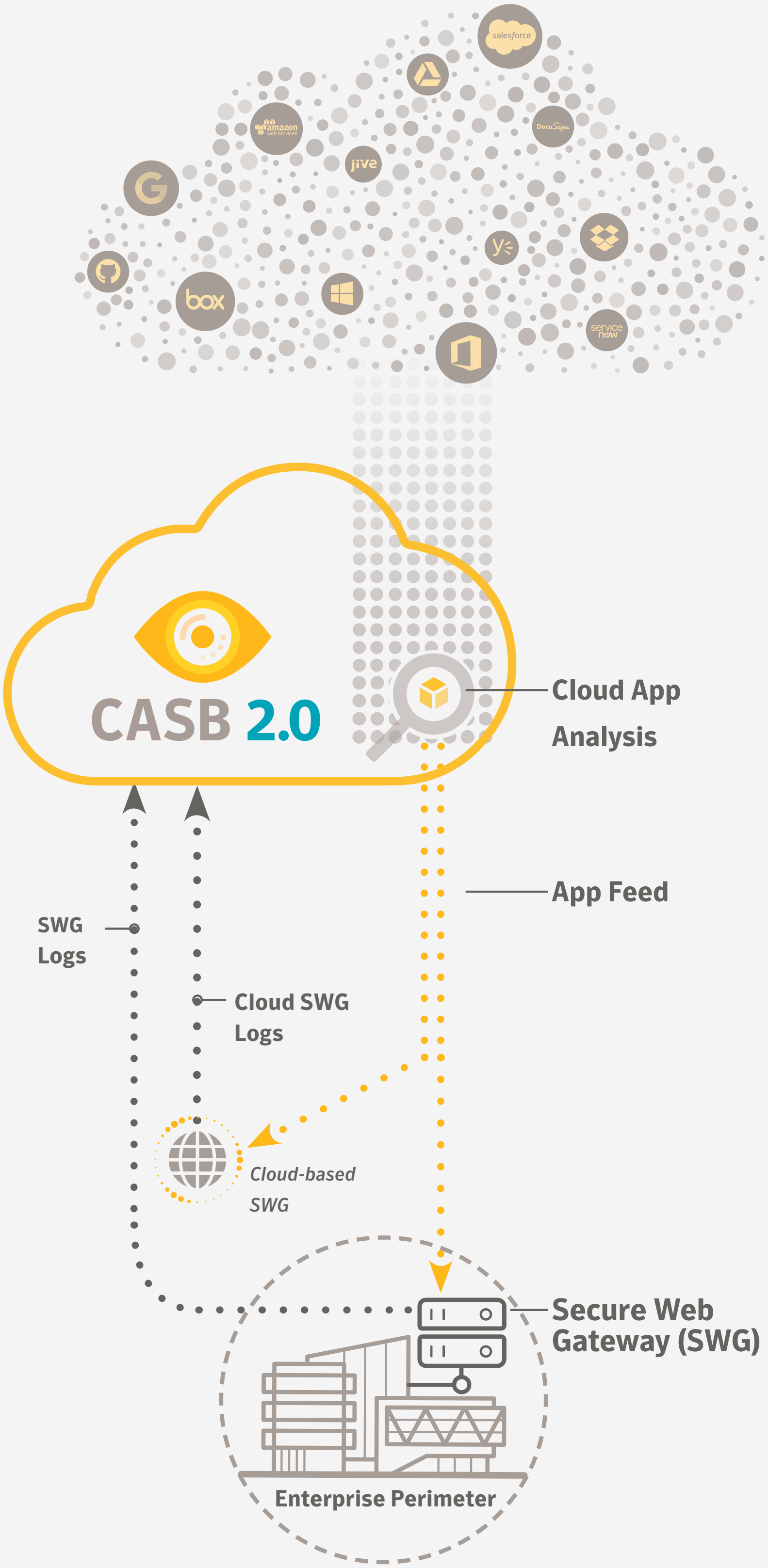


CASB & SWG
Don’t Just Discover Shadow IT, Control IT

Many organizations will require some form of Secure Web Gateway and CASB functionality. However, there are many pragmatic issues to consider when deploying both. How do you steer traffic between them? How many user authentications are required? How can I share information between these systems? How can I take action on risky apps that are discovered?

With a CASB 2.0 approach, the Secure Web Gateway and CASB solutions can be intelligently integrated to deliver more value.

1. **Empower your SWG with rich cloud app data**
   A robust CASB solution should have a powerful app database that can analyze tens of thousands of cloud apps based on dozens of security characteristics (i.e., SOC-2 compliance, MFA support). With CASB 2.0, this database can be automatically distributed to SWG solutions both on-prem and in the cloud, enriching their visibility capabilities. In fact, organizations that are reluctant to deploy anything in the cloud can leverage their existing on-prem SWG hardware to gain CASB functionality.
2. **Get Dynamic Control of Shadow IT**
   Robust CASB solutions are able to discover Shadow IT, including risky apps and services used by employees. But how can organizations take action on this information? Crafting individual policies to restrict or block each risky app based on their name or URL is tedious work—especially when new apps are discovered every week. Instead, a CASB 2.0 solution should enable you to define a dynamic policy based on critical risk attributes, such as the Business Readiness Rating or SOC-2 compliance. These policies can then be enforced by the SWG, without requiring constant manual updates. The CASB 2.0 solution continuously informs the SWG of new apps and services that match the selected criteria, automating control of Shadow IT.
3. **Simplify Deployment**
   Deploying both SWG and CASB can be cumbersome. A CASB 2.0 solution should simplify this deployment by steering traffic between the solutions (streamlined proxy chaining), unifying authentication, automating log ingestion, and integrating the user interface. These and other practical features provide a better user experience for administrators, and reduce operational overhead.

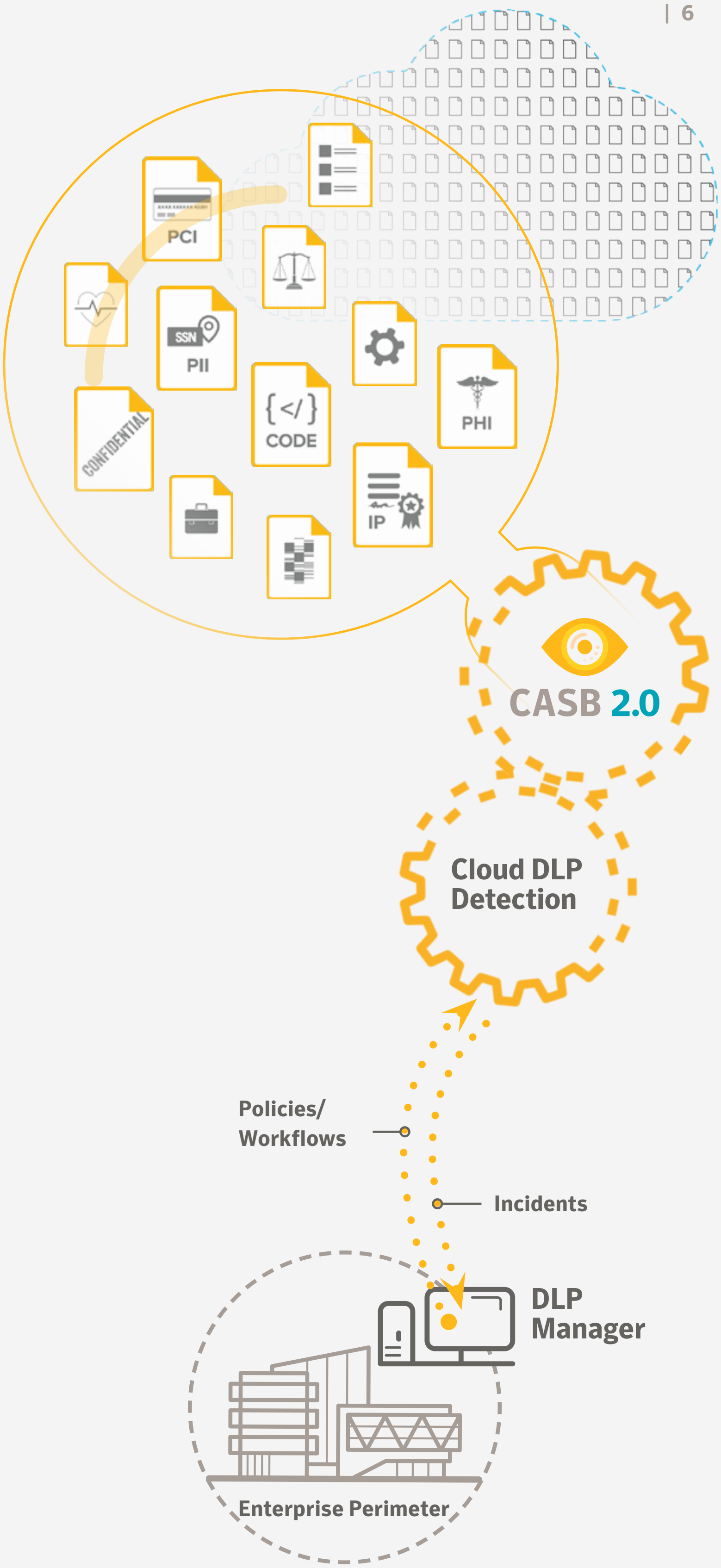


CASB & DLP
Eliminate Multiple Islands of DLP

The rapid growth of cloud apps and services, especially file sharing, has increased the need for effective Data Loss Prevention solutions. The cloud is becoming the de facto mechanism for sharing content, including sensitive or regulated data. Many companies have already invested in DLP solutions that address many channels, including storage, email, endpoint, and others. They are looking for a seamless way to extend their solutions to the cloud.

With a CASB 2.0 approach, DLP can be seamlessly integrated across all channels, ensuring effective coverage and simpler operation.

1. **Deploy consistent DLP policies on-prem and in the cloud**
   A CASB 2.0 should be able to leverage your existing, finely tuned DLP policies, workflows, and business logic to cloud apps and services. This avoids disparate or inconsistent results as you enforce DLP across multiple channels. It also reduces operational overhead, avoiding having two teams managing DLP, along with the efforts to replicate policies and workflows.
2. **Gain optimal performance through native cloud APIs**
   While some have suggested using ICAP with on-prem DLP detection technology to preserve policies, this approach introduces a significant waste of WAN bandwidth and added latency. Instead, a CASB 2.0 solution should leverage cloud-based detection along with a native API to the CASB solution, so that content that is stored in the cloud is also analyzed in the cloud, avoiding shuttling content back and forth to on-prem. A native API solution also enables the sharing of rich attributes between the CASB and the DLP systems, such that traditional DLP solutions can leverage cloud-specific attributes for analysis and policy creation.
3. **Empower DLP with CASB Insights**
   CASB 2.0 solutions should infuse traditional DLP solutions with cloud-specific information. For example, it should enable DLP to leverage additional attributes that are unique to the cloud when creating policies, such as “unshare a link.” Similarly, detailed user activity in the cloud or user threat scores can be shared through the DLP console. The end-goal is to empower the DLP specialists to have complete visibility and control of the functions relevant to them through a single console.



CASB & Encryption
Deliver End-to-End Information Rights Management

Many CASB 1.0 solutions have encryption or tokenization features. These typically involve encryption of content *en route* to cloud apps and services, and then decryption of that same content as it is pulled from the cloud app. However once sensitive content is downloaded from the cloud, it may travel anywhere. End users can upload such content to personal cloud apps, copy it to their own personal devices or USB sticks. In effect, the organization can lose control of that sensitive content.

A CASB 2.0 approach can provide a more robust solution by intelligently integrating end-to-end encryption with CASB technology. Through this approach, content can be encrypted en route to cloud apps and services, and remain encrypted as it is downloaded to various endpoints. Such an approach has many advantages:

1. **Security that follows the data**
   Encryption can be trigged based on a variety of criteria, such as identified PII, PCI, PHI or other sensitive content. As this content is downloaded, it remains encrypted regardless of where it travels—ensuring data protection regardless of how it is propagated. Users must authenticate to be able to view the content, leaving control of the content in the hands of the enterprise.
2. **Content access that can be revoked at any time**
   A robust CASB 2.0 solution should also be able to track content as it travels, and at any point in time, an organization should be able to revoke access to that content. For example, the organization may become uncomfortable with how the content has spread or the data may no longer be valid. The concept of pushing a button to digitally shred such content is powerful.
3. **Multi-platform support**
   While some cloud apps have similar features built into their infrastructure, it is more valuable to have a solution that works across all cloud apps in a consistent way. This provides the security team more flexibility to apply rules across their landscape of cloud apps and services without having to deal with limitations or nuances of individual cloud app features.

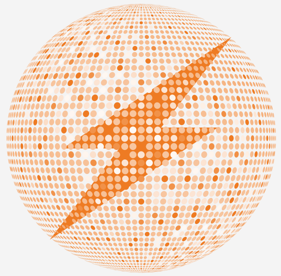
CASB & Malware Protection

Tap Global Threat Intelligence to Protect Cloud Content

Malware, including advanced malware, not only affects files and systems within your network perimeter, but in your cloud accounts as well. Given content may enter cloud apps through direct cloud-to-cloud interactions or may be created natively within cloud apps—traditional perimeter protection is no longer sufficient. Malware in cloud apps is also problematic as many users will sync and share their computing environments with the cloud, enabling malware to spread rapidly.

Many early CASB solutions tap simple open source malware analysis engines, but lack robust advanced malware protection. A CASB 2.0 solution should leverage best-of-breed malware protection technology to fully protect your assets in the cloud.

1. **Leverage Global Threat Intelligence**
   CASB 2.0 solutions should tap best-of-breed global threat intelligence to analyze cloud content, including file reputation analysis and tracking latest breach data on a wide range of cloud apps and services. This provides more consistent coverage across an enterprise's information communication landscape.
2. **Block & Neutralize Malicious Files**
   CASB 2.0 solutions should leverage industry leading A/V scanning engines to be able to fully vet content flowing in and out of cloud apps, as well as data at rest within cloud apps. This analysis should be actionable, allowing users to block and quarantine malicious content, preventing it from infecting your organization.
3. **Detect Zero-Day Threats**
   A CASB 2.0 solution should integrate Advanced Threat Protection (ATP) to be able to detect zero-day threats in your cloud accounts and transactions between users and cloud apps. Cloud sandboxing should also be engaged to analyze unknown files for malicious behavior.



Global Threat Intelligence Network

AV Scanning

Sandboxing

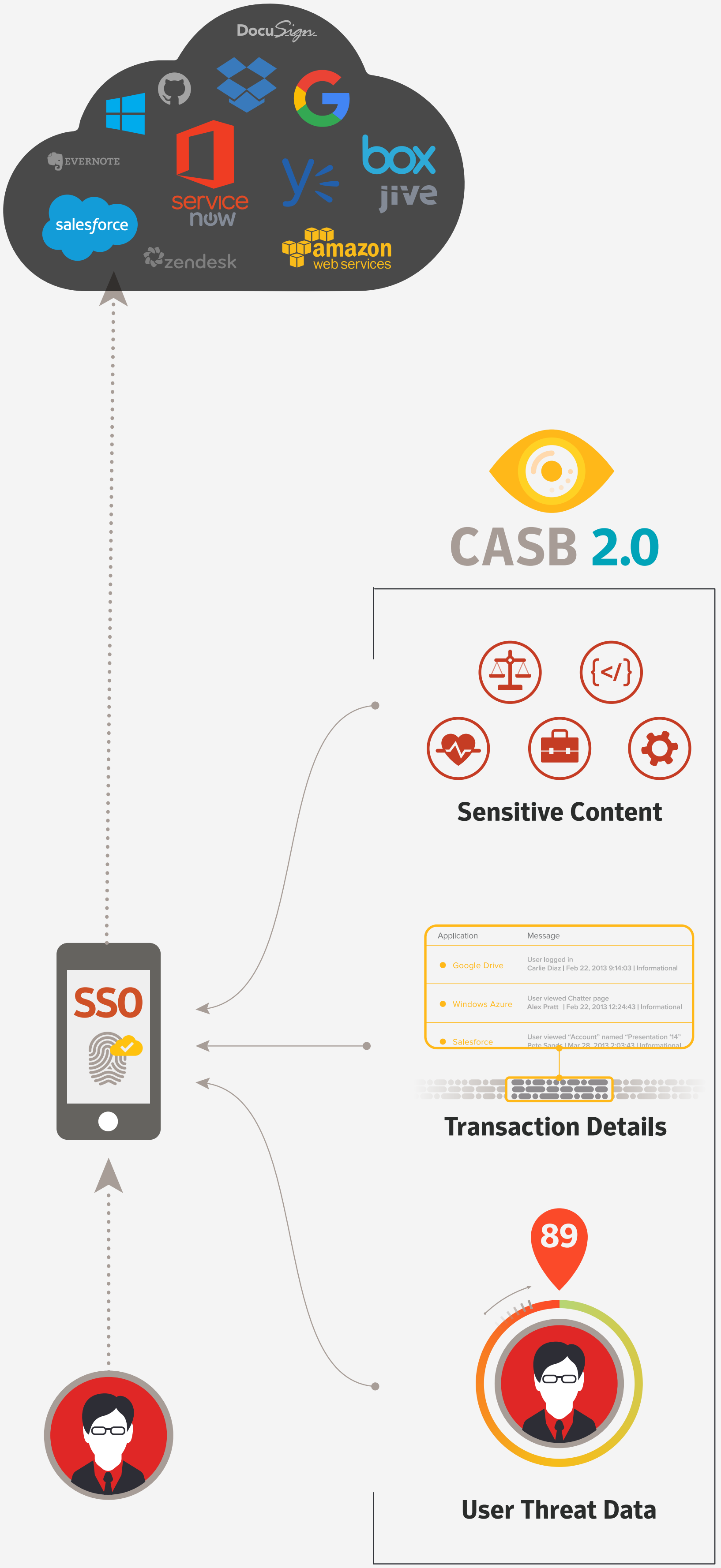
CASB & User Authentication

Go Beyond Single-Sign-On (SSO)

User authentication is an integral component of any cloud security framework. Most CASB 1.0 products support interworking with a range of SSO solutions, typically through SAML integration, to streamline authentication.

A CASB 2.0 approach can provide a deeper level of integration. Rather than a one-way sharing of information (SSO to CASB), CASB 2.0 solutions can leverage a two-way sharing of information, so that CASB insights can inform user authentication solutions. This can prove very valuable, enabling organizations to dynamically adjust their access requirements based on real-time risk conditions in the network, a concept known as Adaptive Authentication.

For example, if a user's threat score exceeds a certain level (based on suspicious activity), the system can trigger the requirement for multifactor authentication (MFA) for that user. Similarly, if a user is accessing sensitive content, the organization may want to step up their MFA requirements. A comprehensive solution would allow organizations to define granular policies based on a wide range of transaction attributes that enable them to step-up authentication requirements as users pursue high risk transactions.



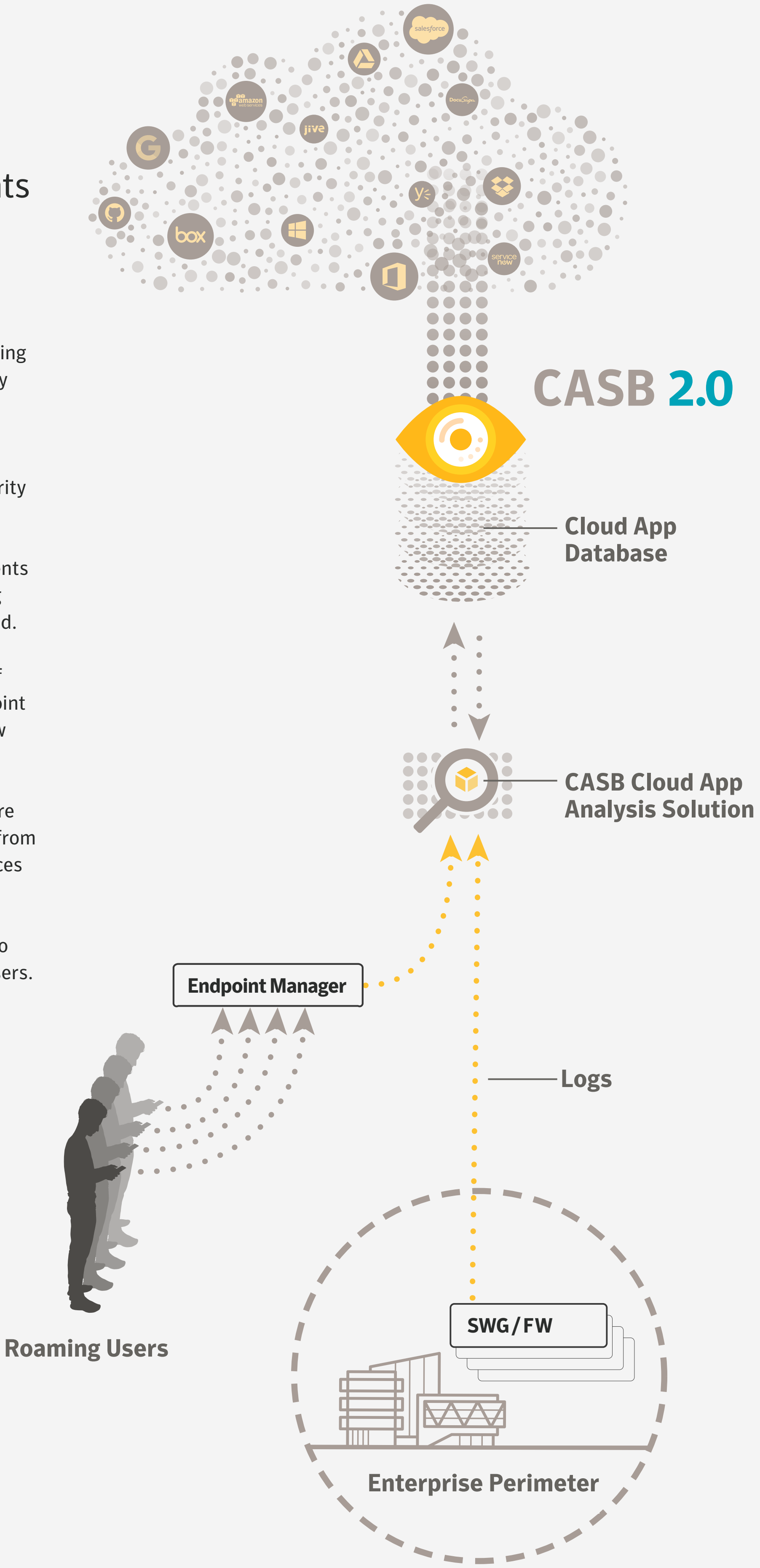
Application	Message
Google Drive	User logged in Carlie Diaz | Feb 22, 2013 9:14:03 | Informational
Windows Azure	User viewed Chatter page Alex Pratt | Feb 22, 2013 12:24:43 | Informational
Salesforce	User viewed "Account" named "Presentation '14" Pete Sands | Mar 28, 2013 2:03:43 | Informational

CASB & Endpoint Protection
Streamline Endpoint Deployments

Many CASB solutions often leverage agent technology to help steer traffic to a CASB gateway or to help with policy enforcement. However, many organizations may already have endpoint solutions in place and often are reluctant to deploy *yet another agent*. In addition, existing endpoint solutions have insights regarding user activity that could be valuable for CASB solutions to leverage.

CASB 2.0 solutions can bring more value by doing a deeper level of integration with existing endpoint security solutions. One obvious simplification is integrating the CASB agent functionality with mainstream endpoint security solutions, thereby reducing the number of agents that need to be managed and deployed, and expanding the footprint of available devices that are CASB-enabled.

In addition, CASB 2.0 solutions can improve analysis of Shadow IT by leveraging telemetry from existing endpoint agents. The most common source for CASB 1.0 Shadow IT discovery solutions are logs from firewalls or secure web gateways. These are essential, but are limited to analyzing on-prem traffic. But what about users who are roaming outside the corporate environment? Working from home, from their local coffee shop or from remote offices that may not have the same firewalls? These roaming users create a blind spot for Shadow IT analysis. CASB 2.0 solutions can leverage data from endpoint agents to expand their Shadow IT analysis to include off-prem users.

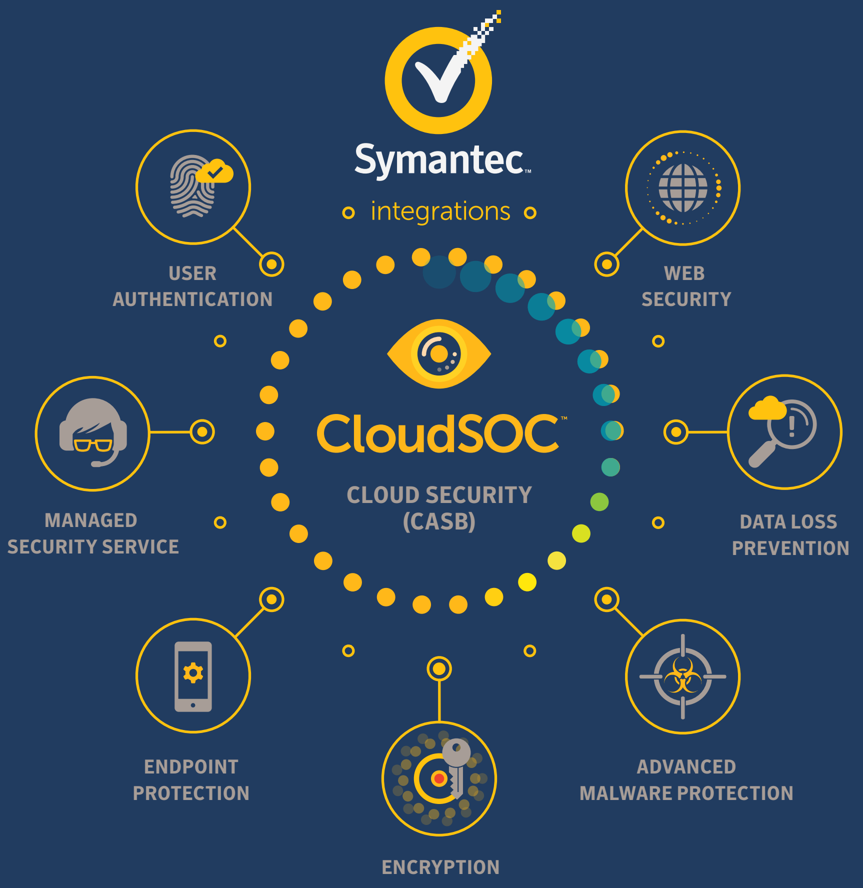


Conclusion

These are just some examples showcasing how integrating CASB technology with core security technologies can deliver significant value for organizations migrating to the cloud. Leveraging CASB 2.0 solutions, you can increase the efficacy of your security framework, avoiding incidents from "falling through the cracks" between various security solutions. You can also reduce operational overhead and expense, and improve overall user experience—both for administrators and end users. Rather than deploying "islands" of security that solve individual problems, a more comprehensive CASB 2.0 approach helps organizations knit together a holistic security framework that seamlessly covers both on-prem and cloud related activity.

Get better security with less complexity

Deploy a cloud security solution that integrates with your existing security infrastructure. A Symantec solution with CloudSOC provides greater security coverage, reduces operational complexity, and provides an optimal user experience.



For more info on Symantec CloudSOC CASB and its industry leading integrations with Symantec Enterprise Security Systems, visit **go.symantec.com/casb**

symantec.com +1 650-527-8000

About CloudSOC

Data Science Powered™ Symantec CloudSOC platform empowers companies to confidently leverage cloud applications and services while staying safe, secure and compliant. A range of capabilities on the CloudSOC platform deliver the full life cycle of cloud application security, including auditing of shadow IT, real-time detection of intrusions and threats, protection against data loss and compliance violations, and investigation of historical account activity for post-incident analysis.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.