

# The Cloud Control Point for continuous real time protection



# Do you know where all your sensitive data is today?

## How can a Cloud Access Security Broker (CASB) enhance your cloud security?

### What is a CASB?

With the large adoption of cloud, IT organizations may have lost track of cloud services and cloud native applications that are used inside an organization by employees. Some of them are not compliant with the company's security requirements. This unsanctioned software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS), known as Shadow IT, represents a major security vulnerability for organizations.

A Cloud Access Security Broker, or CASB, is a central point where you can manage and better secure cloud services to which your sensitive data could be sent. Atos is providing a CASB service able to provide visibility and control over shadow SaaS usage while enabling employees to remain productive.

CASBs have become essential elements of cloud security strategies, helping organizations use the cloud and protect their sensitive data in the cloud. Security and risk management leaders concerned with their organizations' cloud use should evaluate CASBs and use Gartner Magic Quadrant for Cloud Access Security Brokers research<sup>1</sup> to assess the market.

### No blind spots

The need to restore visibility and reassert ownership and control has become a major driver for hybrid cloud security solutions. With real-time monitoring and analytics, a business gains global visibility into the consumption of IT resources inside and outside the organization.

Only when a company has visibility across all platforms can it implement consistent policies for its processes.

To know more on how to build trust in hybrid cloud, please visit:

[atos.net/en/solutions/cyber-security-products/building-trust-hybrid-cloud](https://atos.net/en/solutions/cyber-security-products/building-trust-hybrid-cloud)

### Atos Cloud protection approach



#### Identify

- Identify sensitive data in cloud services
- Understand access to and sharing of sensitive data
- Discover and govern the use of cloud services
- Detects threats - compromised accounts, insider threats, malware



#### Control

- Define and enforce access policies based on device, geography and role
- Delete high-risk files violating Data Loss Protection (DLP) policies
- Quarantine mid-risk files violating DLP policies
- Autonomously remediate low-risk files violating DLP policies
- Receive in time relevant information about security incidents



#### Protect

- Use Atos Security Operation Center experts to detect and remediate the cloud security incident in real time
- Continuously monitor and update cloud security policies to minimize new risk

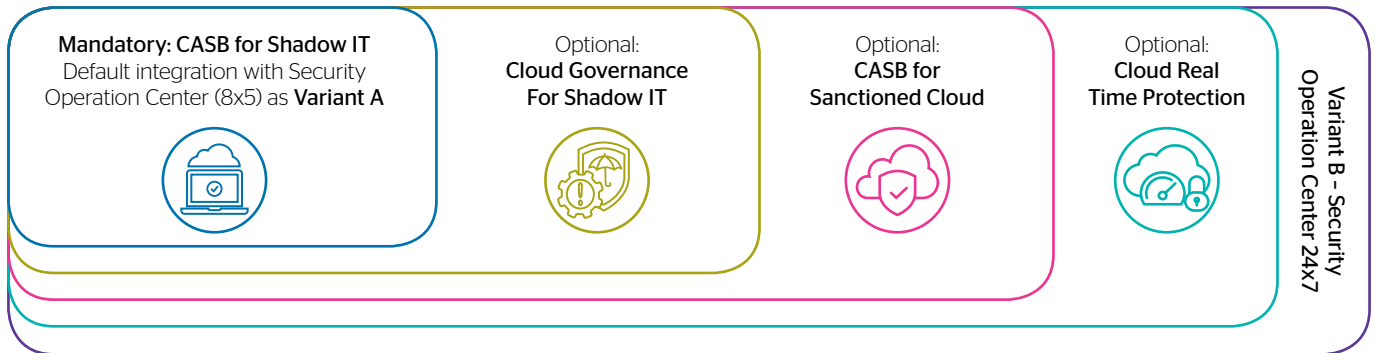
<sup>1</sup>Gartner Magic Quadrant for Cloud Access Security Brokers, October 2019

<https://www.gartner.com/en/documents/3970548/magic-quadrant-for-cloud-access-security-brokers>

# Atos' CASB Service

## Get visibility and control of enterprise applications and data in the Cloud

Atos' Cloud Access Security Broker (CASB) service acts as a security control point for cloud services used by an organization and provides agreed mitigation steps via our Atos Security Operation Center experts. The Atos' CASB service modules have the following structure:

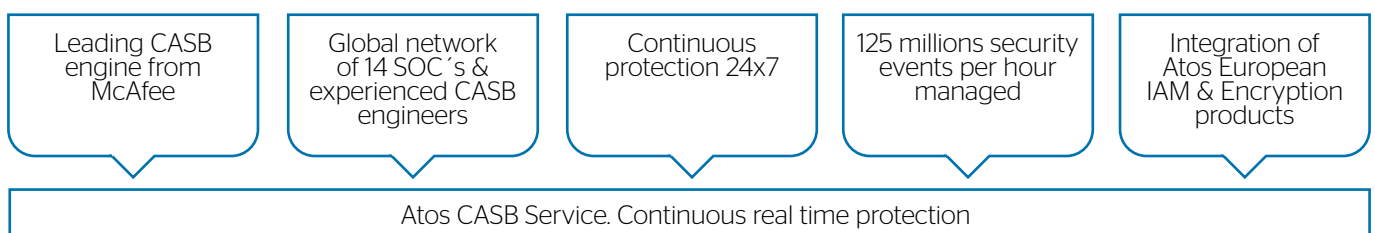


CASB for Shadow IT	Cloud Governance for Shadow IT	CASB for Sanctioned Cloud	Cloud Real Time Protection
<p>This package provides discovery of cloud services in use, their access account, assessment of cloud service security risk and usage trends:</p> <ul style="list-style-type: none"> <li><b>Cloud Services Discovery:</b> overview of cloud service usage, across the organization</li> <li><b>Assess Risk:</b> overall rating on cloud service credibility, using the world's largest accurate registry of cloud services</li> <li><b>Detect Data Exfiltration and Proxy Leakage:</b> detection of malware operating on the enterprise network that leverages the cloud as a vector for data exfiltration</li> </ul>	<p>This package provides a way of mitigating risks based on defined criteria:</p> <ul style="list-style-type: none"> <li><b>Cloud Service Governance:</b> workflow to automatically or manually classify services based on risk criteria and enforcement of acceptable use policies through coaching and/or blocking</li> <li><b>Customizable Risk Scores:</b> ability to customize and preview in real time the risk scoring criteria for all services to match an organization's security priorities</li> <li><b>Cloud Enforcement Gap Analysis:</b> allowed and denied statistics and highlights gaps in cloud policy enforcement with recommendations to close gaps</li> </ul>	<p>This package monitors and provides controls for sanctioned cloud services by capturing an audit trail of all user activity for forensic investigations:</p> <ul style="list-style-type: none"> <li><b>User Behavior Analytics:</b> automated detection of abnormal behaviors when there are deviations from typical patterns using data science and machine learning</li> <li><b>Activity monitoring:</b> visibility on sanctioned cloud usage and post-incident forensic investigations</li> <li><b>Data Loss Prevention:</b> discovery and prevention of sensitive data being created or uploaded in the sanctioned cloud by leveraging content analytics engine</li> <li><b>Threat protection:</b> detection of anomalous cloud activities or its usage pertaining to compromised accounts, insider threats, and privileged user misuse</li> </ul>	<p>This package provides real-time protection for Data Loss Prevention and Access Management for all Sanctioned cloud services in use:</p> <ul style="list-style-type: none"> <li><b>Synchronization of organization certificates</b> to recognize managed and unmanaged devices for protection of downloaded data</li> <li><b>Access control policies</b> enforcement through integration with IAM</li> <li><b>More granular information</b> such as which device was used based on API and reverse proxy</li> <li><b>Real time mail protection</b> for O365 and Gmail</li> </ul>

### Why choose Atos?

Thanks to a strong partnership with McAfee, Atos ensures that customers receive the highest level of support and expertise from the Atos CASB service. In addition, Atos cybersecurity products have been certified by McAfee, the device-to-cloud cybersecurity company, and are part of the [Security Innovation Alliance \(SIA\) program](#).

McAfee and Atos have partnered to provide a Cloud Access Security Broker (CASB) Service combining best of breed technology from McAfee MVISION Cloud and Atos' cybersecurity products: Trustway for data protection and Evidian for access management. The combined offer ensures greater control to customers for their data encryption and Identity and Access Management needs across their multi-cloud environment. Operations are performed by trained security experts with an in-depth knowledge of McAfee technologies and Cybersecurity.



# About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

**atos.net**

**atos.net/cloud-security**

Let's start a discussion together



Do not hesitate to contact us:

[atos.net/en/solutions/cyber-security-products/contact-us-cybersecurity](https://atos.net/en/solutions/cyber-security-products/contact-us-cybersecurity)

Atos, the Atos logo, Atos | Syntel, and Unify are registered trademarks of the Atos group. March 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.