

# Managed CASB

Accelerate your secure cloud migration strategy

Product Sheet: Managed Security

Adopting cloud-based business apps results in greater business agility but an IT security nightmare. Software as a service (SaaS) enables anyone to bypass IT security and provision so-called "shadow IT" apps from the cloud—exposing customer and employee data. That's why CIOs and CISOs use cloud access security broker (CASB) solutions to automatically manage shadow IT risks

## Automated risk management for shadow IT

Masergy Managed CASB consolidates your corporate SaaS app security policy enforcement into a single cloud-based solution. With a Masergy Managed CASB solution, users connected to your corporate network are automatically blocked from installing unsanctioned SaaS app from the cloud and redirected to use safe apps. Setup is simple, with nothing for users to install. And IT managers get comprehensive visibility and control over user cloud app usage in a simple and secure web-based portal.

## Threat protection to work from anywhere

Masergy Managed CASB delivers end-to-end data and threat protection for all applications on any device. With support for SaaS apps such as Microsoft 365, Google Workspace, Salesforce, along with tens of thousands of enterprise cloud apps on the market today, Masergy Managed CASB helps you control corporate data flows to and from the cloud in real time. Extend protection via both APIs and agentless proxies to ensure corporate information stays protected on both mobile and devices—whether located in the office or working remotely.

## Best of breed CASB powered by Forcepoint

Masergy partnered with Forcepoint, named a Leader in the Gartner Magic Quadrant for Cloud Access Security Brokers. By integrating Forcepoint's industry-leading CASB technology with Masergy's managed detection and response services, Masergy Managed CASB delivers 24/7 incident response from live security analysts in three our global Security Operations Centers.

## Per-User and Per-Device Protection For SASE Strategies



### Features

- Turnkey managed protection for all corporate devices accessing cloud apps
- Powered by Forcepoint, recognized as a Leader in the Gartner Magic Quadrant for CASB
- Comprehensive visibility and control of cloud access at a per-user and per-device level from a single interface

### Benefits

- Enables your organization's cloud strategy while protecting sensitive data on any device using any SaaS app
- Scales on demand and deploys quickly for fast time-to-value
- Delivers mandatory 24/7 continuous security monitoring for rapid detection and response

## Enables SASE cybersecurity strategies with Managed CASB

CIOs and CISOs agree that the convergence of networking and security using the Gartner framework called Secure Access Service Edge (SASE) delivers a new level of cloud-ready agility. Masergy's SASE approach is unique because it brings together best-of-breed technologies from leaders in their respective markets into a single service from one provider. That's why we integrated Forcepoint CASB into our global software defined network fabric—enabling a turnkey service that comprehensively secures all your cloud applications on a worldwide scale.

Deploying a Masergy SASE solution provides secure connectivity for every user and device connecting to site-to-site, site-to-cloud, and any hybrid combinations that matches your business needs. And it is all managed 24/7 by Masergy security analysts in global security operations centers strategically located in North America, Europe, and Asia.

## Comprehensive protection for cloud-first IT environments

Masergy Managed CASB powered by Forcepoint is crucial for enabling your organization's cloud-first IT strategy by delivering protection of sensitive data on any user device with:

### User & Entity Behavior Analytics (UEBA)

Masergy Managed CASB can generate baselines for user behavior to detect and respond to malicious insider activity in real time. In the event of compromised credentials and account hijacking, UEBA is a must for distinguishing legitimate data access from malicious data access.

### Data Loss Prevention (DLP)

The managed data loss prevention (DLP) tool enables a customizable, fine-grained approach to data security, protecting information based on its content and the context in which it's being accessed. Use pre-built data patterns, build your own, or import from on-premises DLP systems via Internet Content Adaptation Protocol (ICAP) for more granular policies

### 256-bit Data Encryption

Masergy Managed CASB enables SaaS-independent encryption of data-at-rest. Leverage full-strength Federal Information Processing Standards (FIPS) compliant 256-bit Advanced Encryption Standard (AES), while maintaining normal app functionality—a dual system of control that dramatically increases the safety of data in the cloud

### Contextual Access Control

Set granular policies based on user-specific devices, locations, and more to allow or block access to data in the cloud or anywhere else on your corporate network.

### Seamless Identity Management with Multi-Factor Authentication (MFA)

Masergy Managed CASB comes with a native identity and access management system with MFA or integrates with Microsoft® Active Directory and all major Identity as a Service (IDaaS) solutions. Dual-Security Assertion Markup Language (SAML) termination ensures that the strength of SAML Single Sign-On (SSO) is preserved, without the added phishing risk that comes with competing proxy architectures.