MASERGY

Managed CASB
(Cloud Access Security Broker)

The Enterprise Application Security Paradigm Has Changed

The rapid adoption of Software-as-a-Service (SaaS) has changed the security paradigm for enterprise applications. Provisioning is no longer an activity performed solely by IT. Business managers are independently provisioning cloud apps and skipping security practices, leaving enterprise data exposed and forcing IT/security teams into reactive mode as they try to manage risks with ineffective "whack-a-mole" approaches using their existing security tools.

The most critical SaaS security challenges include:

- Assessing SaaS vendor inherent security risks that are neither readily measurable nor apparent.
- Restricting sensitive data from being uploaded into cloud applications (sanctioned or unsanctioned) and shared into insecure environments.
- Enabling quick detection of stolen credentials and malicious insider usage, and responding to incidents before serious damage is done.
- Extending protection to mobile devices where agents or management is impractical.
- Preventing cloud applications from turning into malware conduits.
- Regulating identities and enforcing appropriate authentication to streamline user experience and productivity while simultaneously managing risks.

Key Benefits:

- Enables your organization's SaaS strategy while protecting sensitive data on any device using any cloud app
- Scales on demand and deploys quickly for fast time-to-value
- Streamlines user security experience to enhance productivity
- Fully managed service optimizes constrained security resources
- Delivers mandatory 24/7 continuous security monitoring for rapid detection and response

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

MASERGY

Get Comprehensive Managed Security Born for the Cloud

Today's threat landscape requires an advanced security approach that goes beyond prevention to include rapid detection and response. While Cloud Access Security Brokers (CASB) consolidate cloud security policy enforcement and solve SaaS security problems, only the largest organizations have the in-house resources and expertise on-hand to enable their value with 24/7 monitoring and response.

Masergy Managed CASB delivers an optimized combination of innovative technology, resilient processes, global 24/7 security operations centers, and expert security analysts all working together to comprehensively and scalably manage SaaS security risks. As a fully managed service, Masergy enhances your constrained security budgets while enabling your team to embrace and accelerate your organization's SaaS initiatives.

One Security Policy for your Entire Cloud App Suite

As organizations adopt a cloud-first approach to IT, they must also avoid a patchwork of point solutions that cannot provide consistent and scalable controls across all cloud apps. Masergy's Managed CASB solution is built from the ground up for visibility, control, and compliance in the cloud, offering end-to-end data and threat protection for all applications on any device. With support for SaaS apps like Office 365 and G-Suite, Salesforce and any of the other thousands of cloud apps that are on the market today, Masergy's Managed CASB solution is built to manage risks with officially sanctioned and unmanaged Shadow IT apps all with one solution.

Visibility

Gain Mission-Critical Visibility and Analytics

Our Managed CASB solution gives you a single-pane, cross-app view into the details of your employees' cloud usage, and allows you to uncover and automatically address potential threats via configurable actions.

Unsanctioned Shadow IT Applications

Our Managed CASB's big data analytics and risk intelligence help uncover Shadow IT applications, automatically categorize those apps, and rate apps based on risk. Leverage unmanaged app controls to block these apps or encourage the use of alternative sanctioned applications.

Comprehensive Protection and Management

At-rest Protection – Our Managed CASB solution leverages APIs for additional visibility and control over data stored in cloud apps. The Managed CASB crawls files within any app that provides access via an API to identify sensitive data and threats, which informs the placement of controls around data so that organizations can govern sharing and access more effectively.

In-Transit Protection – Our Managed CASB Solution uses a combination of reverse, forward, and ActiveSync proxies to protect data-in-transit. Reverse and ActiveSync proxies are an agentless means of securing access to any cloud app from any device or network. Forward proxies secure traffic from managed devices, detect shadow IT, block risky unsanctioned applications, and redirect users to safe, sanctioned apps.

Masergy Managed CASB Architecture

Threat Protection

Dynamically Remediate Threats with Advanced Threat Protection (ATP)

Our Managed CASB solution's machine-learning enabled managed ATP can identify both known and unknown malware in real-time. By analyzing hundreds of file characteristics, the system can detect and stop zero-day threats at upload and on download.

User and Entity Behavior Analytics

With user and entity behavior analytics (UEBA), our Managed CASB solution 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 Protection

Prevent Data Loss – 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.

Protect Mobile – Where mobile devices are widely used, organizations must consider mobile security when choosing a solution to protect cloud data. Masergy's managed agentless proxies enable data security for any app on any mobile device without sacrificing user privacy. Enforce device-level security policies, selectively wipe mobile data, and more.

Enforce Access Control – Contextual access control governs where and how employees can access corporate data. Granular policies can be defined based on access method, device, location, and more. Organizations can block, allow, or provide intermediate levels of access based on a user's access context.

Encrypt Cloud Data – For organizations where the confidentiality of data is of the highest importance, Masergy Managed CASB enables SaaS independent encryption of data-at-rest. Masergy provides 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.

Comprehensive Protection and Management

Intelligent Zero-day Protection – Our Managed CASB solution offers AI-based Zero-day detection and app protection. A combination of intelligent Shadow IT discovery capabilities and unmanaged app controls prevent data loss from any application, including previously unknown apps. The Zero-day engine automatically detects new upload paths in known and unknown apps to restrict the upload of sensitive regulated data immediately.

Rapid Deployment – Our Managed CASB's agentless proxies deploy in minutes—setup is simple and straightforward, with nothing to install for either admins or users. Our Managed CASB solution is hosted globally on the elastic AWS infrastructure, making it highly scalable.

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

MASERGY

Identity

Manage Identity Seamlessly – Ensuring proper control over identity is essential in protecting data in the cloud. Our Managed CASB solution offers a native Identity and Access Management (IAM) system, complete with adaptive step-up multi-factor authentication. Managed CASB also integrates with 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 some proxy architectures.

Step-Up Multi-Factor Authentication – Our Managed CASB offers multi-factor authentication (MFA) to verify users' identities. Authentication methods include passwords, SMS tokens, hardware tokens, and more. In the event of a suspicious login, MFA can be used in a step-up fashion, requiring users to provide risk-based authentication to access corporate data.

Session Management – Our Managed CASB offers session management to defend against account hijacking. If a user is inactive for an extended period of time, a timeout can be forced or re-authentication can be required to prevent malicious parties from accessing any cloud app session.

Masergy and Bitglass Partnership

Masergy has partnered with Bitglass to deliver an integrated turnkey solution that combines industry-leading CASB technology with our proven Managed Detection and Response platform for comprehensively and scalably managing SaaS security risk. Bitglass is consistently recognized as a CASB visionary thanks to their proven rapid deployability, straightforward policy management, innovative data and threat protection functionality, and integrated mobile data protection and identity/SSO capabilities.

Masergy Managed CASB helps organizations offload alert monitoring and response from overworked security/IT teams to our 24/7/365 global Security Operations Center (SOC). Masergy analysts have the certifications, tenure, and aptitude to meet the highest standards required for SOC analysts, and do so with one of the industry's lowest churn rates.

Masergy's Managed Detection and Response Platform

Unified Enterprise Security

Masergy Managed CASB requires a supporting deployment of Unified Enterprise Security, Masergy's Managed Detection and Response platform. Flexibility and scalability are design principles for this platform, so new solutions like CASB can readily be integrated while leveraging Masergy's patented machine learning algorithms that optimize security tool effectiveness.

Features:

- Quickly extend detection and response capabilities to SaaS with Multimodal Architecture/ flexible deployment options (APIs, reverse or forward proxies)
- Gain visibility and control of unsanctioned cloud apps and provide employees with sanctioned alternatives
- Protect data with integrated Data Loss Prevention (DLP) or extend existing systems via ICAP
- Leverage integrated User Behavior and Entity Analytics (UEBA) to stop malicious activity and to mitigate credential theft
- Improve security posture and consolidate user experience with integrated Identity and Access Management (IAM) and step-up Multi-factor Authentication (MFA)

SUPPORTED CASB SOLUTIONS	▪ Bitglass (sold through Masergy) ▪ Netskope* ▪ Skyhigh* *Monitoring and response service only. Features will be different from those listed above
REQUIRED DEPLOYMENT	▪ Requires existing UES deployment
DEPLOYMENT TYPE	▪ Managed SaaS Security deploys as a module on UES Customer Premise Equipment

CONTACT US: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

MASERGY