

CLOUD ACCESS SECURITY BROKER.



Data now moves through dozens of cloud apps IT never approved — a broker sits at that chokepoint to see, control, and secure traffic that firewalls and endpoint agents never touch.

- SHADOW IT DISCOVERY
- DATA LOSS PREVENTION
- THREAT PROTECTION
- COMPLIANCE ENFORCEMENT

01 THE MECHANISM

Visibility & Discovery
Identifying every cloud app in use, including **shadow IT** never approved by security.

Data Security & DLP
Enforcing data policy as content moves **into, out of, and between** cloud applications.

Threat & Compliance
Detecting compromised accounts and **malware moving** through sanctioned cloud services.

02 THE FLOW

The Access Cycle CONTINUOUS

1

A user authenticates and connects to a **sanctioned or discovered cloud application**.

2

The broker inspects the session against **data, threat, and compliance policies**.

3

Policy actions apply in real time — **allow, block, encrypt, or require step-up authentication**.

The Exfiltration Cycle LIVE EVENT

1

A user uploads sensitive data to an **unsanctioned or misconfigured cloud app**.

2

The broker flags the transfer against **data classification and DLP policy**.

3

The session is blocked or quarantined, and **security is alerted before data leaves the environment**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Shadow IT Discovery	Inventories every cloud app in use, sanctioned or not.
Data Loss Prevention	Enforces content policy across upload, download, and sharing.
Threat Protection	Detects compromised accounts and cloud-native malware.
Compliance Enforcement	Applies regulatory policy consistently across cloud services.

04 CASB APPROACHES COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Network Firewall Alone	No	Doesn't see encrypted traffic inside sanctioned cloud apps.
Endpoint Agent Alone	No	Misses cloud-to-cloud data movement with no endpoint involved.
Manual App Approval List	No	Falls behind the pace of new SaaS sign-ups by business units.
Cloud Provider Native Controls	No	Covers one platform, not the multi-cloud environment.
CASB (Visibility + DLP + Threat Protection)	Yes	Applies one consistent policy across every cloud app in use.

CLOUD ACCESS SECURITY BROKER.

DISCOVER · PROTECT · ENFORCE

05 PROGRAM OPERATIONS

Shadow IT outnumbers sanctioned apps. Business units adopt new SaaS faster than IT can approve it.

Sanctioned apps still need policy enforcement. Approval alone doesn't stop risky sharing or misconfiguration.

API-based coverage lags inline control. Retroactive scanning misses data leaving in the moment.

Policy needs to travel with the data, not the app. The same file gets shared across a dozen different services.

06 CONTROL MAPPING

CSA CLOUD CONTROLS MATRIX

Cloud-specific control baseline spanning data, identity, and infrastructure domains.

NIST SP 800-53

Access control and audit requirements applied to cloud service providers.

GDPR / CCPA

Data residency and processing rules that broker policy must enforce in the cloud.

ISO 27017 / 27018

Cloud-specific security and privacy guidance extending ISO 27001 to cloud services.

07 WHAT THIS DOES NOT SOLVE

Unmanaged personal devices

A broker sees managed sessions; it **can't** inspect traffic on unmanaged personal devices.

Insider intent

Policy stops the mechanism of exfiltration, not the motive of a trusted user acting maliciously.

Vendor security posture

Sanctioning an app doesn't guarantee the vendor's own infrastructure is secure.

On-premises data flows

Cloud brokering has no visibility into **data** that never leaves the internal network.

08 MYTHS VS. REALITY

MYTH	REALITY
"A CASB replaces the firewall."	It complements network controls, it doesn't replace them.
MYTH	REALITY
"Sanctioned apps are automatically safe."	Misconfiguration inside approved apps causes most cloud breaches.
MYTH	REALITY
"Shadow IT is a small, manageable problem."	Most orgs have far more unsanctioned apps than approved ones.
MYTH	REALITY
"One broker covers every cloud risk."	Coverage depends on deployment mode and app integration depth.
MYTH	REALITY
"DLP alone stops data loss."	Without context on user, app, and risk, it produces blind spots.

09 SPEAK THE PROGRAM — KEY TERMS

CASB

Cloud Access Security Broker: a control point between users and cloud services.

SHADOW IT

Cloud applications in use without formal approval or visibility.

DLP

Data Loss Prevention: policy that stops sensitive data from leaving in the wrong way.

SANCTIONED APP

A cloud service that has been formally reviewed and approved for use.

API-BASED CASB

A deployment mode that scans data at rest via cloud provider APIs.

INLINE CASB

A deployment mode that inspects traffic in real time as it flows.