GENERAL DYNAMICS
Mission Systems

Route 66 Cyber™ Cloud Access Security Broker

Next-gen Cloud Security for the Modern Enterprise

Gain insight into cloud usage through a single pane view of all apps

Control how data and applications are shared and accessed in the cloud using proxy and deep API integration

Protect structured and unstructured data with data leakage and encryption

Detect suspicious behavior with User and Entity Behavior Analytics (UEBA), and stop known and unknown threats instantly

Secure data and apps between the cloud and any device via fast deployment, agentless architecture

Route 66 Cyber

The use of cloud resources for storage, applications and computing is becoming increasingly integral to the modern enterprise. Although the cloud is recognized as a way to enable broader collaboration and agility, lower infrastructure costs, and increase operational flexibility, many organizations have yet to fully adopt cloud services because of the security implications on their data. Cloud infrastructure and application service providers often do not offer the consistent level of data-centric security necessary to ensure protection of an enterprise's sensitive data.

Transitioning to the cloud could mean:

- Moving outside the company owned and controlled physical and security perimeters, such as buildings, servers/storage and firewalls
- Increased risk from unmanaged device access and external sharing
- Ceding control of the data and the keys protecting the data if not properly orchestrated.
- Relying on access and protection security operated by a 3rd party, resulting in a loss of visibility

Confidently migrate, manage, and monitor data across multiple cloud providers with Route 66 Cyber next-gen cloud access security broker (CASB).

What is a Cloud Access Security Broker (CASB)?

CASBs address security gaps in an organization's use of cloud services. A CASB is a data-centric solution that secures SaaS apps and IaaS platforms, from both managed and unmanaged devices to the cloud. CASBs mediate, or "proxy," all traffic between cloud apps and user devices – giving IT administrators unified and granular access control and visibility over enterprise data and user activities. CASBs extend the enterprise's own security policies into the cloud environment – enabling organizations to safely adopt the cloud.

Route 66 Cyber CASB Uniquely Provides:

Inline security, **any app or workload**

Agentless deployment, **any device**

Real-time data & threat protection, **anywhere**

High grade **encryption** and Enterprise Digital Rights Management **(EDRM)** delivered for the **cloud**

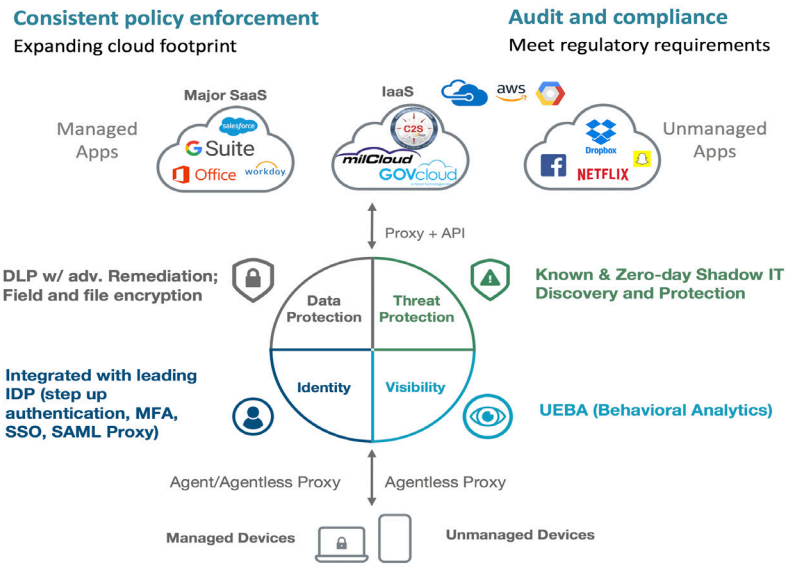
Route 66 Cyber™ Cloud Access Security Broker

Route 66 Cyber CASB Brings Four Essential Functionalities to Your Cloud

- Visibility into access and usage of sanctioned apps on managed and unmanaged devices; unsanctioned apps (Shadow IT) on managed devices.
- Compliance with regulations and data residency requirements, by providing audit logs, encrypting sensitive data-at-rest to protect against breach, and enforcing data leakage prevention policies to control access to regulated data.
- Data Security policies and enforcement preventing unwanted activity based on data classification, discovery, and user activity monitoring. Enforcement is applied through controls such as audit, block, quarantine, delete, and encrypt/tokenize.
- Threat Protection preventing unwanted devices, users, and versions of apps from accessing cloud services.

Route 66 Cyber CASB gives the enterprise full control over data – wherever it goes – through AES-256-bit encryption of data-in-use and seamless, independent key management. It encrypts data before it gets to the cloud service provider via proxy for user uploads/downloads and API for existing data-at-rest and data uploads from other premises and cloud apps.

Extend Your Enterprise Security Policies Into the Cloud and Beyond



And it goes further to provide the full spectrum of cloud security including data loss prevention (DLP), contextual access control, and user behavior analytics.

Machine learning automatically categorizes and optionally learns both known and new applications. Each is assigned a trust score enabling the organization to use the appropriate allow, block, or make read-only policy. These machine learning techniques also classify avenues for data leakage in each app on the fly, so that the organization maintains awareness of the application structure.

Features:

Deployment Options

- Cloud-based SaaS on GD Hosted, Public, and Community Clouds
- Private Cloud, Virtual Private Cloud, or on-premise

Supported Applications

- All major SaaS apps (e.g., Office 365, Salesforce, Box, Slack) via inline proxy and API
- Any SaaS or custom application via inline proxy; machine learning
- All major IaaS platforms

Supported IT Detection

- 400K+ application risk database, constantly updated
- Automated app identification and classification, machine learning
- Coach, block, read-only or machine learning-based DLP for any application

Supported Devices

- Any device, anywhere - fixed enterprise compute and server, mobile compute, and mobile devices
- Real-time, inline data and threat protection for both managed and unmanaged devices
- Agentless reverse proxy for web
- Agentless Activesync and MAPI proxies for mail
- Agent-based forward proxy for apps
- Transparent Single Sign On redirect from any devices

Data and Threat Protection

- Data-at-Rest Encryption
  - Structured data (fields) with patented searchable, full-strength encryption
  - Unstructured data (files)
  - Advanced GD EDRM and Crypto Core integation
  - Bring Your Own Key
- Data Leakage Prevention
  - Keyword, regex, exact data match, occurrence, include/exclude
  - 100's of prebuilt patterns
  - Remediation including allow, block, EDRM, encrypt, redact, quarantine, preview only
  - Integrates/syncs with any major network DLP
- Contextual access control
  - Managed vs. unmanaged device detection
  - Geofencing
  - Role, app, access method restrictions
- Identity
  - Native Single Sign On/Multi-Factor Authentication (MFA)
  - Integrates with all Identity as a Service (IDaaS) and MFA systems
  - Step-up multi-factor authentication
  - App session management override
- Cloud Security Posture Management
  - AWS, Azure, GCP support for Network, Storage, Compute, Identity
  - Visibility and remediation of IaaS configuration issues
- Visibility
  - Detailed logging of every cloud app transaction
  - Suspicious/malicious activity detection and alerting
  - Interactive dashboards and reports
  - Integrates with any major Security Information and Event Management (SIEM)

GENERAL DYNAMICS
Mission Systems

(781) 410-9400 • GDMissionSystems.com/moderndatasecurity • ModernDataSecurity@gd-ms.com

©2019 General Dynamics. All rights reserved. General Dynamics reserves the right to make changes in its products and specifications at anytime and without notice. All trademarks indicated as such herein are trademarks of General Dynamics. All other product and service names are the property of their respective owners. ® Reg. U.S. Pat. and Tm. Off.

D-R66C_CASB-3-0519
PRI-1901-0018