Request for Proposal: Cloud Access Security Broker (CASB) Software Solution

Table of Contents

1. Introduction and Background

Our organization is seeking proposals for a comprehensive Cloud Access Security Broker (CASB) solution to enhance our cloud security posture and ensure protection of our cloud-based resources. The selected CASB solution will serve as a critical security control point between our cloud service consumers and cloud service providers.

1.1 Market Context

- The CASB market is growing at CAGR of approximately 17.6% (2021-2026)
- Implementation costs typically range from $15,000 to $100,000+ annually
- The solution should align with current market leaders' capabilities while providing innovative features

1.2 Business Value Expectations

- Enhanced cloud security posture through unified control
- Improved visibility into cloud service usage
- Strengthened regulatory compliance capabilities
- Significant risk mitigation for cloud operations
- Optimized costs through controlled cloud usage

2. Project Objectives

2.1 Primary Objectives

1. Deploy a comprehensive CASB solution that provides visibility and control over cloud services
2. Implement robust data protection measures for cloud-hosted information
3. Establish real-time monitoring and threat detection capabilities
4. Enable granular policy management across cloud services
5. Ensure compliance with regulatory requirements
6. Optimize cloud service usage and associated costs

2.2 Strategic Goals

1. Reduce security incidents related to cloud service usage by 75%
2. Achieve 100% visibility into cloud application usage
3. Establish automated policy enforcement across all cloud services
4. Implement consistent data protection measures across cloud platforms
5. Enable proactive threat detection and response

6. Streamline security operations through automation

3. Scope of Work

3.1 Technical Architecture Requirements

1. Deployment Models
   - Forward proxy deployment capability
   - Reverse proxy deployment option
   - API-based connectivity for cloud services
   - Multi-mode deployment flexibility
   - Support for hybrid architecture
2. Integration Points
   - Identity and Access Management (IAM) Systems
   - Security Information and Event Management (SIEM)
   - Data Loss Prevention (DLP) Systems
   - Enterprise Mobility Management (EMM)
   - Security Orchestration and Response (SOAR)
   - Existing security infrastructure
3. Core Components
   - Cloud Security Gateway
   - Policy Engine
   - Data Protection Module
   - Threat Prevention System
   - Analytics Engine
   - Management Console

4. Technical Requirements

4.1 Architecture and Infrastructure

1. Deployment Flexibility
   - Cloud-based deployment support
   - On-premises deployment capability
   - Hybrid deployment options
   - Multi-tenant architecture
   - High availability configuration
2. Performance Specifications
   - Maximum latency: 50ms for inline operations
   - Minimum throughput: 10Gbps
   - Support for 100,000+ concurrent users
   - 99.99% uptime guarantee
   - Real-time policy enforcement
3. Security Architecture
   - End-to-end encryption (TLS 1.3)
   - Hardware Security Module (HSM) support
   - Secure key management
   - Certificate lifecycle management
   - Security hardening capabilities

5. Functional Requirements

5.1 User and Access Management

Tip: Robust user and access management is fundamental to cloud security. Ensure the solution provides comprehensive authentication methods, granular access controls, and detailed activity monitoring to maintain security while enabling productivity.

Requirement	Sub-Requirement	Y/N	Notes
User Authentication	Multi-factor authentication support		
	Integration with enterprise SSO solutions		
	Step-up authentication for sensitive operations		
	Session management and timeout controls		
	Device-based authentication options		
Access Control	Role-based access control (RBAC)		
	Attribute-based access control (ABAC)		
	Location-based access restrictions		
	Time-based access policies		
	Device posture checking		
User Activity Monitoring	Real-time activity logging		
	User session recording		
	File access tracking		
	Configuration change logging		
	Administrative activity audit		

5.2 Data Protection

Tip: Comprehensive data protection capabilities should cover the entire data lifecycle in cloud environments. Focus on solutions that provide deep visibility into data movement, robust controls, and flexible encryption options.

Requirement	Sub-Requirement	Y/N	Notes
Data Discovery	Automated sensitive data discovery		

	Custom data pattern recognition		
	Structured and unstructured data scanning		
	Database connection monitoring		
	Real-time data classification		
Data Loss Prevention	Content inspection rules		
	File type controls		
	Watermarking capabilities		
	Screenshot prevention		
	Copy/paste controls		
Encryption Management	Key management		
	Certificate lifecycle management		
	Encryption policy enforcement		
	Data tokenization		
	Format-preserving encryption		

5.3 Cloud Application Control

Tip: Cloud application control is crucial for maintaining security in cloud environments. Focus on capabilities that provide comprehensive visibility into cloud app usage, risk assessment, and granular control over access and data sharing.

Requirement	Sub-Requirement	Y/N	Notes
Application Discovery	Automated app discovery		
	Risk assessment scoring		
	Usage pattern analysis		

	Shadow IT detection		
	App categorization		
Application Management	Allowlist/blocklist management		
	Application access policies		
	API access control		
	Third-party app integration		
	Custom app onboarding		

5.4 Threat Protection

Tip: Modern threat protection requires multi-layered defense mechanisms that can detect and respond to both known and unknown threats. Evaluate solutions based on their ability to provide real-time protection, advanced analytics, and automated response capabilities.

Requirement	Sub-Requirement	Y/N	Notes
Threat Detection	Malware scanning		
	Ransomware protection		
	Anomaly detection		
	Advanced persistent threat (APT) protection		
	Zero-day threat detection		
Security Analytics	Behavioral analysis		
	Risk scoring		
	Threat intelligence integration		
	Pattern recognition		

	Predictive analytics		

5.5 Policy Management

Tip: Effective policy management is the foundation of CASB implementation. Look for solutions that offer flexible policy creation, granular controls, and automated enforcement capabilities.

Requirement	Sub-Requirement	Y/N	Notes
Policy Creation	Template-based policy creation		
	Custom policy builder		
	Policy inheritance		
	Version control		
	Policy testing environment		
Policy Enforcement	Real-time policy enforcement		
	Automated remediation actions		
	Policy violation alerts		
	Exception management		
	Granular policy controls		

5.6 AI and Machine Learning Capabilities

Tip: Advanced AI and ML capabilities should provide practical security benefits while maintaining transparency in decision-making. Focus on solutions that offer explainable AI and demonstrable security improvements.

Requirement	Sub-Requirement	Y/N	Notes
AI-Powered Threat Detection	Adaptive threat pattern recognition		
	Predictive threat analytics		

	Natural language processing for data classification		
	Zero-day attack pattern identification		
	Multi-vector attack correlation		
AI-Enhanced User Behavior Analytics	Dynamic user risk scoring		
	Intelligent session analysis		
	Entity relationship mapping		
	Behavioral baseline adaptation		
	Anomaly detection and correlation		
Autonomous Response and Remediation	Self-learning remediation		
	Smart policy automation		
	Automated response optimization		
	Context-aware policy adaptation		
	Risk-based policy optimization		
AI-Driven Cloud App Intelligence	Application behavior learning		
	Smart app risk assessment		
	Dynamic risk scoring		
	Data flow modeling		
	Integration risk assessment		
Intelligent Data Protection	Adaptive DLP		
	Smart encryption management		

	Content awareness evolution		
	False positive reduction		
	Automated policy suggestion		

5.7 Integration Capabilities

Tip: Integration capabilities determine how well the CASB solution will work with your existing security infrastructure. Prioritize solutions that offer robust APIs and pre-built integrations.

Requirement	Sub-Requirement	Y/N	Notes
Security Tool Integration	SIEM integration		
	DLP integration		
	IAM integration		
	EDR/XDR integration		
	SOAR integration		
API Capabilities	REST API availability		
	Custom integration support		
	Webhook support		
	Authentication methods		
	API documentation		

6. Non-Functional Requirements

6.1 Performance Requirements

1. System Performance

   - Maximum latency of 50ms for inline operations

   - Minimum throughput of 10 Gbps