Cloud Access Security Broker (CASB)

Request for Proposal Template

Table of Contents

Summary and Background

[Company] is currently accepting proposals for a Cloud Access Security Broker (CASB) solution to discover, monitor, secure, and control use of public cloud applications by members of our organization. This RFP process should enable us to conduct a fair and extensive evaluation of multiple vendor solutions based on the criteria enclosed to help us select best solution to meet and/or exceed requirements.

Project Goals

The CASB solution will help [Company] achieve the following goals:

- Visibility and Control over Shadow IT use of Cloud Apps
    1. Discover the cloud apps being used by on-premises and remote employees
    2. Evaluate, compare, and rank the risks presented by the cloud apps in use by our employees
    3. Establish which apps are sanctioned by the company for company use, which apps are permitted but not formally sanctioned, and which apps are prohibited
    4. Set controls to govern what cloud apps can be accessed by employees
- Visibility and Control over sensitive data in cloud services (SaaS, IaaS, email, file sharing, collaboration platforms, etc.)
    1. Automatically identify sensitive company data being shared, stored, and processed (including compliance-related data and sensitive intellectual property in unstructured, structured, and custom formats)
    2. Control access to sensitive data and inappropriate sharing of sensitive data
    3. Prevent theft, loss, and accidental exposure of sensitive data
    4. Apply the same DLP to data in cloud apps as is applied to data on enterprise endpoints, data centers, and networks
- Protection against threats associated with cloud apps without limiting employee use of sanctioned cloud apps
    1. Monitor, remediate and prevent high risk user activity
    2. Detect and prevent proliferation of malware and advanced threats
    3. Control access to cloud accounts and prevent unauthorized access to cloud properties
- Achieve regulatory compliance with the use of cloud apps
    1. Perform risk analysis of cloud apps in use
    2. Identify regulatory compliant and noncompliant cloud services in use and apply appropriate controls over use of these services
    3. Protect and govern regulated content in cloud apps and keep regulated content out of insecure or noncompliant apps
- Easy and effective deployment and ongoing management
    1. Monitor and control all required cloud services including SaaS and IaaS platforms
    2. Provide an intuitive and pleasant user experience
    3. Minimize deployment and administrative complexity
    4. Integrate CASB with extended enterprise security solutions (identity management, directory, DLP, networking, managed services, and endpoints)

Existing Infrastructure and Scope

Please provide information on the proxies, firewalls and SIEMs, DLP, SSO / SAML that have been deployed.

If Encryption, DLP, IAM or other systems are already in place, please specify.

Please include # of users, and estimated cloud applications looking to be monitored.

All infrastructure and users will be considered in scope of this RFP, unless specified here.

Schedule of Events

Task	***Date (9am ET)***
RFP distribution	**XX/XX/XX**
Deadline for vendors questions	**XX/XX/XX**
Answers to vendor questions	**XX/XX/XX**
Deadline for RFP submission	**XX/XX/XX**
Vendor notification of short-listed vendors	**XX/XX/XX**
Vendor presentations	**XX/XX/XX**
Vendor evaluations, POC etc.	**XX/XX/XX**
Vendor selection	**XX/XX/XX**

Vendor Stability

The CASB vendor must demonstrate a necessary level of responsibility, resourcing, and stability. The company requires a reliable solution partner that will be able to support and prioritize the company's requirements for a CASB now and for the foreseeable future.

Requirement	Description
Company legal name	
Company ownership and funding	
Name of CASB solution. Please include all products or add-ons whose functionality is included in the responses below.	
Please list any vendor alliances required for the delivery of your CASB solution.	
How many employees are dedicated to the delivery of the CASB solution?	
Is your CASB solution available globally? Describe any exceptions if not yes.	
How many customers do you have?	
Describe your POC capability and experience	

Platform & Internal Resources

Requirement	Description
How long has the CASB been in market (should be a minimum of 3 years)?	
Do you have a dedicated research team that is global in scope? How large is this team?	
Is the cloud application research team augmented by machine learning and automation? Describe.	
Does your CASB development follow any product lifecycle and information lifecycle methodology?	

CASB Support

Requirement	Description
How big is your support organization?	
Do you have 24x7 support? Globally?	
Please indicate all global locations where you have personnel dedicated to supporting CASB solutions.	
Is support included with the CASB?	
What is the SLA for support?	
Describe the post-sales support and education experience.	

Platform Regulatory Compliance & Data Privacy

Requirement	Description
Is CASB solution SOC-2 Type II compliant? What other vendor regulatory compliance certifications do you possess?	
Does CASB solution comply with accessibility standards?	
Which of the five “trust services” of the SSAE 16 SOC 2 are you audited on? (Security, Availability, Processing Integrity, Confidentiality, Privacy.)	

Please provide a schedule of on-going independent 3rd party assessments of infrastructure, application, data, and services.	
Does the solution provide support to inform a Data Privacy Officer (4-eyes principle)?	

Platform Infrastructure & Operations

Requirement	Description
Does the solution provider own and manage their own data centers, or do they partner with leading cloud providers (AWS, Azure)? Describe.	
Is there an uptime SLA? Describe.	
Is the solution multi-tenant? Describe how data for different customers is protected on these topics: How are customer deployments segregated in the CloudSOC platform? Does the solution provide documentation on the segregation of infrastructure from other customers or other environments?	
Is data replicated as part of backup/data corruption protection, then what method is used, e.g. SRDF? In the event of data corruption, what is the recovery point objective?	
Does the solution provide high-availability and fault-tolerance that can recover from events within a datacenter? Please describe.	
Does the solution provide a fail-over or disaster recovery in the event of a disaster, such as an alternate recovery site, co-location, datacenter, etc.?	
What access does the company have to the client data setup and data? How is this access managed within the company?	
What security solutions are employed for the CASB platform and infrastructure? (e.g. Anti-Virus, Perimeter Firewalls, Web Application Firewalls, Intrusion Detection/Prevention Systems, mobile coverage, etc.)	
What type and level of encryption does the solution platform support?	

Does the solution have the ability to horizontally or vertically scale (linearly or better) to increase throughput, i.e., by increasing the number of processing nodes, CPU Cores, RAM, I/O, etc.? If so, at what point does the ability to scale linearly stop? Please explain for both cloud infrastructure and any SW/HW (if applicable) components.	
Can you provide copies of your last SOC-2 and ISO 27001 certificates?	
Does the solution provide Role Based Access Control (RBAC) to give limited access to admins for selected data in selective applications?	

Shadow IT Use of Cloud Apps

Visibility

Requirement	Yes/No	Description
Does the CASB solution provide information on what cloud apps are used, who is using them, and provide a detailed risk analysis of each app? Describe.		
Does the CASB support at least all of the following sources of log data out of the box? Palo Alto Networks devices, Cisco WSA, Cisco CWS, Symantec ProxySG, McAfee Web Gateway, Barracuda NG Firewall, Juniper SRX and ScreenOS, Sonicwall, Checkpoint, Sophos UTM, Squid, Websense Proxy, Fortinet, Cisco CWS and WSA and ASA Series, Zscaler NSS?		
Does the CASB support data sources via both direct and indirect uploads using HTTPS, SCP, SFTP, S3, and CWS S3?		
Can CASB automate data source collection, and anonymize and tokenize log data?		
Does CASB integrate with endpoint management solutions like MDM? Can you discover or audit your mobile apps in use? Can your solution steer mobile traffic to your secured gateway?		

Can your CASB support multiple security log sources? Describe all other log data sources supported by the CASB?		
How many cloud apps does the CASB support with Shadow IT discovery?		
What risk factors and details are provided on cloud apps and services? How many metrics are used to characterize each cloud app?		
Do you have an automated and manual research methodology that operates on at minimum a bi-weekly update cadence?		
How often do you re-evaluate existing apps in your research database? Do you provide a date last updated stamp for researched cloud apps?		
Does CASB simplify the work of analyzing shadow IT risk and compliance analysis? How?		
Does CASB cover mobile apps for discovery and scoring as part of the shadow IT discovery and analysis?		
Does the CASB console dashboard provide a summary of any cloud apps compromised in the last 90 days? Do those incidents influence the app rating dynamically?		
Does the CASB console display the geographic location of users and cloud app data centers in map form based on live traffic analysis?		
Does the solution provide Cloud App Usage Summary and Analytics?		
Is Cloud Service Usage Reporting viewable by Group, Function, Region, Country, and Location?		
Can the solution identify duplicated app usages?		
Can you prioritize the significance of granular risk factors in cloud app ratings to meet specific requirements customized to the individual organization's security priorities?		

Does the app analysis include their exposure to vulnerabilities, such as Cloudbleed, Heartbleed, etc.?		
Can CASB provide direct side-by-side comparisons of multiple apps with risk attribute ratings? Does the solution have the option to compare an applications risk to others in industry by application category?		
Does the solution identify high-risk user behavior and threats based on source logs from firewalls, proxies, endpoint protection solutions? Can it detect granular anomalies? Detail detectable behavior, such as excessive downloads, excessive sharing with people outside of the company, access from two locations at the same time, etc.		

Control of Data

Requirement	Yes/No	Description
Does the solution provide policy-based controls over Shadow IT use of cloud apps and services? Can you automate policy enforcement based on risk factors and risk ratings as well as just by application list? What parameters can be used to craft filters/ restrictions? What control actions are available?		
Can risky cloud apps be blocked through integrations with secure web gateways or firewalls?		
Does the CASB rely on scripts via flat file to integrate with policy controls on secure web gateways such as Symantec's ProxySG or Web Security Service?		
Can access and granular actions associated with sensitive data be controlled based on user, device, location, and other attributes? What actions can be controlled? What attributes can be defined?		

Data, Apps, Activities, Transactions Coverage

Requirement	Yes/No	Description
Does the solution provide visibility over any cloud service in use -- sanctioned and unsanctioned, personal accounts and corporate accounts?		
Does the CASB provide visibility and control over user actions for over 300 different applications including Box, Dropbox, Office 365, Salesforce, DocuSign, GitHub, Google G Suite, Jive, ServiceNow, SuccessFactors, Adobe, iCloud, Slack?		
Does the solution provide visibility and control over IaaS deployments in AWS and Azure via both API and in-line?		
Does the CASB provide granular visibility and control over user actions and data in Office 365 in OneDrive, Email, Sharepoint, Teams, Groups, Yammer, OneDrive Personal, and Dynamics apps?		
Does the CASB provide visibility and control over user actions and data in Google G Suite in Drive, Gmail, Sites, Calendar, Team Drive, Forms, Groups, Meet, Vault, Admin, and Hangouts apps?		
Can the product correlate user actions and data analysis across multiple cloud services to identify high risk incidents and behavior? Does it use visualizations, normalized risk measurements, and natural language to make analysis easy? What data sources does it use to compile this overview?		
Does the CASB provide advanced tools with visualizations for easy investigation of malicious or high-risk activity?		
Does the CASB correlate user between all CASB data source components (Shadow IT cloud use visibility via log data, behavioral		

data via inline traffic analysis, and API-based user action in apps)?		
Does the solution show the Data Usage per user/session?		

Data Security

Data Governance & DLP

Requirement	Yes/No	Description
Does your CASB contain DLP? How does the feature set compare to a leading industry DLP solution? List the capabilities.		
Can the solution watermark, redact, or encrypt content that is triggered or determined to be anomalous?		
Does solution automatically classify types of sensitive content out-of-the-box? If so, list your automatic classification categories.		
Does CASB include built-in, native automatic data classification? What techniques are used to classify data (regex matching, dictionaries, machine learning, NLP)?		
Does the solution have built-in capabilities to enforce different responses to data governance violations – (e.g. block, log, quarantine, unshare, alert, permit but alert, coach, encrypt, etc.)		
Does the CASB built-in DLP functionality identify potential data exfiltration?		
Does the solution display quantified risk levels for risky transactions and risky users?		
Does solution integrate with enterprise DLP solutions in the cloud (NOT ICAP)? Does it preserve and leverage existing enterprise DLP policies and workflows?		

Encryption

Requirement	Yes/No	Description
Does the solution support tokenization and encryption		

options to protect data while in transit and at rest in the cloud? Describe.		
If encryption is used, where are the keys stored and how are they managed? Does the solution allow the customer (not the vendor) to own and maintain control over encryption keys?		
Can the solution support file-level encryption?		
Can the solution automatically encrypt and/or tokenize compliance-related content in cloud apps?		

Threat Protection

User Behavior Analytics

Requirement	Yes/No	Description
Does the solution identify high-risk user behavior and threats? Can it detect granular anomalies? Detail detectable behavior, such as excessive downloads, excessive sharing with people outside of the company, access from two locations at the same time, etc.		
Can the solution detect and prevent data exfiltration from sanctioned apps/services to unsanctioned services?		
Can the solution take action on the size of data (file sharing) in an attempted transfer, ingress/egress?		
Can the solution describe the changes made to data, the use of that data and access to that data?		
Can the solution quarantine a document, user and/or device?		

Advanced Anti-Malware

Requirement	Yes/No	Description
Does the solution inspect email content? What email content is inspected? What is stored within the CASB database?		
Does CASB integrate with Endpoint Protection solutions for		

identifying off-prem Shadow IT? Describe.		
Can CASB discover incoming malicious VB Macros, viruses, and worms? Describe.		

Meeting Internal Regulatory Compliance

Requirement	Yes/No	Description
Does solution provide a Cloud Confidence Index/Reputation Rating, Risk Rating Based on Industry Alliances, etc? Rating must be customizable based on customer requirements.		
Can the system identify the geographic location of data in cloud apps? How does it do this?		
Does the solution enforce GDPR, HIPAA, and other compliance standards out of the box?		

Management UX and Administration

Requirement	Yes/No	Description
How intuitive is the user interface? Is the user interface Human Factors friendly - easy to create, customize, access and navigate dashboards to understand cloud usage and potential risks?		
Does the solution offer role-based access controls (RBAC)? Can RBAC be applied to custom dashboards? Can it be applied down to the individual cloud app level?		
Does the solution offer custom reporting options? Can they be saved? Can they be rendered as infographics?		
Can you use simple Boolean logic (AND, OR, NOT) to create DLP policies?		
Can an administrator add groups in bulk by a list? Describe.		

Integration with Extended Enterprise Security & Investigations

Requirement	Yes/No	Description
Can multi-app and/or low and slow data exfiltration activity be identified and controlled? How?		
Can CASB integrate with SIEM solutions like ArcSight and Splunk? Describe how.		

Pricing & Licensing

Describe the pricing and licensing options here.

Terms and Conditions

Please provide the links to any terms and conditions documents, as well as service descriptions, support, and education.