Demande de proposition : Solution logicielle CASB (Cloud Access Security Broker)

Table des matières

1. Introduction et contexte

Notre organisation recherche des propositions pour une solution complète de Cloud Access Security Broker (CASB) afin d'améliorer notre posture de sécurité en nuage et d'assurer la protection de nos ressources basées en nuage. La solution CASB sélectionnée servira de point de contrôle de sécurité critique entre nos consommateurs de services en nuage et nos fournisseurs de services en nuage.

1.1 Contexte du marché

- Le marché des CASB croît à un taux de croissance annuel moyen (CAGR) d'environ 17,6 % (2021-2026).
- Les coûts de mise en œuvre vont généralement de 15 000 à plus de 100 000 dollars par an.
- La solution doit s'aligner sur les capacités des leaders actuels du marché tout en offrant des caractéristiques innovantes.

1.2 Attentes en matière de valeur commerciale

- Amélioration de la sécurité de l'informatique dématérialisée grâce à un contrôle unifié
- Meilleure visibilité de l'utilisation des services en nuage
- Renforcement des capacités en matière de conformité réglementaire
- Atténuation significative des risques pour les opérations en nuage
- Optimisation des coûts grâce à une utilisation contrôlée de l'informatique en nuage

2. Objectifs du projet

2.1 Objectifs principaux

1. Déployer une solution CASB complète qui offre une visibilité et un contrôle sur les services en nuage.
2. Mettre en œuvre des mesures robustes de protection des données pour les informations hébergées dans le nuage
3. Mettre en place des capacités de surveillance et de détection des menaces en temps réel
4. Permettre une gestion granulaire des politiques dans les services en nuage
5. Veiller au respect des exigences réglementaires
6. Optimiser l'utilisation des services en nuage et les coûts associés

2.2 Objectifs stratégiques

1. Réduire de 75 % les incidents de sécurité liés à l'utilisation des services en nuage

2. Obtenir une visibilité totale sur l'utilisation des applications en nuage
3. Mise en place d'une application automatisée des politiques dans tous les services en nuage
4. Mettre en œuvre des mesures cohérentes de protection des données sur l'ensemble des plates-formes d'informatique dématérialisée
5. Permettre une détection et une réponse proactives aux menaces
6. Rationaliser les opérations de sécurité grâce à l'automatisation

3. Champ d'application des travaux

3.1 Exigences en matière d'architecture technique

1. Modèles de déploiement
    - Capacité de déploiement d'un proxy avancé
    - Option de déploiement d'un proxy inverse
    - Connectivité basée sur l'API pour les services en nuage
    - Flexibilité du déploiement multimode
    - Prise en charge de l'architecture hybride
2. Points d'intégration
    - Systèmes de gestion des identités et des accès (IAM)
    - Gestion des informations et des événements de sécurité (SIEM)
    - Systèmes de prévention des pertes de données (DLP)
    - Gestion de la mobilité d'entreprise (EMM)
    - Orchestration et réponse en matière de sécurité (SOAR)
    - Infrastructure de sécurité existante
3. Composants essentiels
    - Passerelle de sécurité pour l'informatique en nuage

- Moteur politique
- Module de protection des données
- Système de prévention des menaces
- Moteur d'analyse
- Console de gestion

4. Exigences techniques

4.1 Architecture et infrastructure

1. Flexibilité du déploiement
    - Soutien au déploiement basé sur l'informatique en nuage
    - Capacité de déploiement sur site
    - Options de déploiement hybride
    - Architecture multi-locataires
    - Configuration de la haute disponibilité
2. Spécifications de performance
    - Latence maximale : 50 ms pour les opérations en ligne
    - Débit minimum : 10Gbps
    - Prise en charge de plus de 100 000 utilisateurs simultanés
    - Garantie de temps de fonctionnement de 99,99
    - Application de la politique en temps réel
3. Architecture de sécurité
    - Cryptage de bout en bout (TLS 1.3)
    - Prise en charge du module de sécurité matériel (HSM)
    - Gestion sécurisée des clés
    - Gestion du cycle de vie des certificats

- Capacités de renforcement de la sécurité

5. Exigences fonctionnelles

5.1 Gestion des utilisateurs et des accès

Conseil : Une gestion robuste des utilisateurs et des accès est fondamentale pour la sécurité du cloud. Assurez-vous que la solution propose des méthodes d'authentification complètes, des contrôles d'accès granulaires et un suivi détaillé des activités afin de maintenir la sécurité tout en favorisant la productivité.

Exigence	Sous-exigence	O/N	Notes
Authentification de l'utilisateur	Prise en charge de l'authentification multifactorielle		
	Intégration avec les solutions SSO de l'entreprise		
	Authentification renforcée pour les opérations sensibles		
	Gestion des sessions et contrôle des délais		
	Options d'authentification basées sur l'appareil		
Contrôle d'accès	Contrôle d'accès basé sur les rôles (RBAC)		
	Contrôle d'accès basé sur les attributs (ABAC)		
	Restrictions d'accès basées sur la localisation		
	Politiques d'accès basées sur le temps		
	Vérification de l'état des appareils		

Contrôle de l'activité des utilisateurs	Enregistrement des activités en temps réel		
	Enregistrement de la session de l'utilisateur		
	Suivi de l'accès aux fichiers		
	Enregistrement des changements de configuration		
	Audit des activités administratives		

5.2 Protection des données

Conseil : Des capacités complètes de protection des données doivent couvrir l'ensemble du cycle de vie des données dans les environnements en nuage. Privilégiez les solutions qui offrent une visibilité approfondie des mouvements de données, des contrôles robustes et des options de chiffrement flexibles.

Exigence	Sous-exigence	O/N	Notes
Découverte de données	Recherche automatisée de données sensibles		
	Reconnaissance de modèles de données personnalisés		
	Analyse des données structurées et non structurées		
	Surveillance de la connexion à la base de données		
	Classification des données en temps réel		
Prévention de la perte de données	Règles d'inspection du contenu		
	Contrôle des types de fichiers		
	Capacités de filigrane		

	Prévention des captures d'écran		
	Contrôles copier/coller		
Gestion du chiffrement	Gestion des clés		
	Gestion du cycle de vie des certificats		
	Application de la politique de chiffrement		
	La tokenisation des données		
	Cryptage préservant le format		

5.3 Contrôle des applications en nuage

Conseil : Le contrôle des applications en nuage est essentiel pour maintenir la sécurité dans les environnements en nuage. Concentrez-vous sur les capacités qui offrent une visibilité complète de l'utilisation des applications en nuage, une évaluation des risques et un contrôle granulaire de l'accès et du partage des données.

Exigence	Sous-exigence	O/N	Notes
Découverte de l'application	Découverte automatisée d'applications		
	Cotation de l'évaluation des risques		
	Analyse des schémas d'utilisation		
	Détection de l'informatique fantôme		
	Catégorisation des applications		
Gestion des applications	Gestion des listes d'autorisation/de blocage		
	Politiques d'accès aux applications		
	Contrôle d'accès à l'API		

	Intégration d'applications tierces		
	Onboarding d'applications personnalisées		

5.4 Protection contre les menaces

Conseil : la protection moderne contre les menaces nécessite des mécanismes de défense multicouches capables de détecter les menaces connues et inconnues et d'y répondre. Évaluez les solutions en fonction de leur capacité à fournir une protection en temps réel, des analyses avancées et des capacités de réponse automatisées.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces	Analyse des logiciels malveillants		
	Protection contre les rançongiciels		
	Détection des anomalies		
	Protection contre les menaces persistantes avancées (APT)		
	Détection des menaces de type "jour zéro		
Analyse de la sécurité	Analyse comportementale		
	Evaluation des risques		
	Intégration des renseignements sur les menaces		
	Reconnaissance des formes		
	Analyse prédictive		

5.5 Gestion des politiques

Conseil : une gestion efficace des règles est la base de la mise en œuvre d'un CASB. Recherchez des solutions qui offrent une création flexible des règles, des contrôles granulaires et des capacités d'application automatisées.

Exigence	Sous-exigence	O/N	Notes
Création d'une politique	Création de politiques à partir de modèles		
	Constructeur de polices d'assurance personnalisées		
	Héritage de la politique		
	Contrôle des versions		
	Environnement de test des politiques		
Application de la politique	Application de la politique en temps réel		
	Actions de remédiation automatisées		
	Alertes en cas de violation de la politique		
	Gestion des exceptions		
	Contrôles granulaires des politiques		

5.6 Capacités d'IA et d'apprentissage automatique

Conseil : Les capacités avancées d'IA et de ML doivent offrir des avantages pratiques en matière de sécurité tout en maintenant la transparence dans la prise de décision. Concentrez-vous sur les solutions qui offrent une IA explicable et des améliorations de sécurité démontrables.

Exigence	Sous-exigence	O/N	Notes
Détection des menaces par l'IA	Reconnaissance adaptative des menaces		
	Analyse prédictive des menaces		

	Traitement du langage naturel pour la classification des données		
	Identification de modèles d'attaques de type "zero-day		
	Corrélation des attaques multi-vectorielles		
Analyse du comportement des utilisateurs grâce à l'IA	Évaluation dynamique des risques pour l'utilisateur		
	Analyse intelligente des sessions		
	Cartographie des relations entre les entités		
	Adaptation comportementale de base		
	Détection des anomalies et corrélation		
Réponse autonome et remédiation	Remédiation par auto-apprentissage		
	Automatisation intelligente des politiques		
	Optimisation automatisée des réponses		
	Adaptation des politiques en fonction du contexte		
	Optimisation des politiques en fonction des risques		
Intelligence des applications en nuage pilotée par l'IA	Application de l'apprentissage du comportement		
	Évaluation des risques liés aux applications intelligentes		

	Evaluation dynamique des risques		
	Modélisation du flux de données		
	Évaluation du risque d'intégration		
Protection intelligente des données	DLP adaptatif		
	Gestion intelligente du chiffrement		
	Évolution de la connaissance du contenu		
	Réduction des faux positifs		
	Suggestion automatisée de politiques		

5.7 Capacités d'intégration

Conseil : les capacités d'intégration déterminent dans quelle mesure la solution CASB fonctionnera avec votre infrastructure de sécurité existante. Donnez la priorité aux solutions qui offrent des API robustes et des intégrations prédéfinies.

Exigence	Sous-exigence	O/N	Notes
Intégration des outils de sécurité	Intégration SIEM		
	Intégration DLP		
	Intégration IAM		
	Intégration EDR/XDR		
	Intégration SOAR		
Capacités de l'API	Disponibilité de l'API REST		
	Soutien à l'intégration personnalisée		

	Prise en charge des webhooks		
	Méthodes d'authentification		
	Documentation de l'API		

6. Exigences non fonctionnelles

6.1 Exigences de performance

1. Performance du système
    - Latence maximale de 50 ms pour les opérations en ligne
    - Débit minimum de 10 Gbps
    - Prise en charge de plus de 100 000 utilisateurs simultanés
    - Application de la politique en temps réel
    - Garantie de temps de fonctionnement de 99,99
2. Évolutivité
    - Capacité de mise à l'échelle horizontale
    - Équilibrage automatique de la charge
    - Allocation dynamique des ressources
    - Prise en charge multirégionale
    - Gestion de la capacité élastique
3. Disponibilité
    - Architecture à haute disponibilité
    - Basculement automatisé
    - Capacités de reprise après sinistre
    - Redondance géographique
    - Pas de point de défaillance unique

6.2 Exigences en matière de sécurité

1. Sécurité des données
    - Cryptage AES-256 pour les données au repos
    - TLS 1.3 pour les données en transit
    - Conformité FIPS 140-2
    - Gestion sécurisée des clés
    - Conformité à la souveraineté des données
2. Sécurité d'accès
    - Contrôle d'accès basé sur les rôles
    - Authentification multifactorielle
    - Gestion des accès privilégiés
    - Gestion des sessions
    - Enregistrement des audits d'accès
3. Conformité
    - Certification SOC 2 Type II
    - Certification ISO 27001
    - Conformité au GDPR
    - Conformité HIPAA
    - Conformité à la norme PCI DSS

7. Exigences de mise en œuvre

7.1 Phases du projet

1. Phase de planification (4-6 semaines)
    - Recueil des besoins
    - Conception de l'architecture

- Planification de l'intégration
- Allocation des ressources
- Développement du calendrier

2. Phase de déploiement (8-12 semaines)
    - Configuration initiale
    - Configuration de base
    - Mise en œuvre de l'intégration
    - Développement de la politique
    - Essais et validation
3. Phase d'optimisation (4-6 semaines)
    - Optimisation des performances
    - Affinement de la politique
    - Tests d'acceptation par l'utilisateur
    - Achèvement de la documentation
    - Transfert de connaissances

7.2 Services de mise en œuvre

1. Services professionnels
    - Consultation en matière d'architecture
    - Aide au déploiement
    - Soutien à l'intégration
    - Développement de la politique
    - Optimisation des performances
2. Services de formation
    - Formation des administrateurs

- Formation des équipes de sécurité
- Formation des utilisateurs finaux
- Documentation personnalisée
- Accès à la base de connaissances

8. Exigences opérationnelles

8.1 Services d'appui

1. Support technique
    - Assistance disponible 24 heures sur 24, 7 jours sur 7
    - Réponse en 1 heure maximum pour les questions critiques
    - Options de soutien multicanal
    - Équipe d'assistance dédiée
    - Examens réguliers des services
2. Maintenance
    - Mises à jour et correctifs réguliers
    - Fenêtres de maintenance programmée
    - Processus de gestion du changement
    - Contrôle des versions
    - Capacités de retour en arrière
3. Contrôle
    - Surveillance du système en temps réel
    - Suivi des indicateurs de performance
    - Planification des capacités
    - Analyse des tendances
    - Détection proactive des problèmes

9. Qualifications des fournisseurs

9.1 Profil de l'entreprise

1. Position sur le marché
    - Au moins 5 ans sur le marché CASB
    - Leader reconnu de l'industrie
    - Forte stabilité financière
    - Une présence mondiale
    - Expérience confirmée
2. Base de clients
    - Références d'entreprises clientes
    - Expérience spécifique à l'industrie
    - Mise en œuvre à l'échelle similaire
    - Mesures de la satisfaction des clients
    - Études de cas

9.2 Expertise technique

1. Développement de produits
    - Une équipe de R&D dédiée
    - Cycle de publication régulier
    - Expérience en matière d'innovation
    - Partenariats technologiques
    - Feuille de route du produit
2. Capacités de soutien
    - Présence d'un support mondial
    - Expertise technique

- Expérience de la mise en œuvre
- Capacités de formation
- Disponibilité des ressources

10. Critères d'évaluation

10.1 Évaluation technique (40%)

1. Complétude des caractéristiques
    - Couverture des fonctionnalités de base
    - Disponibilité des fonctionnalités avancées
    - Capacités d'intégration
    - Options d'évolutivité
    - Mesures de performance
2. Architecture
    - Principes de conception
    - Évolutivité
    - Fiabilité
    - Sécurité
    - L'innovation

10.2 Évaluation des fournisseurs (30 %)

1. Stabilité de l'entreprise
    - Santé financière
    - Position sur le marché
    - Trajectoire de croissance
    - Base de clientèle
    - Reconnaissance du secteur

2. Capacités de soutien
    - Une présence mondiale
    - Expertise technique
    - Temps de réponse
    - Disponibilité des ressources
    - Programmes de formation

10.3 Évaluation des coûts (30 %)

1. Coût total de possession
    - Frais de licence
    - Coûts de mise en œuvre
    - Coûts de maintenance
    - Coûts de soutien
    - Coûts de formation

11. Lignes directrices en matière de soumission

11.1 Exigences de la proposition

1. Proposition technique
    - Aperçu de la solution
    - Spécifications techniques
    - Approche de la mise en œuvre
    - Modèle de soutien
    - Exemples de produits à fournir
2. Proposition commerciale
    - Structure des prix
    - Conditions de paiement

- Accords de niveau de service
- Services complémentaires
- Caractéristiques optionnelles

11.2 Format de soumission

- Soumission électronique requise
- Format PDF
- Maximum 100 pages
- Résumé requis
- Documentation d'appui en annexe

12. Calendrier

- Date de publication de l'appel d'offres : [Date]
- Date limite pour les questions : [Date]
- Date d'échéance de la proposition : [Date]
- Présentations des fournisseurs : [Fourchette de dates]
- Date de sélection : [Date]
- Date de début du projet : [Date]

13. Coût total de possession

13.1 Coûts directs

1. Licences de logiciels
    - Frais de licence par utilisateur
    - Coûts liés aux modules
    - Coûts des fonctions supplémentaires
    - Remises sur volume
    - Engagements à terme

2. Coûts de mise en œuvre
    - Services professionnels
    - Services d'intégration
    - Coûts de personnalisation
    - Frais de formation
    - Gestion de projet

13.2 Coûts indirects

1. Coûts opérationnels
    - Allocation des ressources internes
    - Exigences en matière d'infrastructure
    - Maintenance continue
    - Mises à jour régulières
    - Soutenir les renouvellements
2. Autres considérations
    - Impact sur les performances
    - Effets de productivité
    - Exigences en matière de formation
    - Changements de processus
    - Maintenance de l'intégration

14. Considérations pour l'avenir

14.1 Tendances technologiques

1. Technologies émergentes
    - Intégration de la confiance zéro
    - Convergence SASE

- Soutien à l'informatique de pointe
- Préparation à l'informatique quantique
- Capacités de sécurité 5G

2. Évolution du marché
    - Consolidation des fournisseurs
    - Normalisation des caractéristiques
    - Modifications du modèle de tarification
    - Normes d'intégration
    - Exigences réglementaires

14.2 Mesures de réussite

1. Mesures de sécurité
    - Taux de détection des menaces
    - Temps de résolution des violations de la politique
    - Découverte de l'informatique fantôme
    - Efficacité de la protection des données
    - Efficacité du contrôle d'accès
2. Mesures opérationnelles
    - Temps de fonctionnement du système
    - Temps de réponse
    - Délai de résolution des problèmes
    - Satisfaction des utilisateurs
    - Économies de coûts

15. Informations sur les contacts

Veuillez soumettre vos propositions et vos questions à [Nom du contact] [Adresse électronique] [Numéro de téléphone]