Demande de proposition : Solution logicielle de sécurité des fichiers en nuage

Table des matières

1. Introduction et contexte
2. Objectifs du projet
3. Exigences techniques
4. Exigences fonctionnelles
5. Qualifications des fournisseurs
6. Critères d'évaluation
7. Exigences en matière de soumission
8. Calendrier et procédure
9. Informations sur le contact

1. Introduction et contexte

Le présent appel d'offres sollicite des propositions pour une solution logicielle complète de sécurité des fichiers en nuage afin de protéger les fichiers et les données sensibles stockés dans des environnements en nuage. La solution doit mettre en œuvre des mesures de sécurité robustes pour garantir la confidentialité des données et la conformité avec les réglementations sectorielles.

Exigences de base

- Cryptage avancé pour la protection des données
- Contrôle d'accès et authentification des utilisateurs
- Prévention des pertes de données
- Capacités d'audit et d'établissement de rapports

- Intégration avec les services de stockage en nuage et les outils de productivité existants

2. Objectifs du projet

Objectifs principaux

1. Mettre en œuvre une protection complète des données par le biais d'un système de protection des données :
    - Cryptage fort (AES-256) pour les données au repos et en transit
    - Cryptage de bout en bout tout au long du cycle de vie des données
    - Gestion des clés de chiffrement alimentée par l'IA
2. Renforcer la sécurité grâce à l'authentification avancée :
    - Authentification multifactorielle
    - Contrôles d'accès basés sur les rôles
    - Intégration de l'authentification unique (SSO)
    - Analyse comportementale pilotée par l'IA
3. Mettre en place une solide prévention des pertes de données :
    - Contrôler et empêcher le partage non autorisé
    - Inspection et filtrage du contenu
    - Alertes en temps réel en cas de fuite de données
    - Reconnaissance de modèles d'IA pour les tentatives d'exfiltration de données

3. Exigences techniques

Contrôles de sécurité

1. Contrôle des appareils
    - Contrôle granulaire sur différents types d'appareils
    - Gestion de l'utilisation des appareils basée sur des règles

- Détection et classification automatisées des appareils
- Intégration avec les systèmes de gestion de l'identité
- Capacités de gestion à distance des appareils
- Application du chiffrement des appareils

2. Contrôle du Web
    - Filtrage des URL à l'aide de catégories prédéfinies
    - Capacités d'inspection HTTPS
    - Contrôles d'accès basés sur la durée
    - Analyse en temps réel des logiciels malveillants
    - Surveillance et contrôle de la bande passante
    - Règles de filtrage personnalisées
3. Gestion des actifs
    - Recherche automatisée d'actifs
    - Surveillance de l'état en temps réel
    - Gestion du cycle de vie
    - Intégration avec les outils ITSM
    - Rapports sur l'inventaire des actifs
    - Suivi de la conformité
4. Isolation du système
    - Contrôle de la connexion au réseau
    - Capacités de désactivation des applications
    - Des canaux de communication sécurisés
    - Enregistrement des événements d'isolation

- Procédures de récupération
- Intégration de la réponse aux incidents

4. Exigences fonctionnelles

1. Chiffrement et sécurité des données

Conseil : Le cryptage des données constitue la base de la sécurité des fichiers dans le nuage. Concentrez-vous sur l'évaluation de la puissance des algorithmes de cryptage et de la facilité de gestion des clés.

Exigence	Sous-exigence	O/N	Notes
Mise en œuvre du chiffrement	Cryptage AES-256 pour les données au repos		
	Cryptage AES-256 pour les données en transit		
	Prise en charge du cryptage de bout en bout		
Gestion des clés	Gestion des clés de chiffrement alimentée par l'IA		
	Capacités de rotation des clés		
	Stockage sécurisé des clés		

2. Authentification et autorisation de l'utilisateur

Conseil : Les mécanismes d'authentification et d'autorisation doivent concilier sécurité et expérience utilisateur.

Exigence	Sous-exigence	O/N	Notes
Méthodes d'authentification	Prise en charge de l'authentification multifactorielle		
	Options d'authentification biométrique		
	Capacités d'intégration SSO		

Contrôles d'autorisation	Gestion de l'accès basée sur les rôles		
	Analyse comportementale pilotée par l'IA		
	Contrôle continu de l'authentification		

3. Gestion du contrôle d'accès

Conseil : le contrôle d'accès granulaire est essentiel pour maintenir la sécurité tout en permettant la collaboration.

Exigence	Sous-exigence	O/N	Notes
Permissions de fichiers	Contrôle des autorisations d'affichage		
	Contrôle des autorisations d'édition		
	Contrôle des autorisations de téléchargement		
	Contrôle des autorisations de partage		
Contrôles administratifs	Gestion des rôles des utilisateurs		
	Gestion des droits d'accès		
Contrôles temporels	Restrictions d'accès programmées		
	Octroi d'un accès temporaire		
Caractéristiques de l'IA	Ajustement dynamique de l'accès		
	Modification des contrôles en fonction des risques		

4. Prévention de la perte de données (DLP)

Conseil : Les fonctionnalités de DLP doivent protéger contre les fuites de données accidentelles et intentionnelles.

Exigence	Sous-exigence	O/N	Notes
Contrôle	Détection de partage non autorisé		
	Capacités d'inspection du contenu		
	Contrôle en temps réel		
Alertes	Notifications de fuites de données		
	Alertes en cas de violation de la politique		
	Configuration personnalisée des alertes		
Capacités en matière d'IA	Reconnaissance des formes		
	Détection des tentatives d'exfiltration		
	Analyse comportementale		

5. Surveillance en temps réel et détection des menaces

Conseil : une détection efficace des menaces nécessite à la fois une surveillance en temps réel et une analyse intelligente.

Exigence	Sous-exigence	O/N	Notes
Suivi des activités	Suivi de l'accès aux fichiers		
	Suivi du comportement de l'utilisateur		
	Enregistrement des événements du système		
Détection des menaces	Analyse alimentée par l'IA		
	Reconnaissance des formes		
	Détection des anomalies		
Alertes	Notifications en temps réel		
	Seuils d'alerte personnalisables		

	Priorité aux alertes		

6. Audit et rapports

Conseil : Des fonctions complètes d'audit et de reporting sont essentielles pour la gestion de la conformité et de la sécurité.

Exigence	Sous-exigence	O/N	Notes
Enregistrement des activités	Enregistrement des accès aux fichiers		
	Suivi des actions de l'utilisateur		
	Enregistrement des événements du système		
Génération de rapports	Modèles de rapports personnalisables		
	Automatisation des rapports de conformité		
	Rapports de contrôle de la sécurité		
Caractéristiques de l'audit	Pistes d'audit complètes		
	Reconstruction de la chronologie des événements		
	Analyse de l'activité des utilisateurs		
Analyse de l'IA	Automatisation de l'analyse des journaux		
	Capacités de chasse aux menaces		
	Outils d'investigation médico-légale		

7. Gestion de la conformité

Conseil : La gestion de la conformité doit être proactive et s'adapter à l'évolution des réglementations.

Exigence	Sous-exigence	O/N	Notes
Application de la politique	Contrôles de conformité au GDPR		
	Contrôles de conformité HIPAA		
	Réglementations spécifiques à l'industrie		
Modèles	Modèles de conformité préétablis		
	Jeux de contrôle personnalisables		
	Modèles de politiques		
Automatisation	Rapports de conformité automatisés		
	Génération de documents		
	Tests de contrôle		
Adaptation de l'IA	Suivi des modifications réglementaires		
	Mises à jour des contrôles		
	Évaluation du risque de non-conformité		

8. Partage sécurisé de fichiers

Conseil : le partage sécurisé de fichiers doit concilier sécurité et facilité d'utilisation.

Exigence	Sous-exigence	O/N	Notes
Partage interne	Partage au niveau du département		
	Outils de collaboration en équipe		
	Intégration du contrôle d'accès		
Partage externe	Sécuriser les liens externes		
	Paramètres de la date d'expiration		

	Limites d'accès		
Contrôles de sécurité	Protection par mot de passe		
	Chiffrement des fichiers partagés		
	Télécharger les restrictions		
Caractéristiques de l'IA	Évaluation des risques		
	Analyse du modèle de partage		
	Détection des menaces		

9. Contrôle et récupération des versions

Conseil : De solides capacités de contrôle des versions et de récupération protègent contre la perte de données.

Exigence	Sous-exigence	O/N	Notes
Gestion des versions	Suivi des versions de fichiers		
	Enregistrement de l'historique des modifications		
	Comparaison des versions		
Caractéristiques de récupération	Capacités de retour en arrière		
	Récupération ponctuelle		
	Restauration en vrac		
Protection des données	Prévention de la corruption		
	Sauvegardes automatisées		
	Contrôle de l'intégrité des données		
Capacités en matière d'IA	Prévision des pertes		

	Détection de la corruption		
	Optimisation de la récupération		

10. Capacités d'intégration

Conseil : de solides capacités d'intégration garantissent un fonctionnement sans faille avec les systèmes existants.

Exigence	Sous-exigence	O/N	Notes
Stockage en nuage	Intégration de Google Drive		
	Intégration de Dropbox		
	Intégration de OneDrive		
Systèmes d'entreprise	Disponibilité de l'API		
	Soutien à l'intégration personnalisée		
	Intégration du système d'authentification		
Outils de sécurité	Intégration CASB		
	Intégration SIEM		
	Intégration DLP		
Caractéristiques de l'IA	Découverte de l'API		
	Contrôle de l'intégration		
	Validation de la sécurité		

11. Soutien aux appareils mobiles

Conseil : le support mobile doit maintenir la sécurité tout en offrant une expérience utilisateur transparente.

Exigence	Sous-exigence	O/N	Notes
Gestion de l'accès	Accès mobile sécurisé		

	Authentification du dispositif		
	Politiques de contrôle d'accès		
Contrôles de sécurité	Possibilité d'effacement à distance		
	Verrouillage des appareils		
	Cryptage des données		
Multiplateforme	Support iOS		
	Support Android		
	Une sécurité cohérente		
Caractéristiques de l'IA	Politiques tenant compte du contexte		
	Surveillance du comportement		
	Évaluation des risques		

12. Interface conviviale

Conseil : l'interface doit concilier des fonctionnalités puissantes et une utilisation intuitive.

Exigence	Sous-exigence	O/N	Notes
Conception de l'interface	Paramètres de sécurité intuitifs		
	Flux de travail facile pour le partage de fichiers		
	Structure de navigation claire		
Tableaux de bord	Options de personnalisation de l'administration		
	Personnalisation pour l'utilisateur final		
	Vues de contrôle en temps réel		

Expérience	Outils de collaboration transparents		
	Traitement du langage naturel		
	Assistance contextuelle		

13. Évolutivité et performances

Conseil : l'évolutivité et les performances sont essentielles pour les déploiements en entreprise.

Exigence	Sous-exigence	O/N	Notes
Évolutivité	Soutien d'une large base d'utilisateurs		
	Traitement du volume de données		
	Déploiement multisite		
Performance	Transfert de données rapide		
	Synchronisation rapide		
	Accès à faible latence		
Infrastructure	Équilibrage de la charge		
	Haute disponibilité		
	Reprise après sinistre		

14. Défense prédictive alimentée par l'IA

Conseil : La défense alimentée par l'IA offre une sécurité proactive grâce à des analyses avancées et à la reconnaissance des formes.

Exigence	Sous-exigence	O/N	Notes
Analyse du trafic	Surveillance des modèles		
	Analyse du comportement		
	Inspection en temps réel		

Caractéristiques prédictives	Prévision de rupture		
	Prévision des risques		
	Anticipation des menaces		
Analyse du code	Détection de scripts malveillants		
	Enquête automatisée		
	Endiguement de la menace		

15. Réponse automatisée aux incidents

Conseil : L'automatisation de la réponse aux incidents réduit le temps de réaction tout en maintenant la précision de l'atténuation des menaces.

Exigence	Sous-exigence	O/N	Notes
Détection	Détection des brèches par l'IA		
	Classification des incidents		
	Évaluation de la gravité		
Réponse	Confinement automatisé		
	Neutralisation de la menace		
	Restauration du système		
Analyse	Analyse des causes profondes		
	Analyse d'impact		
	Enquête médico-légale		

16. Apprentissage continu et adaptation

Conseil : La formation continue permet de s'assurer que la solution évolue en fonction des nouvelles menaces et des nouveaux défis en matière de sécurité.

Exigence	Sous-exigence	O/N	Notes

Système d'apprentissage	Apprentissage par incident		
	Reconnaissance des formes		
	Analyse du comportement		
Boucle de rétroaction	Amélioration des alertes		
	Réduction des faux positifs		
	Amélioration de la détection		
Mises à jour du modèle	Entraînement régulier des modèles		
	Optimisation des performances		
	Amélioration de la précision		

5. Qualifications des fournisseurs

Expérience requise

1. Au moins 5 ans d'expérience dans le domaine des solutions de sécurité pour l'informatique en nuage
2. Expérience confirmée dans la mise en œuvre de projets d'entreprise
3. Forte présence sur le marché et reconnaissance du secteur
4. Une équipe de R&D dédiée à la sécurité
5. Une infrastructure de soutien complète

Certifications requises

1. Certification ISO 27001
2. Conformité SOC 2 Type II
3. Certifications de sécurité spécifiques à l'industrie
4. Certifications du personnel professionnel
5. Validation de la sécurité des produits

6. Critères d'évaluation

Capacité technique (40%)

- Complétude des caractéristiques
- Capacités de sécurité
- Mesures de performance
- Évolutivité
- Capacités d'intégration

Mise en œuvre et soutien (30 %)

- Méthodologie de mise en œuvre
- Structure de soutien
- Programmes de formation
- Qualité de la documentation
- Expertise technique

Qualification des fournisseurs (20%)

- Stabilité de l'entreprise
- Présence sur le marché
- Références clients
- L'histoire de l'innovation
- L'écosystème du partenariat

Structure des coûts (10%)

- Modèle de licence
- Coûts de mise en œuvre
- Coûts de soutien
- Coûts de formation
- Coût total de possession

7. Exigences en matière de soumission

Documentation requise

1. Proposition technique
    - Description détaillée de la solution
    - Diagrammes d'architecture
    - Spécifications de sécurité
    - Capacités d'intégration
2. Plan de mise en œuvre
    - Calendrier du projet
    - Allocation des ressources
    - Gestion des risques
    - Assurance qualité
3. Plan de soutien
    - Niveaux de soutien
    - Temps de réponse
    - Procédures d'escalade
    - Approche de la formation
4. Proposition commerciale
    - Modèle de licence
    - Coûts de mise en œuvre
    - Coûts de soutien
    - Services complémentaires

8. Calendrier et processus

Dates clés

- 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]

9. Informations sur les contacts

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