Demande de proposition : Solution logicielle de sécurité en périphérie des nuages

Table des matières

1. Introduction et contexte

Notre organisation recherche des propositions pour une solution logicielle complète de sécurité à la périphérie du nuage afin d'améliorer notre infrastructure de sécurité du réseau. Cet appel d'offres décrit nos besoins pour un système robuste qui fournira un accès sécurisé à Internet et aux applications en nuage à la périphérie du nuage, où les capacités de calcul sont positionnées plus près des appareils finaux. La solution doit utiliser la technologie SD-WAN (Software-Defined Wide Area Network) et intégrer les fonctions de sécurité du réseau pour une expérience transparente, en renforçant la sécurité dans les environnements distribués.

2. Objectifs du projet

Les principaux objectifs de ce projet sont les suivants

1. Mettre en œuvre une solution complète de sécurité à la périphérie du nuage qui fournit une protection avancée à la périphérie du réseau.

2. Intégrer les capacités de sécurité dans un cadre SASE unifié
3. Permettre un accès sécurisé aux données et aux applications sur tous les appareils et dans tous les lieux.
4. Déployer des fonctions de sécurité avancées grâce à l'intégration SD-WAN
5. Garantir la sécurité des données et des transactions en temps réel
6. Mettre en œuvre les principes de sécurité "zéro confiance" dans l'ensemble de l'infrastructure
7. Optimiser les capacités de l'informatique en périphérie grâce à une protection intégrée

3. L'étendue des travaux

Le fournisseur sélectionné sera responsable de

1. Fournir une solution de sécurité en périphérie basée sur l'informatique en nuage qui comprend :
    - Mise en œuvre du cadre SASE
    - Intégration de fonctions de sécurité avancées
    - Contrôles de la sécurité des données
    - Sécurité des transactions en temps réel
    - Gestion de la sécurité en périphérie
2. Services de mise en œuvre :
    - Déploiement et configuration de la solution
    - Intégration à l'infrastructure existante
    - Migration des politiques de sécurité existantes
    - Optimisation des performances
3. Formation et soutien :
    - Formation des administrateurs

- Formation des utilisateurs finaux
- Assistance technique permanente
- Documentation et transfert de connaissances

4. Exigences techniques

1. Intégration du cadre SASE :
    - Courtier en sécurité de l'accès au nuage (CASB)
    - Accès au réseau sans confiance
    - Pare-feu en tant que service (FWaaS)
    - Passerelle Web sécurisée
    - Capacités SD-WAN
    - Sécurité de l'informatique en périphérie
2. Fonctions de sécurité avancées :
    - Filtrage du web
    - Protection contre les logiciels malveillants
    - Système de prévention des intrusions (IPS)
    - Pare-feu de nouvelle génération
    - Protection avancée contre les menaces
    - Contrôles de sécurité dans l'informatique dématérialisée
3. Sécurité des données :
    - Cryptage en temps réel
    - Prévention des pertes de données
    - Sécurité des transactions
    - Protection des données dans le nuage
    - Sécurité des données

- Contrôles d'accès

4. Protection de l'informatique en périphérie :
    - Sécurité des appareils en périphérie
    - Sécurité de l'IdO
    - Contrôles de sécurité distribués
    - Optimisation des performances des bords
    - Sécurité du traitement local des données
    - Gestion des ressources en périphérie

5. Exigences fonctionnelles

1. Chiffrement des données en temps réel

Conseil : Le chiffrement des données à la périphérie du nuage exige une attention particulière pour les données en transit et au repos dans les environnements distribués. Privilégiez les solutions qui assurent un chiffrement transparent entre les emplacements du nuage et de la périphérie, tout en maintenant les performances à toutes les extrémités du réseau.

Exigence	Sous-exigence	O/N	Notes
Chiffrement des données en temps réel	Chiffrement des données d'un bout à l'autre du nuage		
	Cryptage intermédiaire		
	Infrastructure sécurisée de gestion des clés		
	Algorithmes de cryptage conformes aux normes industrielles		
	Gestion de la politique de chiffrement en périphérie		
	Intégration de la gestion des clés dans le nuage		

	Gestion du cycle de vie des certificats		
	Cryptage des sauvegardes		
	Gestion des clés à plusieurs endroits		
	Rapport sur le chiffrement distribué		

2. Détection et atténuation des menaces

Conseil : la détection des menaces en périphérie nécessite des capacités de renseignement distribué et de réponse coordonnée. Recherchez des solutions capables de détecter et de répondre aux menaces à la périphérie tout en conservant une visibilité et un contrôle centralisés.

Exigence	Sous-exigence	O/N	Notes
Détection et atténuation des menaces	Surveillance en temps réel basée sur la périphérie		
	Mécanismes de réponse distribués		
	Détection des menaces dans l'informatique en nuage		
	Intégration des renseignements sur les menaces		
	Analyse comportementale à la périphérie		
	Détection des APT distribuées		
	Protection contre les attaques de type "zero-day" basée sur la périphérie		
	Protection contre les ransomwares en nuage		
	Détection des menaces sur les réseaux périphériques		
	Détection distribuée des points d'extrémité		

3. Cadre SASE

Conseil : la mise en œuvre de SASE doit combiner de manière transparente les capacités de réseau et de sécurité à la périphérie. Concentrez-vous sur les solutions qui intègrent efficacement le SD-WAN et les fonctions de sécurité tout en maintenant les performances et l'évolutivité.

Exigence	Sous-exigence	O/N	Notes
Cadre SASE	Intégration CASB		
	Mise en œuvre d'un réseau de confiance zéro		
	Déploiement de FWaaS		
	Optimisation SD-WAN		
	Consolidation de la sécurité en périphérie		
	Intégration de la sécurité dans l'informatique en nuage		
	Application distribuée des politiques		
	Contrôle d'accès à la périphérie		
	Sécurité des applications en nuage		
	Optimisation des performances des bords		

4. Surveillance de l'activité de la périphérie

Conseil : Une surveillance complète de la périphérie nécessite une visibilité sur des sites distribués tout en conservant un contrôle centralisé. La solution doit fournir des informations détaillées sur les activités en périphérie tout en gérant efficacement les données de surveillance sur l'ensemble du réseau.

Exigence	Sous-exigence	O/N	Notes
Surveillance de l'activité de la périphérie	Suivi d'activité distribué		
	Enregistrement des événements de bord		

	Détection des comportements en temps réel		
	Génération de rapports basés sur les bords		
	Contrôle de conformité à la périphérie		
	Analyse de l'activité sur plusieurs sites		
	Analyse du comportement des utilisateurs		
	Audit d'accès distribué		
	Journalisation de l'administration Edge		
	Rapports de bord automatisés		

5. Intelligence périphérique alimentée par l'IA

Conseil : Les capacités d'IA à la périphérie doivent renforcer la sécurité tout en optimisant les performances. Évaluez les solutions en fonction de leur capacité à traiter les charges de travail d'IA à la périphérie tout en maintenant la sécurité et en réduisant la latence.

Exigence	Sous-exigence	O/N	Notes
L'intelligence des bords alimentée par l'IA	Analyse ML basée sur les arêtes		
	Détection des menaces distribuées		
	Prévention de l'hameçonnage		
	Analyse des fichiers locaux		
	Protection basée sur la périphérie		

	Reconnaissance des formes distribuées		
	Modélisation du comportement des bords		
	Analyse prédictive locale		
	Réponse basée sur les bords		
	Capacités d'apprentissage distribué		

6. Gestion des politiques de périphérie assistée par l'IA

Conseil : La gestion des politiques de sécurité à la périphérie nécessite une automatisation intelligente capable de s'adapter aux environnements distribués. Recherchez des solutions capables de maintenir des politiques cohérentes sur toutes les périphéries tout en s'adaptant aux conditions locales.

Exigence	Sous-exigence	O/N	Notes
Gestion de la politique de la périphérie	Configuration de l'IA en fonction de la périphérie		
	Gestion des règles distribuées		
	Politiques de périphérie tenant compte du contexte		
	Optimisation de la politique de lisière		
	Flux de travail simplifiés		
	Contrôle de la conformité des bords		
	Évaluation des risques distribués		
	Validation de la politique de lisière		
	Gestion du changement à plusieurs niveaux		

	Analyse de l'impact sur les bords		

7. Optimisation de l'IA

Conseil : L'optimisation de l'IA en périphérie est cruciale pour maintenir la sécurité sans compromettre les performances dans les environnements distribués. Concentrez-vous sur des solutions qui traitent efficacement les charges de travail de sécurité à la périphérie tout en assurant une protection cohérente.

Exigence	Sous-exigence	O/N	Notes
Optimisation de l'IA	Intégration de l'IA au niveau local		
	Optimisation du déploiement de la périphérie		
	Orchestration distribuée		
	Optimisation des ressources en périphérie		
	Suivi des performances locales		
	Gestion de la latence en périphérie		
	Mise à l'échelle distribuée		
	Optimisation du matériel Edge		
	Gestion locale de l'énergie		
	Protocoles de basculement		

8. Surveillance en temps réel de la périphérie

Conseil : la surveillance en périphérie exige une visibilité complète sur des sites distribués tout en gérant efficacement les volumes d'alertes. Concentrez-vous sur des solutions qui fournissent des informations exploitables à la périphérie tout en maintenant un contrôle central.

Exigence	Sous-exigence	O/N	Notes
Surveillance des bords	Surveillance de l'activité distribuée		

	Seuils d'alerte basés sur les bords		
	Distribution locale des alertes		
	Corrélation entre les événements de bord		
	Intégration de SIEM distribué		
	Actions de réponse basées sur les bords		
	Conservation des données locales		
	Création de règles de bord		
	Analyse distribuée des tendances		
	Détection des menaces à la périphérie		

9. Réponse basée sur les bords

Conseil : La réponse automatisée à la périphérie exige un équilibre délicat entre rapidité et précision. Évaluez les solutions qui peuvent répondre rapidement aux menaces à la périphérie tout en maintenant des contrôles appropriés.

Exigence	Sous-exigence	O/N	Notes
Réponse basée sur les bords	Manuels d'intervention en cas d'urgence		
	Actions de réponse locales		
	Capacités de mise en quarantaine de la périphérie		
	Remédiation distribuée		
	Fonctionnalités de retour en arrière		
	Gestion locale des incidents		
	Automatisation du flux de travail		

	Flux de travail d'approbation distribués		
	Enregistrement de la réaction des bords		
	Test d'efficacité locale		

6. Qualifications des fournisseurs

1. Expérience confirmée dans la mise en œuvre de la sécurité de la périphérie des nuages
2. Forte présence sur le marché des SASE et de la sécurité périphérique
3. Expérience réussie en matière de déploiement d'une sécurité de pointe
4. Prise en charge complète des environnements distribués
5. Stabilité financière
6. Certifications en matière de sécurité
7. R&D active dans le domaine de la sécurité de l'IA de pointe
8. Satisfaction de la clientèle dans les déploiements en périphérie

7. Critères d'évaluation

1. Capacités de sécurité en périphérie
2. Mise en œuvre du cadre SASE
3. Capacités en matière d'IA/ML
4. Capacités d'intégration à la pointe de la technologie
5. Évolutivité des bords
6. Coût total de possession
7. Services de soutien distribués
8. Méthodologie de mise en œuvre d'Edge
9. Approche de la formation en matière de sécurité

8. Lignes directrices pour la soumission

1. Proposition de solution technique
2. Plan de mise en œuvre de l'Edge
3. Structure de tarification de la sécurité des bords
4. Profil de l'entreprise
5. Références de déploiement en périphérie
6. Exemples de rapports sur la sécurité des bords
7. Détails du support de bord
8. Plan de formation à la sécurité des bords

9. Informations sur les contacts

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