# Aufforderung zur Angebotsabgabe: Cloud Edge Security Software-Lösung

## Inhaltsübersicht



## 1. Einleitung und Hintergrund

Unsere Organisation bittet um Angebote für eine umfassende Cloud-Edge-Sicherheitssoftwarelösung zur Verbesserung unserer Netzsicherheitsinfrastruktur. Diese Ausschreibung umreißt unsere Anforderungen an ein robustes System, das einen sicheren Zugang zum Internet und zu Cloud-Anwendungen am Cloud-Edge bietet, wo die Rechenkapazitäten näher an den Endgeräten positioniert sind. Die Lösung muss die SD-WAN-Technologie (Software-Defined Wide Area Network) nutzen und Netzwerksicherheitsfunktionen für eine nahtlose Erfahrung integrieren, um die Sicherheit in verteilten Umgebungen durchzusetzen.

## 2. Projektziele

Die Hauptziele dieses Projekts sind:

1. Implementierung einer umfassenden Cloud-Edge-Sicherheitslösung, die erweiterten Schutz am Netzwerkrand bietet
2. Integration von Sicherheitsfunktionen in einen einheitlichen SASE-Rahmen

3. Ermöglichen Sie den sicheren Zugriff auf Daten und Anwendungen über alle Geräte und Standorte hinweg
4. Bereitstellung erweiterter Sicherheitsfunktionen mit SD-WAN-Integration
5. Gewährleistung der Daten- und Transaktionssicherheit in Echtzeit
6. Umsetzung von Zero-Trust-Sicherheitsprinzipien in der gesamten Infrastruktur
7. Optimierung der Edge-Computing-Funktionen mit integriertem Schutz

## 3. Umfang der Arbeit

Der ausgewählte Anbieter wird für folgende Aufgaben verantwortlich sein:

1. Bereitstellung einer Cloud-basierten Edge-Sicherheitslösung, die Folgendes umfasst:
   - Implementierung des SASE-Rahmens
   - Integration erweiterter Sicherheitsfunktionen
   - Kontrollen der Datensicherheit
   - Transaktionssicherheit in Echtzeit
   - Edge-Sicherheitsmanagement
2. Implementierung von Dienstleistungen:
   - Bereitstellung und Konfiguration der Lösung
   - Integration in die bestehende Infrastruktur
   - Migration bestehender Sicherheitsrichtlinien
   - Optimierung der Leistung
3. Ausbildung und Unterstützung:
   - Ausbildung zum Administrator
   - Schulung der Endbenutzer
   - Laufende technische Unterstützung

- Dokumentation und Wissenstransfer

## 4. Technische Anforderungen

1. SASE Framework Integration:
    - Cloud Access Security Broker (CASB)
    - Zero Trust Netzwerkzugang
    - Firewall als Dienstleistung (FWaaS)
    - Sicheres Web-Gateway
    - SD-WAN-Fähigkeiten
    - Sicherheit beim Edge Computing
2. Erweiterte Sicherheitsfunktionen:
    - Web-Filterung
    - Anti-Malware-Schutz
    - Intrusion Prevention System (IPS)
    - Firewalls der nächsten Generation
    - Erweiterter Schutz vor Bedrohungen
    - Sicherheitskontrollen in der Cloud
3. Datensicherheit:
    - Verschlüsselung in Echtzeit
    - Vermeidung von Datenverlusten
    - Transaktionssicherheit
    - Schutz von Daten in der Cloud
    - Sicherheit von Randdaten
    - Zugangskontrollen
4. Schutz des Edge-Computing:

- Sicherheit von Edge-Geräten
- IoT-Sicherheit
- Verteilte Sicherheitskontrollen
- Optimierung der Kantenleistung
- Sicherheit der lokalen Datenverarbeitung
- Verwaltung der Randressourcen

## 5. Funktionale Anforderungen

### 1. Datenverschlüsselung in Echtzeit

***Tipp: Die Verschlüsselung von Daten am Cloud-Edge erfordert besondere Aufmerksamkeit für Daten, die über verteilte Umgebungen hinweg übertragen und gespeichert werden. Konzentrieren Sie sich auf Lösungen, die eine nahtlose Verschlüsselung über Cloud- und Edge-Standorte hinweg bieten und gleichzeitig die Leistung an allen Netzwerkrändern aufrechterhalten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Datenverschlüsselung in Echtzeit | Edge-to-Cloud-Datenverschlüsselung | | |
| | Inter-Edge-Verschlüsselung | | |
| | Sichere Infrastruktur für die Schlüsselverwaltung | | |
| | Industriestandard-Verschlüsselungsalgorithmen | | |
| | Edge-basierte Verwaltung von Verschlüsselungsrichtlinien | | |
| | Integration der Cloud-Schlüsselverwaltung | | |
| | Verwaltung des Lebenszyklus von Zertifikaten | | |

| | | | |
|---|---|---|---|
| | Edge-Backup-Verschlüsselung | | |
| | Standortübergreifende Schlüsselverwaltung | | |
| | Verteilte Verschlüsselungsberichte | | |

## 2. Erkennung und Eindämmung von Bedrohungen

***Tipp: Edge-basierte Bedrohungserkennung erfordert verteilte Informationen und koordinierte Reaktionsmöglichkeiten. Suchen Sie nach Lösungen, die Bedrohungen am Rande des Netzwerks erkennen und darauf reagieren können, ohne die zentrale Sichtbarkeit und Kontrolle zu verlieren.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Erkennung und Eindämmung von Bedrohungen | Edge-basierte Echtzeit-Überwachung | | |
| | Verteilte Reaktionsmechanismen | | |
| | Erkennung von Bedrohungen aus der Cloud | | |
| | Integration von Edge-Bedrohungsdaten | | |
| | Verhaltensanalyse am Rande | | |
| | Verteilte APT-Erkennung | | |
| | Edge-basierter Zero-Day-Schutz | | |
| | Cloud-basierter Schutz vor Ransomware | | |
| | Erkennung von Bedrohungen im Edge-Netzwerk | | |

| | | | |
|---|---|---|---|
| | Verteilte Endpunkt-Erkennung | | |

### 3. SASE-Rahmen

***Tipp: Eine SASE-Implementierung muss Netzwerk- und Sicherheitsfunktionen am Netzwerkrand nahtlos kombinieren. Konzentrieren Sie sich auf Lösungen, die SD-WAN effektiv mit Sicherheitsfunktionen integrieren und dabei Leistung und Skalierbarkeit beibehalten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| SASE-Rahmen | CASB-Integration | | |
| | Implementierung des Zero Trust Network | | |
| | FWaaS-Bereitstellung | | |
| | SD-WAN-Optimierung | | |
| | Konsolidierung der Edge-Sicherheit | | |
| | Integration der Cloud-Sicherheit | | |
| | Verteilte Durchsetzung von Richtlinien | | |
| | Zugangskontrolle am Rand | | |
| | Sicherheit von Cloud-Anwendungen | | |
| | Optimierung der Kantenleistung | | |

### 4. Überwachung der Randaktivitäten

***Tipp: Umfassende Edge-Überwachung erfordert Transparenz über verteilte Standorte hinweg bei gleichzeitiger zentraler Kontrolle. Die Lösung sollte detaillierte Einblicke in Edge-Aktivitäten bieten und gleichzeitig die Überwachungsdaten im gesamten Netzwerk effizient verwalten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Überwachung von Randaktivitäten | Verteilte Aktivitätsverfolgung | | |
| | Ereignisprotokollierung am Rand | | |
| | Verhaltenserkennung in Echtzeit | | |
| | Edge-basierte Berichterstellung | | |
| | Überwachung der Einhaltung der Vorschriften am Rande | | |
| | Standortübergreifende Aktivitätsanalyse | | |
| | Analyse des Randverhaltens | | |
| | Verteilte Zugriffsprüfung | | |
| | Protokollierung der Edge-Verwaltung | | |
| | Automatisierte Randberichte | | |

### 5. KI-gestützte Edge Intelligence

***Tipp: KI-Funktionen am Edge sollten die Sicherheit verbessern und gleichzeitig die Leistung optimieren. Bewerten Sie Lösungen anhand ihrer Fähigkeit, KI-Workloads am Edge zu verarbeiten und dabei die Sicherheit aufrechtzuerhalten und die Latenz zu reduzieren.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| AI-gestützte Edge-Intelligenz | Kantenbasierte ML-Analyse | | |
| | Erkennung verteilter Bedrohungen | | |
| | Edge-Phishing-Prävention | | |
| | Analyse lokaler Dateien | | |

| | | | |
|---|---|---|---|
| | Kantenbasierter Schutz | | |
| | Verteilte Mustererkennung | | |
| | Modellierung des Kantenverhaltens | | |
| | Lokale prädiktive Analytik | | |
| | Kantenbasierte Antwort | | |
| | Verteilte Lernmöglichkeiten | | |

### 6. KI-gestütztes Edge Policy Management

***Tipp: Die Richtlinienverwaltung für Edge-Sicherheit erfordert eine intelligente Automatisierung, die sich an verteilte Umgebungen anpassen kann. Suchen Sie nach Lösungen, die konsistente Richtlinien über alle Kanten hinweg aufrechterhalten und sich gleichzeitig an lokale Bedingungen anpassen können.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Edge Policy Management | Edge-aware AI-Konfiguration | | |
| | Verteiltes Regelmanagement | | |
| | Kontextabhängige Edge-Richtlinien | | |
| | Optimierung der Randbedingungen | | |
| | Vereinfachte Edge-Workflows | | |
| | Prüfung der Einhaltung von Grenzwerten | | |
| | Verteilte Risikobewertung | | |
| | Validierung der Edge-Policy | | |

| | | | |
|---|---|---|---|
| | Mehrstufiges Änderungsmanagement | | |
| | Analyse der Auswirkungen auf den Rand | | |

### 7. Edge AI-Optimierung

***Tipp: Die Optimierung von Edge AI ist entscheidend für die Aufrechterhaltung der Sicherheit ohne Leistungseinbußen in verteilten Umgebungen. Konzentrieren Sie sich auf Lösungen, die Sicherheits-Workloads am Edge effizient verarbeiten und gleichzeitig einen konsistenten Schutz gewährleisten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Edge AI-Optimierung | Lokale AI-Laufzeitintegration | | |
| | Optimierung des Edge-Einsatzes | | |
| | Verteilte Orchestrierung | | |
| | Optimierung der Randressourcen | | |
| | Lokale Leistungsüberwachung | | |
| | Verwaltung der Latenzzeiten am Rand | | |
| | Verteilte Skalierung | | |
| | Optimierung von Edge-Hardware | | |
| | Lokale Energieverwaltung | | |
| | Edge-Failover-Protokolle | | |

### 8. Echtzeit-Edge-Überwachung

***Tipp: Die Edge-Überwachung erfordert eine umfassende Transparenz über verteilte Standorte hinweg bei gleichzeitiger effektiver Verwaltung des Alarmvolumens. Konzentrieren Sie sich auf Lösungen, die verwertbare***

***Erkenntnisse am Edge liefern und gleichzeitig eine zentrale Kontrolle ermöglichen.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Überwachung der Ränder | Verteilte Aktivitätsüberwachung | | |
| | Edge-basierte Warnschwellenwerte | | |
| | Lokale Verteilung von Warnmeldungen | | |
| | Korrelation von Randereignissen | | |
| | Verteilte SIEM-Integration | | |
| | Kantenbasierte Antwortaktionen | | |
| | Lokale Datenspeicherung | | |
| | Erstellung von Kantenregeln | | |
| | Verteilte Trendanalyse | | |
| | Erkennung von Edge-Bedrohungen | | |

## 9. Kantenbasierte Reaktion

***Tipp: Die automatisierte Reaktion am Netzwerkrand erfordert eine sorgfältige Abwägung zwischen Geschwindigkeit und Genauigkeit. Evaluieren Sie Lösungen, die schnell auf Bedrohungen am Netzwerkrand reagieren können und gleichzeitig angemessene Kontrollen gewährleisten.***

| Anforderung | Teilanforderung | JA/NEIN | Anmerkungen |
|---|---|---|---|
| Kantenbasierte Antwort | Spielbücher für die Kantenreaktion | | |
| | Lokale Reaktionsmaßnahmen | | |

| | | | |
|---|---|---|---|
| | Edge-Quarantäne-Funktionen | | |
| | Verteilte Abhilfemaßnahmen | | |
| | Edge-Rollback-Funktionen | | |
| | Lokales Notfallmanagement | | |
| | Automatisierung von Arbeitsabläufen am Rande | | |
| | Verteilte Genehmigungs-Workflows | | |
| | Protokollierung der Kantenreaktion | | |
| | Lokale Wirksamkeitstests | | |

## 6. Qualifikationen des Anbieters

1. Nachgewiesene Erfahrung in der Implementierung von Cloud-Edge-Sicherheit
2. Starke Präsenz auf dem SASE- und Edge-Security-Markt
3. Erfolgreiche Erfolgsbilanz beim Einsatz von Edge Security
4. Umfassende Unterstützung für verteilte Umgebungen
5. Finanzielle Stabilität
6. Edge-Sicherheitszertifizierungen
7. Aktive FuE im Bereich KI-Sicherheit
8. Kundenzufriedenheit bei Edge-Implementierungen

## 7. Kriterien für die Bewertung

1. Edge-Sicherheitsfunktionen
2. Implementierung des SASE-Rahmens
3. Edge AI/ML-Fähigkeiten
4. Fähigkeiten zur Integration in die Cloud

5. Skalierbarkeit am Rand
6. Gesamtbetriebskosten
7. Verteilte Unterstützungsdienste
8. Methodik der Randeinführung
9. Schulungsansatz für die Sicherheit am Rande

## 8. Einreichungsrichtlinien

1. Vorschlag für eine technische Lösung
2. Plan zur Umsetzung der Kante
3. Preisstruktur für Randsicherheiten
4. Profil des Unternehmens
5. Referenzen für den Edge-Einsatz
6. Beispiele für Sicherheitsberichte am Rande
7. Details zur Kantenunterstützung
8. Schulungsplan für die Sicherheit am Rande

## 9. Kontaktinformationen

Bitte senden Sie Vorschläge und Fragen an: [Name der Kontaktperson] [E-Mail-Adresse] [Telefonnummer]