Aufforderung zur Angebotsabgabe: Cloud Access Security Broker (CASB) Software-Lösung

Inhaltsübersicht

1. Einleitung und Hintergrund

Unsere Organisation bittet um Angebote für eine umfassende Cloud Access Security Broker (CASB)-Lösung, um unsere Cloud-Sicherheitslage zu verbessern und den Schutz unserer Cloud-basierten Ressourcen zu gewährleisten. Die ausgewählte CASB-Lösung wird als wichtiger Sicherheitskontrollpunkt zwischen unseren Cloud-Service-Kunden und Cloud-Service-Anbietern dienen.

1.1 Marktkontext

- Der CASB-Markt wächst mit einer CAGR von ca. 17,6% (2021-2026)
- Die Implementierungskosten liegen in der Regel zwischen $15.000 und $100.000+ pro Jahr.
- Die Lösung sollte sich an den Fähigkeiten der derzeitigen Marktführer orientieren und gleichzeitig innovative Funktionen bieten

1.2 Erwartungen an den Unternehmenswert

- Verbesserte Cloud-Sicherheitslage durch einheitliche Kontrolle
- Verbesserte Transparenz bei der Nutzung von Cloud-Diensten
- Gestärkte Fähigkeiten zur Einhaltung von Vorschriften
- Signifikante Risikominderung für den Cloud-Betrieb
- Optimierte Kosten durch kontrollierte Cloud-Nutzung

2. Projektziele

2.1 Primäre Zielsetzungen

1. Bereitstellung einer umfassenden CASB-Lösung, die Transparenz und Kontrolle über Cloud-Services bietet
2. Umsetzung robuster Datenschutzmaßnahmen für in der Cloud gehostete Informationen
3. Einrichtung von Funktionen zur Echtzeitüberwachung und Erkennung von Bedrohungen
4. Granulares Richtlinienmanagement für alle Cloud-Dienste ermöglichen
5. Sicherstellung der Einhaltung der gesetzlichen Vorschriften
6. Optimierung der Nutzung von Cloud-Diensten und der damit verbundenen Kosten

2.2 Strategische Ziele

1. Reduzierung der Sicherheitsvorfälle im Zusammenhang mit der Nutzung von Cloud-Diensten um 75 %.
2. 100%ige Transparenz bei der Nutzung von Cloud-Anwendungen erreichen

3. Automatisierte Durchsetzung von Richtlinien für alle Cloud-Services
4. Implementierung konsistenter Datenschutzmaßnahmen für alle Cloud-Plattformen
5. Proaktive Erkennung und Reaktion auf Bedrohungen ermöglichen
6. Rationalisierung der Sicherheitsabläufe durch Automatisierung

3. Umfang der Arbeit

3.1 Anforderungen an die technische Architektur

1. Bereitstellungsmodelle
    - Fähigkeit zur Bereitstellung von Forward-Proxys
    - Option zur Bereitstellung eines Reverse-Proxys
    - API-basierte Konnektivität für Cloud-Dienste
    - Flexibilität bei der Bereitstellung in mehreren Modi
    - Unterstützung für hybride Architekturen
2. Integrationspunkte
    - Systeme zur Identitäts- und Zugangsverwaltung (IAM)
    - Sicherheitsinformationen und Ereignisverwaltung (SIEM)
    - Systeme zur Verhinderung von Datenverlusten (DLP)
    - Mobilitätsmanagement für Unternehmen (EMM)
    - Security Orchestration and Response (SOAR)
    - Bestehende Sicherheitsinfrastruktur
3. Kernkomponenten
    - Cloud Security Gateway
    - Politik-Engine
    - Modul Datenschutz

- System zur Verhinderung von Bedrohungen
- Analyse-Engine
- Management-Konsole

4. Technische Anforderungen

4.1 Architektur und Infrastruktur

1. Flexibilität bei der Bereitstellung
    - Unterstützung der Cloud-basierten Bereitstellung
    - Möglichkeit der Bereitstellung vor Ort
    - Hybride Bereitstellungsoptionen
    - Architektur mit mehreren Mandanten
    - Konfiguration für hohe Verfügbarkeit
2. Leistungsspezifikationen
    - Maximale Latenzzeit: 50 ms für Inline-Operationen
    - Minimaler Durchsatz: 10Gbps
    - Unterstützung für mehr als 100.000 gleichzeitige Benutzer
    - 99,99% Betriebszeit-Garantie
    - Durchsetzung von Richtlinien in Echtzeit
3. Sicherheitsarchitektur
    - Ende-zu-Ende-Verschlüsselung (TLS 1.3)
    - Unterstützung von Hardware-Sicherheitsmodulen (HSM)
    - Sichere Schlüsselverwaltung
    - Verwaltung des Lebenszyklus von Zertifikaten
    - Fähigkeiten zur Sicherheitshärtung

5. Funktionale Anforderungen

5.1 Benutzer- und Zugangsverwaltung

Tipp: Eine solide Benutzer- und Zugriffsverwaltung ist für die Cloud-Sicherheit von grundlegender Bedeutung. Stellen Sie sicher, dass die Lösung umfassende Authentifizierungsmethoden, granulare Zugriffskontrollen und eine detaillierte Aktivitätsüberwachung bietet, um die Sicherheit zu gewährleisten und gleichzeitig die Produktivität zu steigern.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Benutzerauthentifizierung	Unterstützung der Multi-Faktor-Authentifizierung		
	Integration mit SSO-Lösungen für Unternehmen		
	Step-up-Authentifizierung für sensible Vorgänge		
	Sitzungsmanagement und Timeout-Kontrollen		
	Gerätebasierte Authentifizierungsoptionen		
Zugangskontrolle	Rollenbasierte Zugriffskontrolle (RBAC)		
	Attributbasierte Zugriffskontrolle (ABAC)		
	Standortbezogene Zugangsbeschränkungen		
	Zeitbasierte Zugangsrichtlinien		
	Überprüfung der Gerätestruktur		
Überwachung der Benutzeraktivitäten	Aktivitätsprotokollierung in Echtzeit		

	Aufzeichnung von Benutzersitzungen		
	Verfolgung des Dateizugriffs		
	Protokollierung von Konfigurationsänderungen		
	Prüfung der Verwaltungstätigkeit		

5.2 Datenschutz

Tipp: Umfassende Datenschutzfunktionen sollten den gesamten Lebenszyklus von Daten in Cloud-Umgebungen abdecken. Konzentrieren Sie sich auf Lösungen, die einen tiefen Einblick in die Datenbewegungen, robuste Kontrollen und flexible Verschlüsselungsoptionen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Entdeckung von Daten	Automatisierte Erkennung sensibler Daten		
	Benutzerdefinierte Datenmustererkennung		
	Scannen von strukturierten und unstrukturierten Daten		
	Überwachung von Datenbankverbindungen		
	Datenklassifizierung in Echtzeit		
Prävention von Datenverlusten	Regeln für die Inhaltskontrolle		
	Dateityp-Kontrollen		
	Wasserzeichen-Funktionen		
	Screenshot-Verhinderung		

	Steuerelemente zum Kopieren/Einfügen		
Verwaltung der Verschlüsselung	Schlüsselverwaltung		
	Verwaltung des Lebenszyklus von Zertifikaten		
	Durchsetzung von Verschlüsselungsrichtlinien		
	Daten-Tokenisierung		
	Formaterhaltende Verschlüsselung		

5.3 Kontrolle von Cloud-Anwendungen

Tipp: Die Kontrolle von Cloud-Anwendungen ist entscheidend für die Aufrechterhaltung der Sicherheit in Cloud-Umgebungen. Konzentrieren Sie sich auf Funktionen, die einen umfassenden Einblick in die Nutzung von Cloud-Anwendungen, eine Risikobewertung und eine granulare Kontrolle über den Zugriff und die gemeinsame Nutzung von Daten bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Entdeckung von Anwendungen	Automatisierte App-Erkennung		
	Einstufung der Risikobewertung		
	Analyse der Verwendungsmuster		
	Erkennung von Schatten-IT		
	App-Kategorisierung		
Verwaltung von Anwendungen	Verwaltung von Erlaubnis-/Blockierlisten		

	Richtlinien für den Anwendungszugang		
	API-Zugangskontrolle		
	Integration von Drittanbieteranwendungen		
	Benutzerdefiniertes App-Onboarding		

5.4 Schutz vor Bedrohungen

Tipp: Moderner Bedrohungsschutz erfordert mehrschichtige Abwehrmechanismen, die sowohl bekannte als auch unbekannte Bedrohungen erkennen und darauf reagieren können. Bewerten Sie Lösungen nach ihrer Fähigkeit, Echtzeitschutz, erweiterte Analysen und automatische Reaktionsmöglichkeiten zu bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Erkennung von Bedrohungen	Malware-Scans		
	Schutz vor Ransomware		
	Erkennung von Anomalien		
	Schutz vor fortgeschrittenen anhaltenden Bedrohungen (APT)		
	Erkennung von Zero-Day-Bedrohungen		
Sicherheitsanalytik	Verhaltensanalyse		
	Risiko-Scoring		
	Integration von Bedrohungsdaten		

	Mustererkennung		
	Prädiktive Analytik		

5.5 Verwaltung von Richtlinien

Tipp: Eine wirksame Richtlinienverwaltung ist die Grundlage für die CASB-Implementierung. Suchen Sie nach Lösungen, die flexible Richtlinienerstellung, granulare Kontrollen und automatische Durchsetzungsfunktionen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Politikgestaltung	Vorlagenbasierte Richtlinienerstellung		
	Custom policy builder		
	Politische Vererbung		
	Versionskontrolle		
	Testumgebung für Richtlinien		
Durchsetzung der Politik	Richtliniendurchsetzung in Echtzeit		
	Automatisierte Abhilfemaßnahmen		
	Warnungen bei Richtlinienverstößen		
	Verwaltung von Ausnahmen		
	Granulare Richtlinienkontrolle		

5.6 KI- und maschinelle Lernfähigkeiten

Tipp: Fortschrittliche KI- und ML-Funktionen sollten praktische Sicherheitsvorteile bieten und gleichzeitig die Transparenz bei der Entscheidungsfindung wahren. Konzentrieren Sie sich auf Lösungen, die erklärbare KI und nachweisbare Sicherheitsverbesserungen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
KI-gestützte Erkennung von Bedrohungen	Adaptive Erkennung von Bedrohungsmustern		
	Vorausschauende Analyse von Bedrohungen		
	Verarbeitung natürlicher Sprache zur Datenklassifizierung		
	Identifizierung von Zero-Day-Angriffsmustern		
	Korrelation von Multi-Vektor-Angriffen		
KI-unterstützte Analyse des Benutzerverhaltens	Dynamische Bewertung von Benutzerrisiken		
	Intelligente Sitzungsanalyse		
	Abbildung von Entitätsbeziehungen		
	Verhaltensbasierte Anpassung		
	Erkennung von Anomalien und Korrelation		
Autonome Reaktion und Abhilfemaßnahmen	Selbstlernende Abhilfemaßnahmen		
	Intelligente Automatisierung von Richtlinien		
	Automatisierte Antwortoptimierung		

	Kontextabhängige Anpassung von Richtlinien		
	Risikobasierte Optimierung der Politik		
KI-gesteuerte Cloud-App-Intelligenz	Anwendung Verhalten lernen		
	Risikobewertung für intelligente Anwendungen		
	Dynamische Risikoeinstufung		
	Modellierung des Datenflusses		
	Risikobewertung der Integration		
Intelligente Datensicherung	Adaptives DLP		
	Intelligentes Verschlüsselungsmanagement		
	Entwicklung des Bewusstseins für Inhalte		
	Reduzierung von Falsch-Positiven		
	Automatisierte Vorschläge für Richtlinien		

5.7 Integrationsfähigkeiten

Tipp: Die Integrationsmöglichkeiten bestimmen, wie gut die CASB-Lösung mit Ihrer bestehenden Sicherheitsinfrastruktur zusammenarbeitet. Bevorzugen Sie Lösungen, die robuste APIs und vorgefertigte Integrationen bieten.

Anforderung	Teilanforderung	JA/NEIN	Anmerkungen
Integration von Sicherheitstools	SIEM-Integration		

	DLP-Integration		
	IAM-Integration		
	EDR/XDR-Integration		
	SOAR-Integration		
API-Fähigkeiten	Verfügbarkeit der REST-API		
	Unterstützung für benutzerdefinierte Integration		
	Webhook-Unterstützung		
	Authentifizierungsmethoden		
	API-Dokumentation		

6. Nicht-funktionale Anforderungen

6.1 Leistungsanforderungen

1. Systemleistung
    - Maximale Latenzzeit von 50 ms für Inline-Operationen
    - Mindestdurchsatz von 10 Gbps
    - Unterstützung für mehr als 100.000 gleichzeitige Benutzer
    - Richtliniendurchsetzung in Echtzeit
    - 99,99% Betriebszeit-Garantie
2. Skalierbarkeit
    - Horizontale Skalierbarkeit
    - Automatischer Lastausgleich
    - Dynamische Ressourcenzuweisung
    - Unterstützung mehrerer Regionen

- Elastisches Kapazitätsmanagement

3. Verfügbarkeit
    - Architektur für hohe Verfügbarkeit
    - Automatisierte Ausfallsicherung
    - Disaster Recovery-Funktionen
    - Geografische Redundanz
    - Kein einzelner Fehlerpunkt

6.2 Sicherheitsanforderungen

1. Datensicherheit
    - AES-256-Verschlüsselung für Daten im Ruhezustand
    - TLS 1.3 für Daten bei der Übertragung
    - FIPS 140-2-Konformität
    - Sichere Schlüsselverwaltung
    - Einhaltung der Datenhoheit
2. Zugangssicherheit
    - Rollenbasierte Zugriffskontrolle
    - Multi-Faktor-Authentifizierung
    - Verwaltung des privilegierten Zugangs
    - Sitzungsmanagement
    - Protokollierung der Zugangsprüfung
3. Einhaltung der Vorschriften
    - SOC 2 Typ II-Zertifizierung
    - ISO 27001-Zertifizierung
    - Einhaltung der GDPR

- Einhaltung des HIPAA
- PCI DSS-Konformität

7. Anforderungen an die Umsetzung

7.1 Projekt-Phasen

1. Planungsphase (4-6 Wochen)
    - Sammlung von Anforderungen
    - Architekturentwurf
    - Planung der Integration
    - Zuweisung von Ressourcen
    - Entwicklung der Zeitachse
2. Einführungsphase (8-12 Wochen)
    - Ersteinrichtung
    - Kern-Konfiguration
    - Umsetzung der Integration
    - Entwicklung der Politik
    - Prüfung und Validierung
3. Optimierungsphase (4-6 Wochen)
    - Leistungsoptimierung
    - Verfeinerung der Politik
    - Benutzerakzeptanztests
    - Fertigstellung der Dokumentation
    - Wissenstransfer

7.2 Implementierungsdienste

1. Professionelle Dienstleistungen

- Architekturberatung
- Unterstützung bei der Bereitstellung
- Unterstützung der Integration
- Entwicklung der Politik
- Optimierung der Leistung

2. Ausbildungsdienste
    - Ausbildung zum Administrator
    - Schulung des Sicherheitsteams
    - Schulung der Endbenutzer
    - Benutzerdefinierte Dokumentation
    - Zugang zur Wissensdatenbank

8. Operative Anforderungen

8.1 Unterstützungsdienste

1. Technische Unterstützung
    - 24/7-Support-Verfügbarkeit
    - Maximal 1 Stunde Reaktionszeit für kritische Probleme
    - Multi-Channel-Support-Optionen
    - Engagiertes Unterstützungsteam
    - Regelmäßige Dienstüberprüfungen
2. Wartung
    - Regelmäßige Updates und Patches
    - Geplante Wartungsfenster
    - Prozess des Änderungsmanagements
    - Versionskontrolle

- Rollback-Funktionen

3. Überwachung
    - Systemüberwachung in Echtzeit
    - Verfolgung von Leistungskennzahlen
    - Kapazitätsplanung
    - Trendanalyse
    - Proaktive Problemerkennung

9. Qualifikationen des Anbieters

9.1 Unternehmensprofil

1. Marktposition
    - Mindestens 5 Jahre auf dem CASB-Markt
    - Anerkannter Branchenführer
    - Starke finanzielle Stabilität
    - Globale Präsenz
    - Nachgewiesene Erfolgsbilanz
2. Kundenstamm
    - Referenzen von Unternehmenskunden
    - Branchenspezifische Erfahrung
    - Ähnliche Umsetzungen
    - Metriken zur Kundenzufriedenheit
    - Fallstudien

9.2 Technisches Fachwissen

1. Produktentwicklung
    - Engagiertes F&E-Team

- Regelmäßiger Veröffentlichungszyklus
- Erfolgsbilanz der Innovation
- Technologie-Partnerschaften
- Produkt-Fahrplan

2. Unterstützungskapazitäten
    - Globale Support-Präsenz
    - Technisches Fachwissen
    - Erfahrung mit der Umsetzung
    - Ausbildungsmöglichkeiten
    - Verfügbarkeit von Ressourcen

10. Kriterien für die Bewertung

10.1 Technische Bewertung (40%)

1. Vollständigkeit der Merkmale
    - Abdeckung der Kernfunktionen
    - Verfügbarkeit erweiterter Funktionen
    - Integrationsfähigkeit
    - Optionen zur Skalierbarkeit
    - Leistungsmetriken
2. Architektur
    - Grundsätze der Gestaltung
    - Skalierbarkeit
    - Verlässlichkeit
    - Sicherheit
    - Innovation

10.2 Bewertung des Anbieters (30%)

1. Stabilität des Unternehmens
    - Finanzielle Gesundheit
    - Marktstellung
    - Wachstumskurve
    - Kundenstamm
    - Anerkennung durch die Industrie
2. Unterstützungskapazitäten
    - Globale Präsenz
    - Technisches Fachwissen
    - Reaktionszeiten
    - Verfügbarkeit von Ressourcen
    - Ausbildungsprogramme

10.3 Kostenbewertung (30%)

1. Gesamtbetriebskosten
    - Lizenzkosten
    - Kosten der Durchführung
    - Instandhaltungskosten
    - Kosten der Unterstützung
    - Ausbildungskosten

11. Leitlinien für die Einreichung

11.1 Anforderungen an den Vorschlag

1. Technischer Vorschlag
    - Überblick über die Lösung

- Technische Daten
- Ansatz für die Umsetzung
- Modell unterstützen
- Beispiele für Leistungen

2. Kommerzieller Vorschlag
    - Struktur der Preisgestaltung
    - Zahlungsbedingungen
    - Service Level Agreements
    - Zusätzliche Dienstleistungen
    - Optionale Merkmale

11.2 Format der Einreichung

- Elektronische Einreichung erforderlich
- PDF-Format
- Maximal 100 Seiten
- Zusammenfassung erforderlich
- Unterstützende Dokumentation als Anhänge

12. Zeitleiste

- RFP-Freigabedatum: [Datum]
- Einsendeschluss: [Datum]
- Fälligkeitsdatum des Vorschlags: [Datum]
- Präsentationen des Anbieters: [Datumsbereich]
- Datum der Auswahl: [Datum]
- Datum des Projektbeginns: [Datum]

13. Total Cost of Ownership

13.1 Direkte Kosten

1. Software-Lizenzierung
    - Pro-Benutzer-Lizenzgebühren
    - Modulbezogene Kosten
    - Zusätzliche Kosten für das Merkmal
    - Mengenrabatte
    - Laufzeitverpflichtungen
2. Kosten der Durchführung
    - Professionelle Dienstleistungen
    - Integrationsdienste
    - Kosten für die Anpassung
    - Ausbildungskosten
    - Projektleitung

13.2 Indirekte Kosten

1. Operative Kosten
    - Interne Ressourcenzuweisung
    - Anforderungen an die Infrastruktur
    - Laufende Wartung
    - Regelmäßige Aktualisierungen
    - Unterstützung von Verlängerungen
2. Zusätzliche Überlegungen
    - Auswirkungen auf die Leistung
    - Auswirkungen auf die Produktivität
    - Anforderungen an die Ausbildung

- Prozessänderungen
- Pflege der Integration

14. Künftige Überlegungen

14.1 Technologische Trends

1. Aufkommende Technologien
    - Zero Trust-Integration
    - SASE-Konvergenz
    - Unterstützung von Edge Computing
    - Bereitschaft zum Quantencomputing
    - 5G-Sicherheitsfunktionen
2. Marktentwicklung
    - Konsolidierung von Anbietern
    - Standardisierung von Merkmalen
    - Änderungen des Preismodells
    - Integrationsstandards
    - Regulatorische Anforderungen

14.2 Erfolgsmetriken

1. Sicherheitsmetriken
    - Erkennungsrate der Bedrohung
    - Zeit für die Lösung von Richtlinienverstößen
    - Entdeckung der Schatten-IT
    - Wirksamkeit des Datenschutzes
    - Effizienz der Zugangskontrolle
2. Operative Metriken

- Betriebszeit des Systems
- Reaktionszeit
- Problemlösungszeit
- Zufriedenheit der Nutzer
- Kosteneinsparungen

15. Kontaktinformationen

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