Solicitud de Propuesta: Solución de Software de Broker de Seguridad de Acceso a la Nube (CASB)

Índice

1. Introducción y Antecedentes

Nuestra organización está buscando propuestas para una solución integral de Broker de Seguridad de Acceso a la Nube (CASB) para mejorar nuestra postura de seguridad en la nube y garantizar la protección de nuestros recursos basados en la nube. La solución CASB seleccionada servirá como un punto crítico de control de seguridad entre nuestros consumidores de servicios en la nube y los proveedores de servicios en la nube.

1.1 Contexto del Mercado

- El mercado CASB está creciendo a una TCAC de aproximadamente 17.6% (2021-2026)
- Los costos de implementación típicamente varían entre $15,000 y $100,000+ anualmente
- La solución debe alinearse con las capacidades de los líderes actuales del mercado mientras proporciona características innovadoras

1.2 Expectativas de Valor Comercial

- Mejora de la postura de seguridad en la nube a través del control unificado
- Mayor visibilidad en el uso de servicios en la nube
- Fortalecimiento de las capacidades de cumplimiento normativo
- Mitigación significativa de riesgos para las operaciones en la nube
- Costos optimizados a través del uso controlado de la nube

2. Objetivos del Proyecto

2.1 Objetivos Principales

1. Implementar una solución CASB integral que proporcione visibilidad y control sobre los servicios en la nube
2. Implementar medidas robustas de protección de datos para la información alojada en la nube
3. Establecer capacidades de monitoreo en tiempo real y detección de amenazas
4. Permitir la gestión granular de políticas en todos los servicios en la nube
5. Asegurar el cumplimiento de los requisitos regulatorios
6. Optimizar el uso de servicios en la nube y los costos asociados

2.2 Metas Estratégicas

1. Reducir los incidentes de seguridad relacionados con el uso de servicios en la nube en un 75%
2. Lograr una visibilidad del 100% en el uso de aplicaciones en la nube

3. Establecer la aplicación automatizada de políticas en todos los servicios en la nube
4. Implementar medidas consistentes de protección de datos en todas las plataformas en la nube
5. Habilitar la detección y respuesta proactiva a amenazas
6. Optimizar las operaciones de seguridad a través de la automatización

3. Alcance del Trabajo

3.1 Requisitos de Arquitectura Técnica

1. Modelos de Implementación
    - Capacidad de implementación de proxy directo
    - Opción de implementación de proxy inverso
    - Conectividad basada en API para servicios en la nube
    - Flexibilidad de implementación multi-modo
    - Soporte para arquitectura híbrida
2. Puntos de Integración
    - Sistemas de Gestión de Identidad y Acceso (IAM)
    - Gestión de Información y Eventos de Seguridad (SIEM)
    - Sistemas de Prevención de Pérdida de Datos (DLP)
    - Gestión de Movilidad Empresarial (EMM)
    - Orquestación y Respuesta de Seguridad (SOAR)
    - Infraestructura de seguridad existente
3. Componentes Principales
    - Puerta de Enlace de Seguridad en la Nube
    - Motor de Políticas

- Módulo de Protección de Datos
- Sistema de Prevención de Amenazas
- Motor de Análisis
- Consola de Gestión

4. Requisitos Técnicos

4.1 Arquitectura e Infraestructura

1. Flexibilidad de Implementación
    - Soporte para implementación en la nube
    - Capacidad de implementación en sitio
    - Opciones de implementación híbrida
    - Arquitectura multi-inquilino
    - Configuración de alta disponibilidad
2. Especificaciones de Rendimiento
    - Latencia máxima: 50ms para operaciones en línea
    - Rendimiento mínimo: 10Gbps
    - Soporte para más de 100,000 usuarios concurrentes
    - Garantía de disponibilidad del 99.99%
    - Aplicación de políticas en tiempo real
3. Arquitectura de Seguridad
    - Cifrado de extremo a extremo (TLS 1.3)
    - Soporte para Módulo de Seguridad de Hardware (HSM)
    - Gestión segura de claves
    - Gestión del ciclo de vida de certificados
    - Capacidades de fortalecimiento de seguridad

5. Requisitos Funcionales

5.1 Gestión de Usuarios y Accesos

Consejo: La gestión robusta de usuarios y accesos es fundamental para la seguridad en la nube. Asegure que la solución proporcione métodos de autenticación integrales, controles de acceso granulares y monitoreo detallado de actividades para mantener la seguridad mientras se permite la productividad.

Requisito	Sub-Requisito	S/N	Notas
Autenticación de Usuarios	Soporte para autenticación multifactor		
	Integración con soluciones SSO empresariales		
	Autenticación escalonada para operaciones sensibles		
	Controles de gestión y tiempo de sesión		
	Opciones de autenticación basada en dispositivos		
Control de Acceso	Control de acceso basado en roles		
	Control de acceso basado en atributos		
	Restricciones de acceso basadas en ubicación		
	Políticas de acceso basadas en tiempo		
	Verificación de postura del dispositivo		
Monitoreo de Actividad de Usuarios	Registro de actividad en tiempo real		
	Grabación de sesiones de usuario		
	Seguimiento de acceso a archivos		

	Registro de cambios de configuración		
	Auditoría de actividad administrativa		

5.2 Protección de Datos

Consejo: Las capacidades de protección de datos integrales deben cubrir todo el ciclo de vida de los datos en entornos en la nube. Enfóquese en soluciones que proporcionen visibilidad profunda del movimiento de datos, controles robustos y opciones flexibles de cifrado.

Requisito	Sub-Requisito	S/N	Notas
Descubrimiento de Datos	Descubrimiento automatizado de datos sensibles		
	Reconocimiento de patrones de datos personalizados		
	Escaneo de datos estructurados y no estructurados		
	Monitoreo de conexiones a bases de datos		
	Clasificación de datos en tiempo real		
Prevención de Pérdida de Datos	Reglas de inspección de contenido		
	Controles de tipo de archivo		
	Capacidades de marca de agua		
	Prevención de capturas de pantalla		
	Controles de copiar/pegar		
Gestión de Cifrado	Gestión de claves		
	Gestión del ciclo de vida de certificados		

	Aplicación de políticas de cifrado		
	Tokenización de datos		
	Cifrado con preservación de formato		

5.3 Control de Aplicaciones en la Nube

Consejo: El control de aplicaciones en la nube es crucial para mantener la seguridad en entornos cloud. Enfóquese en capacidades que proporcionen visibilidad integral del uso de aplicaciones en la nube, evaluación de riesgos y control granular sobre el acceso y el intercambio de datos.

Requisito	Sub-Requisito	S/N	Notas
Descubrimiento de Aplicaciones	Descubrimiento automático de aplicaciones		
	Puntuación de evaluación de riesgos		
	Análisis de patrones de uso		
	Detección de TI en la sombra		
	Categorización de aplicaciones		
Gestión de Aplicaciones	Gestión de listas blancas/negras		
	Políticas de acceso a aplicaciones		
	Control de acceso API		
	Integración de aplicaciones de terceros		
	Incorporación de aplicaciones personalizadas		

5.4 Protección contra Amenazas

Consejo: La protección moderna contra amenazas requiere mecanismos de defensa multicapa que puedan detectar y responder tanto a amenazas conocidas como desconocidas. Evalúe las soluciones según su capacidad para

proporcionar protección en tiempo real, análisis avanzado y capacidades de respuesta automatizada.

Requisito	Sub-Requisito	S/N	Notas
Detección de Amenazas	Escaneo de malware		
	Protección contra ransomware		
	Detección de anomalías		
	Protección contra amenazas persistentes avanzadas (APT)		
	Detección de amenazas día cero		
Análisis de Seguridad	Análisis conductual		
	Puntuación de riesgos		
	Integración de inteligencia de amenazas		
	Reconocimiento de patrones		
	Análisis predictivo		

5.5 Gestión de Políticas

Consejo: La gestión eficaz de políticas es la base de la implementación de CASB. Busque soluciones que ofrezcan creación flexible de políticas, controles granulares y capacidades de aplicación automatizada.

Requisito	Sub-Requisito	S/N	Notas
Creación de Políticas	Creación de políticas basada en plantillas		
	Constructor de políticas personalizadas		
	Herencia de políticas		

	Control de versiones		
	Entorno de prueba de políticas		
Aplicación de Políticas	Aplicación de políticas en tiempo real		
	Acciones de remediación automatizadas		
	Alertas de violación de políticas		
	Gestión de excepciones		
	Controles granulares de políticas		

5.6 Capacidades de IA y Aprendizaje Automático

Consejo: Las capacidades avanzadas de IA y ML deben proporcionar beneficios prácticos de seguridad mientras mantienen la transparencia en la toma de decisiones. Enfóquese en soluciones que ofrezcan IA explicable y mejoras de seguridad demostrables.

Requisito	Sub-Requisito	S/N	Notas
Detección de Amenazas Potenciada por IA	Reconocimiento adaptativo de patrones de amenazas		
	Análisis predictivo de amenazas		
	Procesamiento de lenguaje natural para clasificación de datos		
	Identificación de patrones de ataques día cero		
	Correlación de ataques multi-vector		
Análisis de Comportamiento de Usuario Mejorado por IA	Análisis inteligente de sesiones		
	Mapeo de relaciones entre entidades		

	Adaptación de línea base conductual		
	Detección y correlación de anomalías		
Respuesta y Remediación Autónoma	Remediación autoaprendizaje		
	Automatización inteligente de políticas		
	Optimización de respuesta automatizada		
	Adaptación de políticas contextual		
	Optimización de políticas basada en riesgos		
Inteligencia de Aplicaciones en la Nube basada en IA	Aprendizaje de comportamiento de aplicaciones		
	Evaluación inteligente de riesgos de apps		
	Puntuación dinámica de riesgos		
	Modelado de flujo de datos		
	Evaluación de riesgos de integración		
Protección Inteligente de Datos	DLP adaptativo		
	Gestión inteligente de cifrado		
	Evolución de conciencia de contenido		
	Reducción de falsos positivos		

	Sugerencia automatizada de políticas		

5.7 Capacidades de Integración

Consejo: Las capacidades de integración determinan qué tan bien funcionará la solución CASB con su infraestructura de seguridad existente. Priorice soluciones que ofrezcan APIs robustas e integraciones preconfiguradas.

Requisito	Sub-Requisito	S/N	Notas
Integración de Herramientas de Seguridad	Integración con SIEM		
	Integración con DLP		
	Integración con IAM		
	Integración con EDR/XDR		
	Integración con SOAR		
Capacidades de API	Disponibilidad de API REST		
	Soporte de integración personalizada		
	Soporte de webhook		
	Métodos de autenticación		
	Documentación de API		

6. Requisitos No Funcionales

6.1 Requisitos de Rendimiento

1. Rendimiento del Sistema
    - Latencia máxima de 50ms para operaciones en línea
    - Rendimiento mínimo de 10 Gbps
    - Soporte para más de 100,000 usuarios concurrentes

- Aplicación de políticas en tiempo real
- Garantía de disponibilidad del 99.99%

2. Escalabilidad
    - Capacidad de escalado horizontal
    - Equilibrio de carga automático
    - Asignación dinámica de recursos
    - Soporte multi-región
    - Gestión de capacidad elástica
3. Disponibilidad
    - Arquitectura de alta disponibilidad
    - Conmutación por error automatizada
    - Capacidades de recuperación ante desastres
    - Redundancia geográfica
    - Sin puntos únicos de fallo

6.2 Requisitos de Seguridad

1. Seguridad de Datos
    - Cifrado AES-256 para datos en reposo
    - TLS 1.3 para datos en tránsito
    - Cumplimiento FIPS 140-2
    - Gestión segura de claves
    - Cumplimiento de soberanía de datos
2. Seguridad de Acceso
    - Control de acceso basado en roles
    - Autenticación multifactor

- Gestión de acceso privilegiado
- Gestión de sesiones
- Registro de auditoría de accesos

3. Cumplimiento
    - Certificación SOC 2 Tipo II
    - Certificación ISO 27001
    - Cumplimiento GDPR
    - Cumplimiento HIPAA
    - Cumplimiento PCI DSS

7. Requisitos de Implementación

7.1 Fases del Proyecto

1. Fase de Planificación (4-6 semanas)
    - Recopilación de requisitos
    - Diseño de arquitectura
    - Planificación de integración
    - Asignación de recursos
    - Desarrollo del cronograma
2. Fase de Despliegue (8-12 semanas)
    - Configuración inicial
    - Configuración principal
    - Implementación de integraciones
    - Desarrollo de políticas
    - Pruebas y validación
3. Fase de Optimización (4-6 semanas)

- Ajuste de rendimiento
- Refinamiento de políticas
- Pruebas de aceptación de usuario
- Finalización de documentación
- Transferencia de conocimiento

7.2 Servicios de Implementación

1. Servicios Profesionales
    - Consultoría de arquitectura
    - Asistencia en el despliegue
    - Soporte de integración
    - Desarrollo de políticas
    - Optimización de rendimiento
2. Servicios de Capacitación
    - Capacitación de administradores
    - Capacitación del equipo de seguridad
    - Capacitación de usuarios finales
    - Documentación personalizada
    - Acceso a base de conocimiento

8. Requisitos Operativos

8.1 Servicios de Soporte

1. Soporte Técnico
    - Disponibilidad de soporte 24/7
    - Tiempo máximo de respuesta de 1 hora para problemas críticos
    - Opciones de soporte multicanal

- Equipo de soporte dedicado
- Revisiones regulares del servicio

2. Mantenimiento
    - Actualizaciones y parches regulares
    - Ventanas de mantenimiento programadas
    - Proceso de gestión de cambios
    - Control de versiones
    - Capacidades de reversión
3. Monitoreo
    - Monitoreo del sistema en tiempo real
    - Seguimiento de métricas de rendimiento
    - Planificación de capacidad
    - Análisis de tendencias
    - Detección proactiva de problemas

9. Calificaciones del Proveedor

9.1 Perfil de la Empresa

1. Posición en el Mercado
    - Mínimo 5 años en el mercado CASB
    - Líder reconocido de la industria
    - Fuerte estabilidad financiera
    - Presencia global
    - Historial comprobado
2. Base de Clientes
    - Referencias de clientes empresariales

- Experiencia específica en la industria
- Implementaciones de escala similar
- Métricas de satisfacción del cliente
- Casos de estudio

9.2 Experiencia Técnica

1. Desarrollo de Productos
    - Equipo dedicado de I+D
    - Ciclo regular de lanzamientos
    - Historial de innovación
    - Asociaciones tecnológicas
    - Hoja de ruta del producto
2. Capacidades de Soporte
    - Presencia global de soporte
    - Experiencia técnica
    - Experiencia en implementación
    - Capacidades de formación
    - Disponibilidad de recursos

10. Criterios de Evaluación

10.1 Evaluación Técnica (40%)

1. Completitud de Funcionalidades
    - Cobertura de funcionalidad central
    - Disponibilidad de funciones avanzadas
    - Capacidades de integración
    - Opciones de escalabilidad

- Métricas de rendimiento

2. Arquitectura
    - Principios de diseño
    - Escalabilidad
    - Fiabilidad
    - Seguridad
    - Innovación

10.2 Evaluación del Proveedor (30%)

1. Estabilidad de la Empresa
    - Salud financiera
    - Posición en el mercado
    - Trayectoria de crecimiento
    - Base de clientes
    - Reconocimiento en la industria
2. Capacidades de Soporte
    - Presencia global
    - Experiencia técnica
    - Tiempos de respuesta
    - Disponibilidad de recursos
    - Programas de formación

10.3 Evaluación de Costos (30%)

1. Costo Total de Propiedad
    - Costos de licencias
    - Costos de implementación

- Costos de mantenimiento
- Costos de soporte
- Costos de formación

11. Pautas de Presentación

11.1 Requisitos de la Propuesta

1. Propuesta Técnica
    - Visión general de la solución
    - Especificaciones técnicas
    - Enfoque de implementación
    - Modelo de soporte
    - Entregables de muestra
2. Propuesta Comercial
    - Estructura de precios
    - Términos de pago
    - Acuerdos de nivel de servicio
    - Servicios adicionales
    - Características opcionales

11.2 Formato de Presentación

- Presentación electrónica requerida
- Formato PDF
- Máximo 100 páginas
- Resumen ejecutivo requerido
- Documentación de respaldo como anexos

12. Cronograma

- Fecha de Publicación de la RFP: [Fecha]
- Fecha Límite para Preguntas: [Fecha]
- Fecha de Entrega de la Propuesta: [Fecha]
- Presentaciones de Proveedores: [Rango de Fechas]
- Fecha de Selección: [Fecha]
- Fecha de Inicio del Proyecto: [Fecha]

13. Costo Total de Propiedad

13.1 Costos Directos

1. Licenciamiento de Software
    - Tarifas de licencia por usuario
    - Costos basados en módulos
    - Costos de características adicionales
    - Descuentos por volumen
    - Compromisos de plazo
2. Costos de Implementación
    - Servicios profesionales
    - Servicios de integración
    - Costos de personalización
    - Gastos de capacitación
    - Gestión de proyectos

13.2 Costos Indirectos

1. Costos Operativos
    - Asignación de recursos internos
    - Requisitos de infraestructura

- Mantenimiento continuo
- Actualizaciones regulares
- Renovaciones de soporte

2. Consideraciones Adicionales
    - Impacto en el rendimiento
    - Efectos en la productividad
    - Requisitos de capacitación
    - Cambios en los procesos
    - Mantenimiento de integraciones

14. Consideraciones Futuras

14.1 Tendencias Tecnológicas

1. Tecnologías Emergentes
    - Integración de Confianza Cero
    - Convergencia SASE
    - Soporte para computación en el borde
    - Preparación para computación cuántica
    - Capacidades de seguridad 5G
2. Evolución del Mercado
    - Consolidación de proveedores
    - Estandarización de características
    - Cambios en el modelo de precios
    - Estándares de integración
    - Requisitos regulatorios

14.2 Métricas de Éxito

1. Métricas de Seguridad
    - Tasa de detección de amenazas
    - Tiempo de resolución de violaciones de políticas
    - Descubrimiento de TI en la sombra
    - Efectividad de la protección de datos
    - Eficiencia del control de acceso
2. Métricas Operativas
    - Tiempo de actividad del sistema
    - Tiempo de respuesta
    - Tiempo de resolución de problemas
    - Satisfacción del usuario
    - Ahorro de costos

15. Información de Contacto

Por favor, envíe propuestas y preguntas a:

- Nombre del Contacto: [Nombre]
- Correo Electrónico: [Email]
- Número de Teléfono: [Teléfono]