Documento de especificaciones del producto

# Contoso CipherGuard Sentinel X7

# 1. Información general del producto

## 1.1 Introducción

Contoso CipherGuard Sentinel X7 es un producto de seguridad avanzado y resistente diseñado cuidadosamente para fortalecer la infraestructura de red informática frente a un espectro de amenazas y vulnerabilidades. Este documento profundiza en las especificaciones técnicas, características y funcionalidades de Contoso CipherGuard Sentinel X7.

## 1.2 Características principales

* **Protección de firewall:** al usar un firewall de inspección con estado, Contoso CipherGuard Sentinel X7 emplea técnicas de inspección profunda de paquetes. Inspecciona y analiza paquetes de red en la capa de aplicación y ofrece un control detallado de los flujos de datos. El firewall adapta su conjunto de reglas de forma dinámica según el contexto de red en evolución y mitiga los riesgos asociados a los ataques en la capa de aplicación.
* **Sistema de detección y prevención de intrusiones (IDPS):** con tecnología de algoritmos de aprendizaje automático, nuestro IDPS supervisa continuamente las anomalías y los patrones de tráfico de red. Saca provecho de la detección basada en firmas, la detección de anomalías y el análisis heurístico para identificar e impedir amenazas potenciales. El sistema utiliza fuentes de inteligencia sobre amenazas y garantiza que se mantiene actualizado con los modelos de ataque conocidos más recientes.
* **Compatibilidad con red privada virtual (VPN):** Contoso CipherGuard Sentinel X7 admite los protocolos VPN estándar del sector, como IPsec y OpenVPN. Facilita una comunicación segura en redes públicas al cifrar los datos en tránsito. El módulo VPN utiliza algoritmos criptográficos avanzados, como AES-256, lo que garantiza un canal de comunicación sólido y seguro para los usuarios remotos y sucursales.
* **Seguridad de puntos de conexión:** al usar un enfoque de defensa multicapa, nuestro módulo de seguridad de puntos de conexión incorpora funcionalidades antivirus, antimalware y de prevención de intrusiones basadas en host. Realiza análisis del comportamiento y detección heurística en tiempo real, por lo que garantiza una detección proactiva y la contención de las actividades malintencionadas. Además, se integra con plataformas de inteligencia sobre amenazas para dar una respuesta rápida a las amenazas emergentes.
* **Registro y supervisión:** el subsistema de registro y supervisión captura datos completos en las actividades de red. Incluye registros detallados de los modelos de tráfico, eventos de autenticación de usuarios y violaciones de las directivas de seguridad. Al integrarse con SIEM (Administración de eventos e información de seguridad), esta característica facilita la supervisión y análisis centralizados, lo que permite los administradores de seguridad responder con velocidad a los incidentes de seguridad potenciales.
* **Autenticación de usuario y control de acceso**: Contoso CipherGuard Sentinel X7 admite mecanismos de autenticación multifactor (MFA), incluida la autenticación biométrica y la integración de tarjetas inteligentes. Las directivas de control de acceso se basan en los roles de usuario, que sacan provecho de la integración de LDAP y Active Directory. La aplicación dinámica de directivas garantiza que solo los usuarios autorizados tengan acceso a los recursos confidenciales.

# 2. Especificaciones técnicas

## 2.1 Requisitos de hardware

* **Procesador:** cuatro núcleos de 2,5 GHz o superior con compatibilidad con aceleración de hardware
* **RAM:** mínimo 16 GB, se recomienda ECC (código de corrección de errores)
* **Almacenamiento:** mínimo 200 GB, SSD para un rendimiento óptimo
* **Tarjetas de interfaz de red (NIC):** Dual Gigabit Ethernet con compatibilidad con marcos jumbo

## 2.2 Requisitos de software

* **Sistema operativo:** compatible con Windows Server 2019 y versiones posteriores, CentOS 8 o equivalente
* **Base de datos:** PostgreSQL 13 para el almacenamiento de datos, optimizado para la indexación de alto rendimiento
* **Actualizaciones de seguridad:** actualizaciones automatizadas para fuentes de inteligencia sobre amenazas y parches periódicos de seguridad

## 2.3 Compatibilidad de red

* **Protocolos:** compatibilidad con TCP/IP, UDP, ICMP, IPv6
* **Integración:** integración perfecta con protocolos de enrutamiento BGP y OSPF
* **Compatibilidad:** interoperabilidad con Cisco, Juniper y otros proveedores principales de redes

# 3. Plan de implementación

## 3.1 Pasos de implementación

1. **Evaluación previa a la implementación:** realizar una evaluación completa de las vulnerabilidades de red, incluidas las pruebas de penetración y el análisis de riesgos.
2. **Instalación:** implementar Contoso CipherGuard Sentinel X7 en servidores dedicados o máquinas virtuales, lo que garantiza un uso óptimo del hardware y de la asignación de recursos.
3. **Configuración:** personalizar las directivas de seguridad, los controles de acceso y las reglas de firewall en función de los requisitos de la organización. Ajustar los parámetros de detección de intrusiones para la máxima precisión.
4. **Pruebas:** ejecutar un plan de pruebas exhaustivo, incluyendo escenarios de ataque simulados y pruebas de carga, para validar la eficacia y el rendimiento de la solución.
5. **Formación:** proporcionar sesiones de aprendizaje detalladas para el personal de TI, que cubran las operaciones diarias, los procedimientos de respuesta a incidentes y las tareas de mantenimiento.

## 3.2 Mantenimiento y asistencia

* **Actualizaciones periódicas:** Contoso garantiza actualizaciones continuas del producto, incorporando la inteligencia sobre amenazas y las mejoras de seguridad más recientes.
* **Soporte técnico:** Contoso proporciona un equipo de soporte técnico dedicado las 24 horas del día, los 7 días de la semana, para garantizar la asistencia rápida para cualquier consulta o problema técnico relacionado con Contoso CipherGuard Sentinel X7 .