مستند مواصفات المنتج

# Contoso CipherGuard Sentinel X7

# 1. نظرة عامة على المنتج

## 1.1 المقدمة

Contoso CipherGuard Sentinel X7 هو منتج أمان متقدم ومرن تم تصميمه بعناية لتعزيز البنية التحتية لشبكة الحاسوب ضد مجموعة من التهديدات والثغرات الأمنية. يتعمق هذا المستند في تعقيدات المواصفات الفنية والميزات والوظائف الخاصة بـ Contoso CipherGuard Sentinel X7.

## 1.2 الميزات الرئيسية

* **حماية جدار الحماية:** باستخدام جدار حماية لفحص الحالة، يستخدم Contoso CipherGuard Sentinel X7 تقنيات فحص حزم البيانات العميقة. يقوم بفحص وتحليل حزم بيانات الشبكة على مستوى طبقة التطبيق، مما يوفر تحكمًا دقيقًا في تدفقات البيانات. يقوم جدار الحماية بتكييف مجموعة القواعد الخاصة به ديناميكيًا استنادًا إلى سياق الشبكة المتطور، ما يخفف من المخاطر المرتبطة بهجمات طبقة التطبيق.
* **نظام اكتشاف التسلل والوقاية منه (IDPS):** بفضل خوارزميات التعلم الآلي، يراقب نظام اكتشاف التسلل والوقاية منه (IDPS) لدينا أنماط تدفق البيانات على الشبكة والأمور الخارجة عن المألوف بشكل مستمر. فهو يستفيد من الكشف المستند إلى التوقيع، والكشف عن الأمور الخارجة عن المألوف، والتحليل الموجّه لتحديد التهديدات المحتملة وإحباطها. يستخدم النظام موجزات التحليل الذكي للمخاطر، ما يضمن استمرار تحديثه بأحدث أنماط الهجمات المعروفة.
* **دعم الشبكة الظاهرية الخاصة (VPN):** يدعم Contoso CipherGuard Sentinel X7 بروتوكولات VPN القياسية في المجال مثل IPsec و OpenVPN. فهو يسهل الاتصال الآمن عبر الشبكات العامة عن طريق تشفير البيانات أثناء النقل. تستخدم وحدة VPN خوارزميات تشفير متقدمة، بما في ذلك AES-256، مما يضمن قناة اتصال قوية وآمنة للمستخدمين عن بعد والمكاتب الفرعية.
* **أمان نقطة النهاية:** من خلال استخدام نهج دفاعي متعدد الطبقات، تتضمن وحدة أمان نقطة النهاية لدينا قدرات مكافحة الفيروسات، ومكافحة البرامج الضارة، ومنع التسلل المستند إلى المضيف. ويُجري تحليلًا سلوكيًا في الوقت الحقيقي ومسحًا موجّهًا، مما يضمن الكشف الاستباقي واحتواء الأنشطة الضارة. بالإضافة إلى ذلك، فإنه يتكامل مع منصات التحليل الذكي للمخاطر للاستجابة السريعة للتهديدات الناشئة.
* **التسجيل والمراقبة:** يلتقط النظام الفرعي للتسجيل والمراقبة بيانات شاملة عن أنشطة الشبكة. إنه يتضمن سجلات مفصلة حول أنماط تدفق البيانات، وأحداث مصادقة المستخدم، وانتهاكات سياسة الأمان. متكامل مع SIEM (إدارة معلومات الأمان والأحداث)، تسهل هذه الميزة المراقبة والتحليل المركزيين، ما يمكن مسؤولي الأمان من الاستجابة بسرعة للحوادث الأمنية المحتملة.
* **مصادقة المستخدم والتحكم في الوصول**: يدعم Contoso CipherGuard Sentinel X7 آليات المصادقة متعددة العوامل (MFA)، بما في ذلك المصادقة البيومترية وتكامل البطاقة الذكية. تعتمد سياسات التحكم في الوصول على أدوار المستخدم، مع الاستفادة من تكامل LDAP و Active Directory. يضمن فرض السياسة الديناميكية أن المستخدمين المصرح لهم فقط هم من يمكنهم الوصول إلى الموارد الحساسة.

# 2. المواصفات الفنية

## 2.1 متطلبات الأجهزة

* **المعالج:** رباعي النواة بسرعة 2.5 GHz أو أعلى مع دعم تسريع الجهاز
* **ذاكرة الوصول العشوائي (RAM):** 16 GB كحد أدنى، يوصى باستخدام ECC (رمز تصحيح الأخطاء)
* **التخزين:** 200 GB كحد أدنى، SSD للحصول على الأداء الأمثل
* **بطاقات واجهة الشبكة (NIC):** شبكة جيجابت إيثرنت مزدوجة (Dual Gigabit Ethernet) مع دعم الإطارات الضخمة

## 2.2 متطلبات البرمجيات

* **نظام التشغيل:** متوافق مع Windows Server 2019 والإصدارات الأحدث، CentOS 8 أو ما يعادله
* **قاعدة البيانات:** PostgreSQL 13 لتخزين البيانات، مُحسَّنة للفهرسة عالية الأداء
* **تحديثات الأمان:** تحديثات تلقائية لخلاصات التحليل الذكي للمخاطر وتصحيحات الأمان المنتظمة

## 2.3 توافق الشبكة

* **البروتوكولات:** دعم TCP/IP و UDP و ICMP و IPv6
* **التكامل:** التكامل السلس مع بروتوكولات التوجيه BGP و OSPF
* **التوافق:** إمكانية التشغيل التفاعلي مع Cisco و Jniper وموردي الشبكات الرئيسيين الآخرين

# 3. خطة التنفيذ

## 3.1 خطوات النشر

1. **تقييم ما قبل النشر:** إجراء تقييم شامل للثغرات الأمنية للشبكة، بما في ذلك اختبار الاختراق وتحليل المخاطر.
2. **التثبيت:** نشر Contoso CipherGuard Sentinel X7 على خوادم مخصصة أو أجهزة ظاهرية، ما يضمن الاستخدام الأمثل للأجهزة وتخصيص الموارد.
3. **التكوين:** تخصيص نُهج الأمان وعناصر التحكم في الوصول وقواعد جدار الحماية استنادًا إلى المتطلبات التنظيمية. ضبط معلمات الكشف عن الاختراق لأقصى دقة.
4. **الاختبار:** تنفيذ خطة اختبار شاملة، بما في ذلك سيناريوهات محاكاة الهجوم واختبار حمل العمل، للتحقق من فعالية وأداء الحل.
5. **التدريب:** توفير دورات تدريبية متعمقة لموظفي تكنولوجيا المعلومات، وتغطي العمليات اليومية وإجراءات الاستجابة للحوادث ومهام الصيانة.

## 3.2 الصيانة والدعم

* **التحديثات المنتظمة:** تضمن شركة Contoso التحديثات المستمرة للمنتج، والتي تتضمن أحدث تحسينات التحليل الذكي للمخاطر والأمان.
* **الدعم الفني:** توفر Contoso فريق دعم متخصص يعمل على مدار الساعة طوال أيام الأسبوع لضمان المساعدة السريعة لأي مشكلات فنية أو استفسارات تتعلق بـ Contoso CipherGuard Sentinel X7.