製品仕様ドキュメント

# Contoso CipherGuard Sentinel X7

# 1. 製品の概要

## 1.1 概要

Contoso CipherGuard Sentinel X7 は、さまざまな脅威や脆弱性に対してコンピューター ネットワーク インフラストラクチャを強化するために細心の注意を払って設計された、高度で回復性のあるセキュリティ製品です。このドキュメントでは、Contoso CipherGuard Sentinel X7 の技術的な仕様、機能、および機能の複雑さについて説明します。

## 1.2 主な機能

* **ファイアウォールによる保護:** ステートフル検査ファイアウォールを利用する Contoso CipherGuard Sentinel X7 では、詳細なパケット検査手法が採用されています。アプリケーション レイヤーのネットワーク パケットを検査および分析し、データ フローをきめ細かく制御します。ファイアウォールは、進化するネットワーク コンテキストに基づいてルール セットを動的に調整し、アプリケーション レイヤー攻撃に関連するリスクを軽減します。
* **侵入検出および防止システム (IDPS):** 機械学習アルゴリズムによって強化された IDPS は、ネットワーク トラフィック パターンと異常を継続的に監視します。シグネチャベースの検出、異常検出、ヒューリスティック分析を活用して、潜在的な脅威を特定して阻止します。システムは脅威インテリジェンス フィードを使用し、最新の既知の攻撃パターンで更新された状態を維持します。
* **仮想プライベート ネットワーク (VPN) のサポート:** Contoso CipherGuard Sentinel X7 では、IPsec や OpenVPN などの業界標準の VPN プロトコルがサポートされています。転送中のデータを暗号化することで、パブリック ネットワーク経由のセキュリティで保護された通信を容易にします。VPN モジュールは、AES-256 を含む高度な暗号アルゴリズムを採用し、リモート ユーザーとブランチ オフィス向けの堅牢で安全な通信チャネルを保証します。
* **エンドポイントのセキュリティ:** 多層防御アプローチを採用したエンドポイント セキュリティ モジュールには、ウイルス対策、マルウェア対策、およびホストベースの侵入防止機能が組み込まれています。リアルタイムの行動分析とヒューリスティック スキャンを行い、悪意のあるアクティビティを事前に検出して封じ込めます。さらに、脅威インテリジェンス プラットフォームと統合して、新たな脅威に迅速に対応します。
* **ログ記録と監視:** ログ記録と監視サブシステムは、ネットワーク アクティビティに関する包括的なデータをキャプチャします。トラフィック パターン、ユーザー認証イベント、セキュリティ ポリシー違反に関する詳細なログが含まれています。SIEM (セキュリティ情報イベント管理) と統合されたこの機能は、一元的な監視と分析を容易にし、セキュリティ管理者が潜在的なセキュリティ インシデントに迅速に対応できるようにします。
* **ユーザー認証とアクセス制御**: Contoso CipherGuard Sentinel X7 では、生体認証やスマート カードの統合など、多要素認証 (MFA) メカニズムがサポートされています。アクセス制御ポリシーは、LDAP と Active Directory の統合を利用して、ユーザー ロールに基づいています。動的ポリシーの適用により、承認されたユーザーのみが機密性の高いリソースにアクセスできるようになります。

# 2. 技術仕様

## 2.1 ハードウェア要件

* **プロセッサ:** クアッド コア 2.5 GHz 以上 (ハードウェア アクセラレーション サポート付き)
* **RAM:** 16 GB 以上、ECC (エラー訂正コード) をお勧めします
* **ストレージ:** 200 GB 以上、最適なパフォーマンスを実現する SSD
* **ネットワーク インターフェイス カード (NIC):** ジャンボ フレームをサポートするデュアル ギガビット イーサネット

## 2.2 ソフトウェア要件

* **オペレーティング システム:** Windows Server 2019 以降、CentOS 8 以降または同等のものと互換性があります
* **データベース:** データ ストレージのための PostgreSQL 13、高パフォーマンスのインデックス作成用に最適化
* **セキュリティ更新プログラム:** 脅威インテリジェンス フィードと定期的なセキュリティ パッチの自動更新

## 2.3 ネットワークの互換性

* **プロトコル:** TCP/IP、UDP、ICMP、IPv6 のサポート
* **統合:** BGP および OSPF ルーティング プロトコルとのシームレスな統合
* **互換性:** Cisco、Juniper、およびその他の主要なネットワーク ベンダーとの相互運用性

# 3. 実装計画

## 3.1 デプロイメントの手順

1. **デプロイ前評価:** 侵入テストやリスク分析を含む包括的なネットワーク脆弱性評価を実施します。
2. **インストール:** Contoso CipherGuard Sentinel X7 を専用サーバーまたは仮想マシンにデプロイし、最適なハードウェア使用率とリソース割り当てを確保します。
3. **構成:** 組織の要件に基づいてセキュリティ ポリシー、アクセス制御、ファイアウォール規則をカスタマイズします。侵入検出パラメーターを微調整して、精度を最大限に高めます。
4. **テスト:** シミュレートされた攻撃シナリオやロード テストなど、徹底的なテスト計画を実行して、ソリューションの有効性とパフォーマンスを検証します。
5. **トレーニング:** IT 担当者向けの詳細なトレーニング セッションを提供し、日常業務、インシデント対応手順、およびメンテナンス タスクをカバーします。

## 3.2 メンテナンスとサポート

* **定期的な更新:** Contoso は、最新の脅威インテリジェンスとセキュリティの強化を組み込み、製品の継続的な更新を保証します。
* **テクニカル サポート:** Contoso は、Contoso CipherGuard Sentinel X7 に関連する技術的な問題や問い合わせに対して迅速な支援を行うために、24 時間 365 日の専用サポート チームを提供しています。