Sophos ZTNA

Zero Trust Network Access

誰でも、どこでも、どんなアプリケーションでも、安全に接続。Sophos ZTNA は、ユーザーを重要な業務アプリケーションやデータに透過的に接続し、従来のリモートアクセス VPN と比較して、より高度なセグメンテーション、セキュリティ、可視性を提供します。スタンドアロン製品として動作するだけでなく、Sophos Firewall および Intercept X と完全に統合された Synchronized Security ソリューションとしても動作します。

ゼロトラストの世界で信頼を取り戻す

Sophos ZTNA は、「何も信頼せず、すべてを検証する」というゼロトラストの原則に基づいたソリューションです。各ユーザーやデバイスは、それぞれのマイクロセグメント化された境界のように処理され、常に評価・検証されます。このため、従来の「ネットワーク上」にある場合と異なり、暗黙的な信頼とアクセス権はなくなります。信頼は付与されるのではなく、獲得するものになります。

より優れたリモートワーク環境

Sophos ZTNA を使用すると、リモートワーカーは必要なアプリケーションやデータに安全かつシームレスにアクセスできます。また、導入、登録、管理は従来の VPN よりもはるかに簡単になります。

アプリケーションのマイクロセグメント化

Sophos ZTNA は究極のマイクロセグメンテーションを提供し、アプリケーションがオンプレミス、データセンター、パブリッククラウドのいずれのインフラでホストされているかに関わらず、アプリケーションへのセキュアなアクセスを実現できます。また、状態、セキュリティポスチャ、および使用状況について、アプリケーションのアクティビティをリアルタイムで可視化できます。IP アドレス制限を使用して、Sophos ZTNA で多くの SaaS アプリケーションへのアクセスを制御して、ZTNA ゲートウェイからの接続のみを許可することもできます。

ランサムウェアや脅威の阻止

ZTNA を使用すれば、ランサムウェアやその他の脅威が、侵害されたユーザーデバイスからネットワーク全体に広がる恐れはなくなります。ユーザーとデバイスには、特定のアプリケーションに対する、明示的にポリシーで指定されたアクセス権のみがあります。これによって、VPN の重要な課題の 1つであった、暗黙的な信頼と広範にわたるネットワークアクセス権は排除されます。

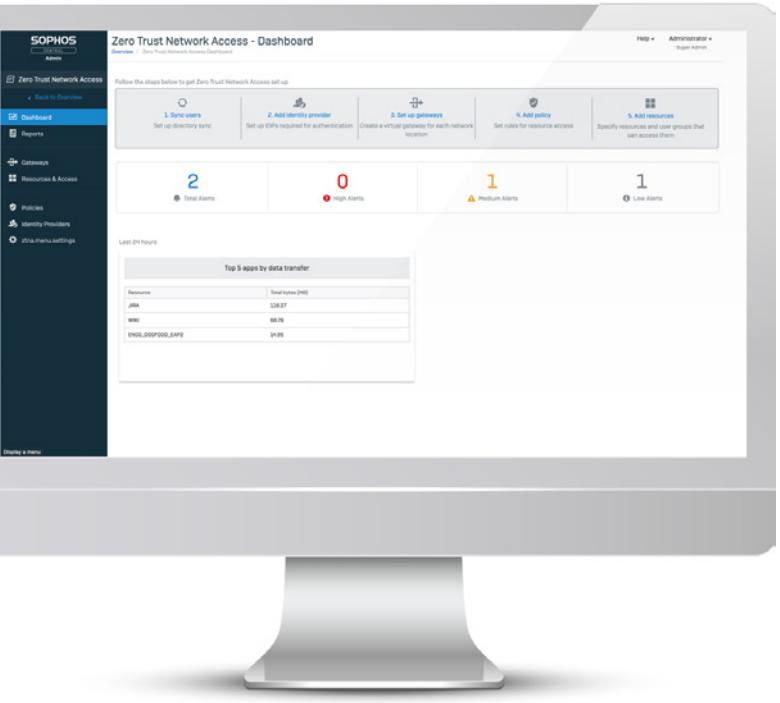
迅速な導入、適応、拡張

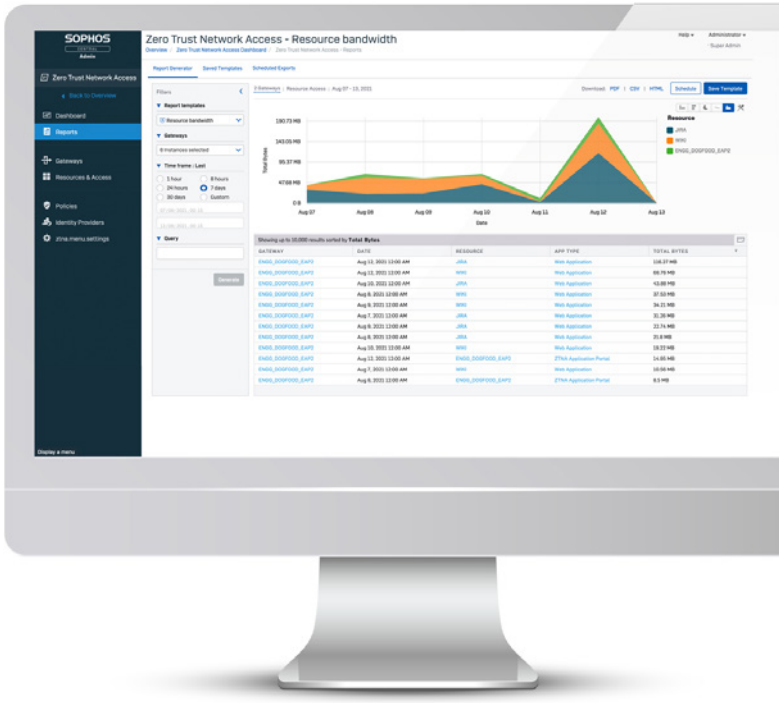
Sophos ZTNA は、動的に変化し、急速に成長し、迅速にクラウドに移行している最新のネットワーク向けに構築されています。無駄のないクリーンなソリューションで、新しいアプリケーションの安全な立ち上げ、ユーザーとデバイスの登録または使用停止、およびアプリケーションの状態や使用状況に関する重要な情報の取得を迅速かつ簡単に行うことができます。

主な特長

- ゼロトラスト：何も信頼せず、すべてを検証する
- Sophos Intercept X と統合されたエージェント
- Sophos Firewall に組み込まれたゲートウェイ
- 単一エージェント、単一ゲートウェイ、単一コンソールのソリューション
- リモートアクセス VPN に代わる究極のソリューション
- ネットワークアプリケーションをマイクロセグメント化して保護
- 場所、さらにネットワークに接続しているかどかに関わらず動作
- クラウド管理・クラウド配信型
- エンドユーザーに対して透過的
- アプリケーションの優れた可視化と洞察
- デバイスのセキュリティ状態をアクセスポリシーに統合
- よりシンプルなユーザー単位の年間サブスクリプションライセンスと、無償で導入できるゲートウェイ

SOPHOS





クラウドで提供・管理

Sophos ZTNA は、Zero Trust Network Access を簡単、統合型、安全にするために最初から設計されています。Sophos ZTNA はクラウドで提供・管理され、業界で最も信頼性の高い、サイバーセキュリティのクラウド管理およびレポートのプラットフォームである Sophos Central に統合されています。

Sophos Central では、ZTNA だけでなく、ファイアウォール、エンドポイントやサーバー保護、モバイルデバイス管理、クラウドセキュリティ、メール保護なども管理できます。いつでもどこからでも、どのデバイスからでもログオンして IT セキュリティを管理できます。

単一エージェント、単一ゲートウェイ、単一コンソール、単一ベンダー

Sophos ZTNA は、完全なソフォスのサイバーセキュリティ エコシステムと独自に統合されており、作業が大幅に簡素化されます。単一のエージェントソリューションは、ZTNA と次世代型エンドポイント保護の両方に対応します。ZTNA ゲートウェイが Sophos Firewall に統合され、単一画面の管理コンソールである Sophos Central も使用できるため、すべての IT セキュリティ製品に関するこれまでにない洞察を得ることができます。すべてが単一のベンダーから提供されます。

独自に統合：ZTNA と次世代型エンドポイント保護

Sophos ZTNA は、次世代型エンドポイント製品 (Sophos Intercept X) と緊密に統合された唯一の ZTNA ソリューションです。これによって、保護、導入、管理に大きな利点がもたらされます。

- エンドツーエンドのセキュリティ対策：業界で最も強力な機械学習と次世代型エンドポイントテクノロジーで、アプリケーションアクセスを保護し、セキュリティ侵害やランサムウェアなどの脅威から、エンドポイントとネットワークを保護します。
- Synchronized Security：ZTNA とエンドポイントは統合されているため、常にセキュリティ状態などの情報を共有し、侵害されたシステムを自動的に隔離して、データの移動や窃取を防止します。
- 単一エージェント、単一コンソール、単一ベンダーの利便性。

他社にはない優れた組み合わせです。

単一エージェントの導入

Sophos ZTNA は、Sophos Intercept X による次世代型エンドポイント保護と緊密に統合されており、単一のクライアントで導入できます。

世界最高レベルのエンドポイント保護とランサムウェア対策、ならびにアプリケーションのセキュリティとセグメント化の究極の機能をすべて他単一のクライアントで導入できます。

ブラウザベースのアプリケーションへのクライアントレスのアクセスも可能です。

スケーラブルなアプリケーションゲートウェイ

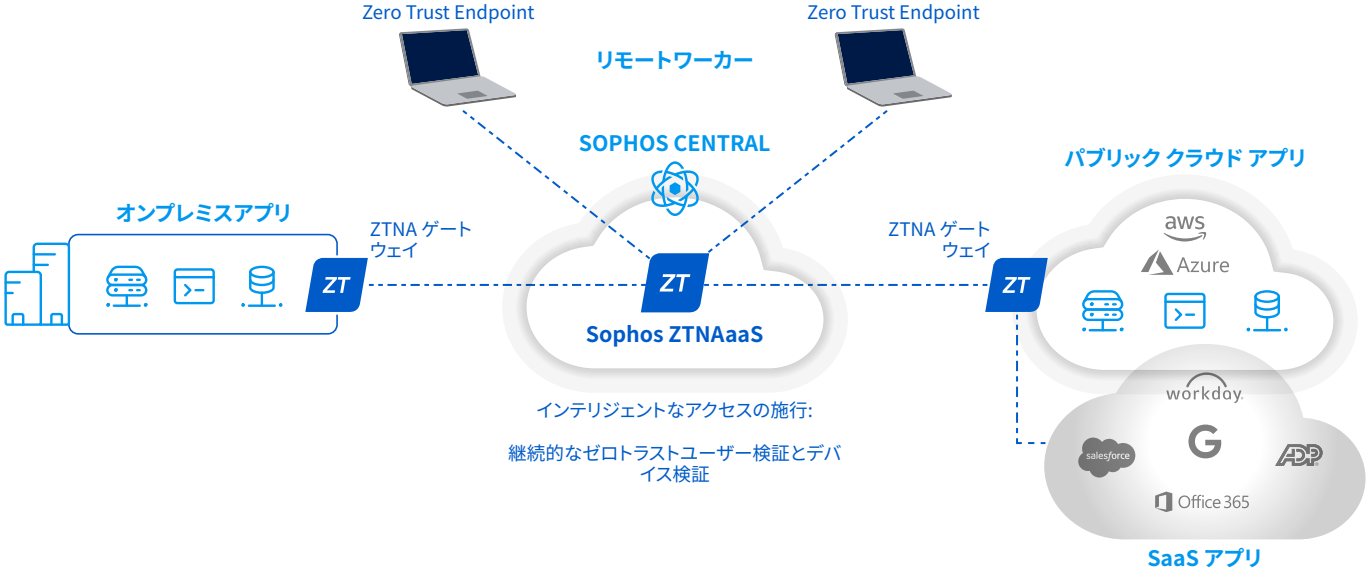
Sophos ZTNA ゲートウェイは、必要な場所に簡単かつ無償で導入できます。仮想アプライアンスとして利用でき、高可用性ゲートウェイを簡単に導入し、組織の成長に合わせて拡張できます。

デバイスのセキュリティ状態の同期

Sophos ZTNA は、Sophos Synchronized Security を最大限に活用し、Sophos Intercept X エンドポイントと Sophos Central および ZTNA の間の Security Heartbeat™ を利用して、デバイスのセキュリティ状態を評価し、アクティブな脅威と攻撃の兆候を検出します。その結果、ネットワークに接続しているかどうかに関わらず、侵害されたデバイスや準拠していないデバイスによるアクセスを迅速に制限できます。

統合された ID

ゼロトラストでは、ユーザー ID がすべてです。Sophos ZTNA は、Microsoft Azure や Okta など、最も一般的な IdP ソリューションに対応しており、ユーザー ID を常に検証しています。もちろん、このような IdP と統合するご利用中の多要素認証 (MFA) ソリューションを活用して、認証情報の窃取やデバイスの侵害から保護することもできます。



Sophos Zero Trust Endpoint

エージェントレスで実行するか、Sophos Intercept X と統合された独自の軽量 Sophos ZTNA エージェントを使用して、Synchronized Security による究極のゼロトラスト エンドポイント ソリューションを提供します。Sophos ZTNA は、必要に応じて、既存のエンドポイント保護製品とも連携できます。

Sophos Central

ZTNA as a Service は、迅速な導入、詳細なポリシー制御、クラウドからの洞察に富んだ可視性とレポート機能により、簡単に利用することができます。一般的な ID プロバイダーと統合して、継続的なユーザー認証とデバイスの検証を通じて、アプリケーションに対するインテリジェントなアクセスの実施を可能にします。

Sophos ZTNA ゲートウェイ

ハードウェア、仮想、クラウド (AWS と Azure) を含むすべての Sophos Firewall v20 以降に統合され、Hyper-V や VMware 上のスタンドアロン仮想アプライアンスとしても利用できます。Sophos ZTNA ゲートウェイは、簡単かつ無償で導入できます。これにより、アプリケーションを公共のインターネットから見えなくなると同時に、認証されたユーザーや検証済みのデバイスに、業務に必要なアプリケーションへの安全な接続を提供することができます。

Sophos ZTNA 機能の概要

- セキュアなアクセス：オンプレミスまたはパブリッククラウドなどのインフラでホストされている業務アプリケーションへの安全なアクセス
- アプリケーション：ブラウザベースの Web アプリすべてには、クライアントレスでアクセス。SSH、VNC、RDP などのシックアプリには、ZTNA クライアントを介したアクセス
- アクセスポリシー：ユーザーグループベースのポリシーや、Synchronized Security のセキュリティ状態を基にしたアクセスポリシー
- アプリケーションの状態、アクセス、使用状況を、Sophos Central を使用してレポート、監視、ログ、監査
- エンドユーザーがブックマークしたアプリケーションにアクセスするためのユーザーポータル

技術仕様

対応プラットフォーム	
IdP (Identity Provider)	Microsoft Azure および Okta
ZTNA ゲートウェイのプラットフォーム	VMware ESXi 6.5+、Hyper-V 2016+、および Sophos Firewall v20+ (AWS や Azure を含むすべてのハードウェア、仮想、およびクラウドプラットフォーム)
ZTNA クライアントのプラットフォーム	Windows 10 1803 以降、macOS 11 (Big Sur) 以降；すべてのプラットフォームでエージェントレス Web アプリケーションアクセスがサポートされています
ZTNA デバイスのセキュリティ状態	Sophos Security Heartbeat (Intercept X)

ゲートウェイの仕様	
推奨 VM	2コア / 4GB
複数ノードクラスタリング	パフォーマンス、容量、事業継続のために、最大 9 ノードで負荷分散
ノードの容量と拡張性	1つのノードに 10,000 エージェントコネクション、1つのクラスタに最大 90,000 エージェントコネクション (最大 9 ノード)

購入方法

Sophos ZTNA は、ユーザー単位の年間サブスクリプションでライセンスされています。ZTNA ゲートウェイは、必要な数だけ無償で導入できます。

詳細はこちら
sophos.com/ztna

ソフォス株式会社営業部
Email: sales@sophos.co.jp

© Copyright 2024.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK.
Sophos は、Sophos Ltd の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

24-02-26 DS-JA (NP)