VMware Workspace ONE Trust Network

進化するデジタルワークスペースに最適なセキュリティ

概要

VMware Workspace ONE™ Trust Network™ は、従業員、アプリケーション、エンドポイント、ネットワークを保護するための、最新の包括的なエンタープライズ セキュリティ アプローチを提供します。今日の脅威からの保護、検出、修正を実現する機能を備えており、インテリジェンスベースの Workspace ONE プラットフォームに組み込まれているセキュリティ機能を、パートナー ソリューションのエコシステムと連携させ、より強化することで、継続的なリスクの監視と迅速な問題の修正が可能です。

主なメリット

Workspace ONE Trust Network は、信頼と検証のフレームワークを活用し、セキュリティと管理を簡素化できるほか、次のようなメリットを実現できます。

- アクションベースのフレームワークから、デジタルワークスペース全体を統合的に可視化することで、セキュリティ ソリューションのサイロを解消し、複雑さを低減
- アクセス、デバイス、アプリケーションのセキュリティ / 管理と、インサイトおよびオートメーションを独自の方法で組み合わせ、エンド ユーザー コンピューティング エコシステム全体のリスクを低減
- オープンかつ信頼性の高いパートナー エコシステムにより、既存の投資を引き続き活用することでコスト削減をサポート

セキュリティ：今日のデジタルワークスペース戦略における最も深刻な課題

デジタルワークスペースで、任意のデバイスからアプリケーションやデータに簡単かつセキュアにアクセスできるようにすることで、従業員の生産性を約 5 倍向上させることが可能です[1]。多くの企業でデジタル トランスフォーメーションへの移行に向けた継続的な取り組みをはじめ、BYOD や IT のコンシューマライゼーションが進む中、従業員、アプリケーション、エンドポイント、ネットワークからなるデジタルワークスペースのエコシステムも従来の境界を越えて発展し、進化を続けています。また、既存の境界の消滅に伴い、ゼロデイ攻撃、中間者攻撃（MITM）攻撃、フィッシング、ボット、ランサムウェアなどの高度なサイバー脅威も増大しています。

モバイルの活用とデジタルワークスペースへの投資においてセキュリティは最優先事項[2]ですが、サイロ化されている既存のセキュリティ ツールでは包括的に状況を把握することは困難です。一方で、複数のツールを使い分けてデジタルワークスペースを保護するには複雑な手作業が必要となり、非常にコストがかかるため、今日のデジタルワークスペース戦略では、セキュリティが非常に深刻な課題となっています。

境界のない業務環境に対応した包括的な予測型セキュリティ

ユーザーの使用環境を損なうことなくセキュリティのニーズに対応するためには、新たな要件への対応が必要です。

1. 包括的な視認性：エコシステムを保護するコンポーネント間の信頼と検証のフレームワークの活用
2. リスクの継続的な低減：デジタルワークスペース保護に向けた、予測可能で自動化された対策を実現するために環境からインサイトの取得が必要

Workspace ONE Trust Network は、従業員、アプリケーション、エンドポイント、ネットワークを保護する最新の包括的なエンタープライズ セキュリティ アプローチを提供するものです。コンポーネント間の信頼と検証のフレームワークを活用し、進化するデジタルワークスペースを対象とした脅威からの保護、検出、修正を実現する機能を利用できます。デジタルワークスペース全体の信頼性が高まることで、相互に接続された最小限の権限付与で済むシステムを構築し、ユーザーの振る舞いに応じたセキュリティ対策を適用できるほか、インテリジェンスベースの Workspace ONE プラットフォームからのインサイトと信頼性の高いセキュリティ パートナー ソリューションを組み合わせて、予測可能で自動化されたセキュリティ対策を実現し、今日のサイバー脅威のリスクに対応することが可能です。

---

1 出典：https://www.vmware.com/radius/impact-digital-workforce/

2 CCS Insight、「Mobile Technology Buyer Survey」、2017 年 12 月

保護、検出、修正

最も考慮すべきは、サイバー攻撃を受けてしまうかどうかではなく、いつ狙われるかという可能性です。この点を踏まえ、NIST のサイバーセキュリティ フレームワークなどのフレームワークを IT 運用チームとセキュリティ チームが活用することで、セキュリティの各機能を Workspace ONE Trust Network が提供する機能と対応させ簡素化することにより、サイバーセキュリティのリスクを管理できます。

- デジタルワークスペースの保護から始める一連のセキュリティ機能：これには、機械学習によるマルウェア感染の防止、企業のクラウドベースのアプリケーションからのデータ持ち出しの禁止、マイクロセグメンテーションによる、Advanced Persistent Threat（APT）攻撃からの保護が含まれます。
- デジタルワークスペース内に侵入した脅威の検出：適応型の監視機能を継続的に活用することで、IT 運用チームおよびセキュリティ チームはモバイルやデスクトップのエンドポイントおよびアプリケーションの脅威を見つけることができます。
- 脅威の検出と修正の自動化：強力な意思決定エンジンの活用によって修正を自動化できます。異常な動作による攻撃が検出された場合、企業データへのアクセスを自動的にブロックするポリシーを始動させることが可能です。

アクセス、デバイス、アプリケーションの管理と分析機能の統合

Workspace ONE Trust Network は、インテリジェンスベースの Workspace ONE プラットフォームに組み込まれたセキュリティ機能（アクセス、デバイス、アプリケーションのセキュリティと管理を含む）と分析機能を独自の方法で組み合わせることで、管理およびセキュリティ ソリューションのサイロ化を解消します。Workspace ONE Intelligence サービスは、Workspace ONE プラットフォームの分析機能を強化し、ワークスペースのデータの集約、関連付け、推奨事項を提供して、インサイトおよび自動化と組み合わせることができるため、Workspace ONE Trust Network の機能とインテリジェンス サービスを統合することで、境界のない環境におけるセキュリティ リスクの継続的な監視と迅速な問題解決が可能です。

意思決定エンジンは、ネットワーク外にある企業のデバイスなどの情報とユーザーの振る舞いを関連付け、アクセス ポリシーに基づいた脅威の検出と問題修正の自動化を支援します。脅威に関するデータと、デバイスのコンプライアンス状態についての詳細情報を統合することで、セキュリティの問題をリアルタイムで検出、修正し、デジタルワークスペースのセキュリティ対策を強化することが可能です。IT チームは意思決定エンジンを使用して、重要な更新プロフラムを適用し、Windows 10 のエンドポイントの脆弱性の修正や、グループまたは個人レベルでのアプリケーションやサービスへの条件付きアクセス制御の設定など、一般的なタスクを自動化および最適化するためのルールを作成できます。

信頼性の高いパートナー ソリューションで構成された優れたエコシステムとの連携

デジタルワークスペース全体にわたる包括的なセキュリティを有効にするには、進化するデジタルワークスペースを保護するコンポーネント間で信頼関係を確立する必要があります。Workspace ONE Trust Network は Workspace ONE プラットフォームを基盤とする API を活用することにより、信頼性の高いフレームワークを提供します。これらの API を通じて豊富なセキュリティ ソリューション エコシステムと Workspace ONE が通信することにより、包括的に環境を把握し、セキュリティと管理を簡素化することが可能です。また、セキュリティ ソリューションのサイロが解消されることで、既存の投資を活用しながら、継続的な監視とリスク分析を飛躍的に向上させ迅速な対応ができることから、傾向やパターンに基づいた、予測可能なセキュリティ対策を実現できます。

詳細情報

Workspace ONE Trust Network の詳細については、次の URL を参照してください。
www.vmware.com/jp/products/workspace-one/security

無償のハンズオン ラボもご利用いただけます。
https://my.vmware.com/jp/web/vmware/evalcenter?p=workspace-one-hol

VMware 製品のご購入または詳細情報のお問い合わせ先

VMware 製品のご購入または詳細情報については製品 Web サイトをご覧ください。

http://www.vmware.com/jp/products
認定リセラーは Web サイトで検索いただけます。

主な機能

Workspace ONE Trust Network が提供するセキュリティ機能を活用することで、増大するサイバー脅威からの保護、検出、修正を行うことができます。

機能	説明
複数のセキュリティ ソリューションをつなぐ基盤となるデジタルワークスペース プラットフォーム	オープンなセキュリティ エコシステムと Workspace ONE との通信を可能にする API による信頼性の高いフレームワークを使用して、セキュリティと管理を簡素化
業務を簡素化するアクセス管理	アプリケーションのプロビジョニング、セルフサービス カタログ、多要素認証、すべてのアプリケーションを対象とするシングル サインオン（SSO）などの機能を提供します。
コンテキストベースのポリシーで最適化されたユーザーの使用環境とセキュリティ	デバイスのコンプライアンス状況、ユーザー認証の強度、データの機密性、ユーザーの場所など、条件に基づくアクセス ポリシーによる認証の制御が可能です。
情報漏洩防止対策（DLP）ポリシーによる情報の保護	デバイスレベルの暗号化ポリシー、データ暗号化ポリシー、ハードウェア セキュリティ ポリシーを有効にできます。アプリケーション ブラックリスト、デバイス ペアリング、Wi-Fi セキュリティ、TLS の適用などのポリシーを設定できます。マルウェアの脅威、悪意のあるアプリケーション、インメモリ攻撃、ジェイルブレイクされたデバイスを監視し、リモート ロック、デバイス データワイプ、アクセスのブロック、またはカスタマイズ可能なデバイス検疫コントロールを使用して自動的に修正できます。
ユーザーの使用環境を損なわないアプリケーション保護	VMware のセキュアな業務アプリケーション（VMware Boxer™、Browser™、Content Locker™）のセキュリティ制御機能を活用します。それ以外のアプリケーションもすべてクラウド サービスで脅威を検出し、修正を自動化します。
保存データおよび転送中のデータの暗号化	デバイス上のアプリケーションからデータセンターへのトラフィックを VMware Tunnel で認証し、暗号化します。AES 256 ビット暗号化を使用してアプリケーションの保存データおよび転送中のデータを保護できます。
マイクロセグメンテーションによるネットワーク全体のセキュリティの自動化	VMware NSX®（https://www.vmware.com/jp/products/nsx.html）のマイクロセグメンテーション機能を使用してデータセンターの攻撃対象領域を最小化し、ネットワーク全体のセキュリティを自動化します。
インサイトとオートメーションを組み合わせた予測型セキュリティ	Workspace ONE Intelligence（https://www.vmware.com/jp/products/workspace-one/intelligence.html）から提供される脅威に関するデータおよびデバイスのコンプライアンス状態の詳細を統合することで、セキュリティの問題をリアルタイムで検出して修正します。

ヴイエムウェア株式会社 〒105-0013 東京都港区浜松町 1-30-5 浜松町スクエア 13F www.vmware.com/jp