ホワイトペーパー：2018 年 3 月

デジタル ワークスペースのセキュリティに対する包括的なアプローチ

vmware®

目次

従業員が必要とするアプリケーションを時間、場所、デバイスを問わずに提供する企業は、個人および組織レベルの意思決定、生産性、効率性を大幅に向上させることができます[1]。

はじめに

デジタルワークスペースの活用による従業員の生産性向上や従来のワークスペースを上回る効率性という新しいビジネス メリットが定量化されるにつれて、企業の関心は、あらゆるデバイスにアプリケーションを安全に配布しながら、このようなメリットを実現する方法に集まっています。ビジネス上 Forbes Insights の『Impact of the Digital Workforce』で紹介されているようなメリットが求められていますが、従来型の業務環境における境界が消滅したとしても、メリットの実現のためにセキュリティを妥協することは容認できません。

業務環境の境界の消滅により脅威にさらされる組織

どの組織の IT 部門も、その数と深刻度が増していくセキュリティの脅威と日々戦い続けています。マルウェアの侵入によって多くの損失を伴う運用の中断を余儀なくされた IT 部門は少なくありません。たとえば、WannaCry によるサイバー攻撃では Microsoft Windows の脆弱性により数百万台のコンピューターが狙われ、同時に約 150 か国のコンピューターで身代金の要求がありました。また、米国では、2017 年に確認されたデータ侵害の件数が過去最高を記録しました[2]。

拡大し続ける組織および業務環境の境界は、サイバー犯罪者にとって絶好の機会となっています。最近のゼロデイ攻撃や中間者（MITM）攻撃は、その代表的な例です。ゼロデイ攻撃という名前は、開発者が脆弱性に気付く前または気付いた当日（ゼロ日目）に攻撃が発生することに由来します。中間者（MITM）攻撃という名前は、攻撃者が公開鍵メッセージのやり取りを傍受して盗聴を行い、要求された鍵を別の鍵に置き換えてメッセージを再送信するといった傍受の方法に由来しています。MITM 攻撃の特徴は、本来の送信者と受信者が気付かないうちに通信の乗っ取り、監視、変更が行われることです[3]。ソーシャル エンジニアリングやプログラミングの専門知識を使用する高度なフィッシング手法や、ボット、ランサムウェアの脅威にさらされる組織の数は増え続けています。最新の対策を講じている組織も例外ではありません。

脅威への対策とエンタープライズ データの保護

進化を続けるデジタルワークスペースを保護するためには、インテリジェンスベースのプラットフォームを通じて脅威からの保護、脅威の検出修正を実現する優れたアプローチが必要です。このようなアプローチを採用することで、動的なサイバー攻撃の脅威が増加し、従来の境界では想定されなかった新たな脆弱性が狙われるなかでも、組織のデジタルワークスペースの戦略拡大と進化に合わせて機密データを効果的に保護することができます。

このホワイトペーパーでは、境界のない世界における新しい包括的で予測型のセキュリティ アプローチについて説明するとともに、進化するデジタルワークスペースを保護する重要性と、エンタープライズ エコシステムのコンポーネント間にトラスト フレームワークを構築する必要性について解説します。また、収集したデータから得たインサイトを活用して、脅威からの保護や攻撃の拡散防止について適切な意思決定を行うのに必要な、保護、検出、修正に関する 8 つの主な機能についても紹介します。

1 Forbes Insights、『The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT』、2017 年 10 月

2 Identity Theft Resource Center、『2017 Annual Data Breach Year-End Review』

3 Technopedia、『Zero-Day Threat』、2018 年

「2018 年のモビリティ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です」

– CCS Insight

セキュリティは現在のデジタルワークスペース戦略の最大の障壁

現在の働き方は、場所に左右されません。従業員は、さまざまなネットワークを介して、オフィスや自宅だけでなく、カフェや飛行中の機内からでも個人または企業の所有する各種デバイスを駆使して情報やアプリケーションにアクセスします。IT 部門は、重要なエンタープライズ データを保護するとともに、業務を行う時間、場所、デバイスに幅広い選択肢を求める従業員のニーズを満たそうと努力しています。

しかし、既存のセキュリティ ソリューションは十分ではありません。IT 部門は、急速に変化するエンド ユーザーのニーズを、複雑でレガシーなセキュリティ テクノロジーを寄せ集めて満たそうとしますが、一部のテクノロジーは本来の対象とは異なるものを保護するために展開されていることもあります。長期間にわたってさまざまなソリューションを導入した結果、十分に連携できないテクノロジーが増えてしまい、攻撃に対してさまざまな潜在的脆弱性が存在することになりました。組織の成功にとって従業員の満足度は極めて重要な要素ですが、多くの IT リーダーは、2018 年のモビリティおよび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が最優先事項であると考えています[4]。

CCS Insight が最近実施したアンケートでは、IT 購入担当者の約半数（47 %）が、今後 12 か月間のデジタルワークスペースへの投資における最重要事項はネットワーク セキュリティであると回答しています。そして、続いてデバイス セキュリティ（42 %）、アプリケーション セキュリティ（27 %）という回答になりました。これらの投資は社外などから業務をする際のデータやアプリケーションの保護の強化には役立つかもしれませんが、個別のセキュリティ ソリューションのサイロ型の導入では、複雑さが増すだけでなく運用上のエラーを誘発する可能性もあります。たとえば、あるシステムへの侵入をネットワーク ファイアウォールが阻止できたとしても、さまざまなシステム間の East-West トラフィックへの侵入と感染を数か月間検出できなかったために、エンタープライズ全体に損害を与える可能性があります。トラスト フレームワークに基づいてサイロ化されているセキュリティ ソリューション同士を橋渡しするアプローチを使用することで、継続的に脅威からの保護、脅威の検出と修正の実行が可能になることから、保護、検出、修正に優先順位を設定する必要がなくなります。

企業は、従業員のデジタルワークスペース全体をカバーするデジタルワークスペース セキュリティへの最新のアプローチを使用することで、システムとデータを狙って絶えず進化するサイバー脅威への対策を効果的に展開することができます。このモデルでは、エンド ユーザー コンピューティングのエコシステムを保護するためのコンポーネント、すなわち従業員、アプリケーション、エンドポイント、ネットワークの間で信頼関係を確立し、検証によって承認されたアクセスのみを許可する必要があります。包括的で統合されたトラスト フレームワークを使用することで、データを確実に保護するとともに、インサイトと自動化されたインテリジェンスを通じて継続的な検出と問題修正を行い、リスクを最小限に抑えることが可能になります。

4 CCS Insight のアンケート「IT Buyer Survey」、2017 年 9 月

新しいセキュリティ要件

- 組織を保護するため、保護、検出、修正に関する 8 つの主要な機能の導入
- エコシステムを保護するコンポーネント間に信頼関係を確立するフレームワークを使用することで包括的な可視化の実現
- 環境から取得したさまざまな情報に基づく予測型および意思決定の自動化によるデジタルワークスペースの保護とリスクの継続的な低減

進化するデジタルワークスペースの包括的なセキュリティを実現するための 3 つのステップ

IT 組織には、エンド ユーザー環境を保護するための包括的なエンタープライズ セキュリティ アプローチが必要です。サイロ化されたセキュリティ テクノロジー間を橋渡しすることで、エンドポイント、アプリケーション、従業員、ネットワークにわたるセキュリティを網羅するモデルです。最善の結果を得るためには、次に説明する各ステップを踏まえて、進化を続けるデジタルワークスペースを戦略的に保護する必要があります。

ステップ 1：脅威からの保護と、脅威の検出/修正

サイバー脅威は進化しています。システムに不正にアクセスし、すぐに退散して友人に自慢する学生のような愉快犯から始まったハッキング行為は、現在ではほとんどのケースで悪意のあるハッカーまたはハッカー集団によって行われています。サイバー犯罪から保護するためには、次の 3 つの観点で、正規のアクセスは許可するとともに不正アクセスを防止する包括的な対応が必要です。

保護

企業（特に金融サービスや医療機関など規制の厳しい業界の組織）は、機密性が非常に高い重要なデータを格納するバックエンド ストレージに関して、さまざまなコンプライアンス要件を満たすための努力を重ねています。一方、現在では顧客とのミーティング中でもタブレットから機密データにアクセスできるため、そのタブレットをタクシーに置き忘れただけで機密データが盗まれる可能性があります。顧客情報の損失や漏洩が発生すると、企業ブランドに対するマイナスの影響と経済的な打撃は避けがたいものになります。

従業員に対するデータとアプリケーションへのシームレスでコンシューマー製品のようなシンプルなアクセスの提供は、高いリスクを伴うものであってはなりません。エンタープライズ セキュリティ機能を検討する場合、まず最初に従業員のデジタルワークスペースの保護を考慮する理由は、ここにあります。IT 部門は、不審なリンクをクリックしないよう従業員を教育し、データ損失を防止するポリシーを展開することによって、環境へのマルウェアの侵入を防ぐ必要があります。また、従業員やアプリケーションからデバイスとネットワークにいたるまで、組織のすべての資産を完全に可視化することで、脆弱性を特定して組織の内外の脅威から環境の保護が可能になります。アクセス制御、機密データの分類、デバイスの使用制限、アプリケーションへの定期的な修正プログラムの適用など、ポリシーの徹底を含むさまざまな保護を完全に実装したあとでのみ、次の段階である「検出」に移ることができます。保護のための取り組みと、効果的な検出方法が対になっていないと、もっとも重要な課題に対処しているのかがわからないためです。

検出

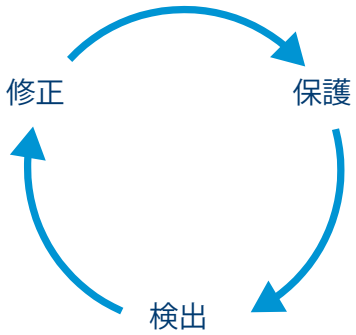
境界の消失、内部からの脅威、攻撃手法のますますの多様化によって、セキュリティ対策の前提は「攻撃を受けるかどうか」から「いつ攻撃を受けるか」へとシフトしました。その結果、企業は資産の保護に加えて、認証情報の漏洩からパッチが適用されていない脆弱性への攻撃まで、さまざまな侵入の発生を検出する必要性に直面しています。IT 部門は、大きな被害が発生する前にアクティブな脅威を検出して無効化する必要があります。また、検出は、アラートの大量発生が起きないように実装する必要もあります。

脅威がデジタルワークスペースに侵入しても、準備ができている企業であれば、継続的で適応型の監視機能によって検出できるため、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。自動化された継続的な監視とアラートの機能により、情報にアクセスしているユーザー、アクセスに使用された方法とネットワーク、アクセスされている情報、アクセス元を把握することで IT のコントロール性を維持できます。次に、最後に確認された正常な状態、ログ、インテリジェンスを分析に使用することにより、異常を認識し、その情報を使って次のステップに向けた適切な意思決定を行うことができます。

修正

デジタル ビジネスは変化が激しく、ほとんどのタスクで手作業による修正が必要な従来のセキュリティ ソリューションでは対応できません。現在の企業では、悪意のある侵入や予期しない障害が発生した場合に迅速に対応することが求められています。対応の遅れは被害の拡大につながる可能性があります。VMware の調査では、お客様企業の 10 社に 1 社が、ほとんどまたはすべてのエンドポイントに影響する Windows 修正プログラムの適用を完了するまでに 1 年以上を要していることがわかりました。これだけの時間があれば、サイバーセキュリティ犯罪者は新しい攻撃方法を開発することができます。

IT 部門は、環境から取得した情報を活用して確実なポリシーを事前に定義し、根本原因に応じて対応とリカバリをすばやく自動化して最良の結果を得る必要があります。自動化機能を使用して、隔離、サスペンド、アプリケーションやクラウド サービスへのアクセスのブロックを選択できます。対策済みの企業では、脅威が検出された場合に自動で修正を行う効果的なソリューションを実装しています。このようなソリューションのエンジンは、異常な振る舞いを検出した場合、機密データへのアクセスをブロックするポリシーを自動で適用します。



エコシステムのコンポーネント間、およびコンポーネントを保護するソリューションの間に信頼関係を確立できる戦略的フレームワークを導入したエンタープライズは、重要な企業資産を完全に保護し、検出と修正までの時間を短縮することができます。

ステップ 2：保護、検出、修正の機能

ここで紹介する 8 つの主要な機能は、新しい包括的なデジタルワークスペース セキュリティの実現に不可欠です。

単一のオープン プラットフォーム アプローチ	単一のオープン プラットフォームを採用することで、デバイスやアプリケーションなどへのコンプライアンスの適用が簡素化され、リスクを低減できます。単一のオープン プラットフォームを導入して、アクセス、デバイス、アプリケーションの管理と分析機能、およびインテリジェンスを組み合わせることで、複雑でコストのかかる既存のサイロ化されたセキュリティ ソリューション間を独自の方法で橋渡しできます。また、インテリジェンス サービスを備えた単一のプラットフォームでは、ワークスペースのデータの集約、関連付け、推奨事項の提供により、統合化されたインサイトとオートメーションを実現できます。 このアプローチを使用する企業では、従業員、アプリケーション、エンドポイント、ネットワークの包括的な可視化を実現できます。このプラットフォーム アプローチは、エンタープライズ エコシステムのコンポーネント間の信頼関係を確立する API 通信のフレームワークを基盤とする必要があります。このようにデジタル ワークスペース全体の信頼性を高めることで、相互に接続された最小権限のシステムによって従業員全体の保護が可能になり、業務の効率が向上します。
情報漏洩防止対策（DLP）ポリシー	DLP ポリシーは、組織のデータがデータセンターの内部にあるか外部にあるかにかかわらず、データの保護に役立ちます。IT 部門は、紛失または盗難に遭ったデバイスのリモート ロックや企業情報ワイプ、所在不明のデバイスの捜索のほか、デバイスのオペレーティング システムのバージョン、最終更新日、位置などの情報をリアルタイムで取得できる必要があります。仮想デスクトップ インフラストラクチャ（VDI）を使用してデスクトップとアプリケーションを一元管理することにより、置き忘れや盗難に遭ったデバイスに起因する情報漏洩のリスクを低減することができます。 また、すべてのエンドポイントにわたって OS で提供されているネイティブの DLP 制御機能を使用して、アプリケーションごとにセキュリティ ポリシーを適用および管理し、E メールの添付ファイルの制御、カット/コピー/ペーストの制限、動的な電子透かしなどでコンテンツ全体の情報漏洩を防止する必要があります。ユーザーが社内のコンテンツを削除することができないように、SDK を使用して管理、制限する必要もあります。 ポリシーおよびコンプライアンス エンジンで、高度な DLP コンプライアンスの確保を自動化できます。高度なセキュリティ ポリシーには、root 化されたデバイスやジェイルブレイクされたデバイスに対する保護の設定、ホワイトリストおよびブラックリストへのアプリケーションの登録、アプリケーションで開く機能の制限、ジオフェンス、ネットワーク設定、エクスポートとスクリーンショットのブロック、外部 SD カードやリモートのクラウド バックアップ ソリューションへの企業情報のバックアップや保存の制限などが含まれます。
コンテキストベースのポリシー	コンテキストベースのポリシーを使用して条件に基づいたアクセスをエンド ユーザーに適用することにより、承認されたユーザーのみが機密情報やリソースにアクセスできるようにします。企業は、役割、部門、機密情報の取り扱いレベルなどによって条件に基づいたアクセス権を確立し、承認されたユーザーのみが特定の情報やリソースにアクセスできるように制限する必要があります。 ポリシーの適用をアクセスおよびデバイスの管理と組み合わせることによって、データ、アプリケーション、デバイスに対するユーザーの権限を制限できます。同じテクノロジーをモバイル アプリケーションに対する条件に基づいたアクセスに適用することで、コンプライアンスに準拠したアプリケーションのみが社内システムにアクセスできるようにすることもできます。

アプリケーションの保護	アプリケーション レベルで DLP ポリシーを適用することにより、よりきめ細かいアクセス ポリシーでデータの保護を大幅に強化できます。デジタルワークスペースには、アプリケーション レベルで同様の機能を提供する DLP ポリシー（前述の 2 つめの機能）を含める必要があります。 個人所有（BYO）デバイスと企業所有のデバイスの両方で、モバイル アプリケーション管理によってプロビジョニングとアクセス制御を容易にし、ID ごとに定義されたポリシーをアプリケーションに適用できます。同様に、クラウドでの情報漏洩防止に加えて、承認および非承認のクラウド サービスへのアクセスとアクティビティの管理を行うことによって、データのセキュリティと脅威に対する保護を向上させることができます。 iOS、Android、macOS、Windows 10 など、すべての主要 OS におけるデバイス単位の VPN、アプリケーション単位の VPN、SDK ベースのプロキシ ゲートウェイ通信により、アプリケーションの接続の保護に適切なソリューションを柔軟に選択できます。 さらに、業務アプリケーション（E メールやドキュメント管理など）には、次のような DLP および RMS（Rights Management Services）機能を提供する必要があります。 • IRM（Information Rights Management）による E メールの保護 • PKI を使用する S/MIME • E メールの分類 • 機密情報や個人情報（PII）に関するポリシー • 添付ファイルの暗号化 • 印刷、表示、ローミングに関するアクセス ポリシー • ドキュメントの有効期限 • 電子透かし
アクセス管理	企業は、ユーザー ID を複数の要素に基づいて確認したり（多要素認証）、複数のアプリケーションに対して一括で確認する（シングル サインオン）などして、データの保護を強化しています。増え続けるアプリケーション、デバイス、クラウド サービスに個別のポリシーを設定するような複雑なタスクを排除するためには、エンドユーザーの ID を使用してセキュリティ パラメーターを確立する必要があります。 ワンタッチ シングル サインオン（SSO）では、ユーザーは何度もログインすることなく、デスクトップ、モバイル、クラウドのさまざまなアプリケーションにアクセスすることが可能になります。SSO は複数のアプリケーションに対して一括でユーザー認証を行うため、デジタルワークスペースへの単一のアクセス ポイントが提供され、任意のエンドポイントからアプリケーション カタログを通じてさまざまな Web、モバイル、SaaS、レガシーのアプリケーションにアクセスできます。 多要素認証（MFA）では、ユーザー ID やシステム コンポーネントが、要求されたアクセスや機能のリスクに応じて、パスワードのほかに複数の要素を使用することで認証されます。
暗号化	暗号化を行うことにより、データの送受信時に意図しない第三者によるデータの受信を防止して、機密データを保護できます。重要なビジネス プロセスのベストプラクティスには、すべてのデータを暗号化して保存および転送することが含まれます。暗号化しておくと、情報漏洩が発生して重要なファイルが盗まれても、攻撃者は読み取り不能なデータしか入手できません。転送中や保存時のデータには、AES 256 ビット暗号化など、高度な暗号化規格を適用することが重要です。 デバイス プラットフォームとエンタープライズ システムを連携させることにより、トンネルやアプリケーション単位の VPN を使用して、コンプライアンスに準拠したデバイス上の個々のアプリケーションからバックエンド システムへの一意の証明書を使用したトラフィックの認証と暗号化を行うことができます。

マイクロセグメンテーション	組織は、ネットワーク全体でマイクロセグメンテーションを活用し、脅威への対策、リスクの低減、セキュリティ状態の向上を積極的に推進できます。マイクロセグメンテーションは、次のような機能を組み合わせて提供します。 • 分散型のステートフル ファイアウォールと ALG（アプリケーション レベル ゲートウェイ）をワークロード単位の粒度で実行することにより、データセンターの境界内の攻撃対象領域を削減 • 仮想マシン（仮想デスクトップと仮想アプリケーション ホストを含む）へのオブジェクト ベースのポリシー適用にセキュリティ グループを使用できるようにして、アプリケーション レベルでの詳細な制御を作成 • 基盤となるネットワーク ハードウェアに関係なく、ラックまたはデータセンター全体にまたがって、論理ネットワークによるオーバーレイに基づく分離化とセグメント化を可能にすることで、複数のデータセンターのセキュリティ ポリシーの統合管理を実現 IT 環境全体を小さなパーツに分割することで管理しやすくし、環境の一部が攻撃を受けても被害の拡大を阻止します。アプリケーションからの East-West トラフィックをデータセンター内の特定のワークロードに分離することで、ビジネスに大きな脅威を与えるマルウェアやウイルスの攻撃経路を大幅に削減できます。
分析	企業は、アプリケーションの展開や使用状況から取得した実用的な情報に基づいてセキュリティ状態を改善します。アプリケーションの展開、使用状況、デバイスのセキュリティ、エンド ユーザーの使用環境の詳細情報を集約することにより、デジタルワークスペース環境のパフォーマンスとセキュリティに関する理解を深めることができます。自動化されたアクションを含む組み込みのインテリジェンス サービスは、計画立案の迅速化、セキュリティの強化、エンド ユーザーの使用環境の向上に役立ちます。また、境界が消滅した今日の環境でも、セキュリティ リスクを継続的に監視し、迅速にリスクを緩和するための対応ができます。インテリジェンス サービスと意思決定エンジンを組み合わせて使用することで、さまざまな情報を関連付けて、アクセス ポリシーに基づいた脅威の検出と自動修正を行うことができます。

ステップ 3：信頼性の高いパートナーによるセキュリティの強化

セキュリティの脅威は、頻度やコストが増しているだけでなく、ターゲットや精巧さも増しています。脅威から保護し、脅威を検出、修正するためには、単一のプラットフォームと、シームレスで信頼性の高いセキュリティ パートナーを組み合わせることが理想的なアプローチです。重要な情報の保護を目的に設計された従来の単体のセキュリティ ツールは、IT 部門のための可視化が限定的であり、環境全体でソリューションのサイロ化が発生する原因にもなります。このような連携を欠いたアプローチでは、デジタルワークスペースの保護が複雑になり、手作業に依存するため、コストがかさむというマイナスの影響が生じます。

成長と進化を続け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ことで、包括的なセキュリティを実現できます。理想的なアプローチは、実績のあるデジタルワークスペース プラットフォームを基盤とする API を利用したトラスト フレームワークを活用することです。これは、API によって、多彩なセキュリティ ソリューションで構成されるエコシステムとプラットフォームとの通信が可能になり、セキュリティと管理の簡素化に不可欠な統合的な可視化が実現されるためです。

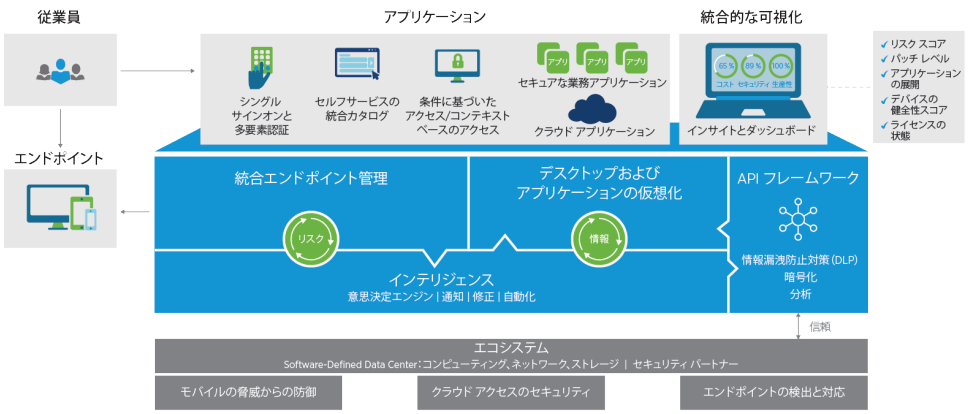
堅牢なデジタルワークスペース戦略には、次のような領域における攻撃の阻止とリスクの低減に特化した、信頼性の高いセキュリティ ソリューションが含まれます。

- OS のセキュリティ脆弱性の可視化
- デバイスの健全性の評価
- デバイスの復元
- アクセスと制御の管理
- ポリシー設定
- ウイルス スキャン
- パッチ適用
- ディザスタ リカバリ
- コンプライアンスの監視

VMware が実現する従来型デジタルワークスペース セキュリティの変革

サイバーセキュリティ ツールには多くのイノベーションが起きていますが、市場にあふれるツールの数と種類こそが、デジタルワークスペースのセキュリティに対する最善のアプローチがまだ実現していないと IT リーダーが感じている原因でもあります。VMware のソリューションは、変化し続ける脅威からの攻撃に対処するためのフレームワークを活用してセキュリティを簡素化するため、企業は確信を持って導入することができます。

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、新しい包括的なエンタープライズ クラスのセキュリティ アプローチを提供します。信頼性と認証のフレームワークに基づく Workspace ONE Trust Network は、進化を続けるデジタルワークスペース全体を保護し、脅威の検出と修正といった一連の機能を提供します。デジタルワークスペース全体の信頼性を高めることで、相互に接続された最小権限のシステムによって従業員全体を保護することで、業務効率を向上できます。最新のサイバー脅威に関連するリスクを管理するため、Workspace ONE Trust Network ではインテリジェンスベースのデジタルワークスペース プラットフォームである Workspace ONE の提供する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ることで、デジタルワークスペースに自動化された予測型のセキュリティ機能を提供します。



保護、検出、修正

VMware のアプローチでは、IT 運用チームとセキュリティ チームは、NIST のサイバーセキュリティ フレームワークなどといったフレームワークを利用することで、セキュリティの各機能と Workspace ONE Trust Network が提供するソリューションとの位置付けを簡素化することで、サイバーセキュリティ リスクの管理を可能にします。

- セキュリティ機能の検討は、デジタルワークスペースの保護から開始します。これには、機械学習によるマルウェアの認識、Advanced Persistent Threat（APT）攻撃から保護するためのネットワークのマイクロセグメンテーションの活用、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防止が含まれます。
- デジタルワークスペースに脅威が侵入した際、VMware のセキュリティ機能に含まれる、モバイルおよびデスクトップのエンドポイントとアプリケーション全体を網羅する継続的で適応型の監視機能を提供する VMware セキュリティによって脅威が検出されます。
- 強力な意思決定エンジンによって修正が自動化されます。たとえば、異常な振る舞いに基づいてトロイの木馬や MITM 攻撃が検出された場合、ポリシーの自動適用によって企業データへのアクセスがブロックされます。

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、Workspace ONE の主要なデジタルワークスペース機能（アクセス、デバイス、アプリケーションの管理）を Workspace ONE Intelligence の分析機能と組み合わせて、既存のサイロ化されたセキュリティ ソリューション同士を橋渡しします。Workspace ONE Intelligence サービスは、ワークスペースのデータの集約、関連付け、推奨事項の提供により、インサイトの統合と自動化を実現します。Workspace ONE Intelligence サービスによって Workspace ONE Trust Network の機能を拡大させることで、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対応が可能になります。

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することで、アクセス ポリシー全体での脅威の検出と問題修正の自動化を支援します。脅威のデータやデバイスのきめ細かいコンプライアンス状態に対しての統合化されたインサイトによって、リアルタイムでセキュリティ問題を簡単に特定および緩和することができます。これにより、デジタルワークスペースでのセキュリティに関する感染予防の方法を改善することができます。IT 部門は意思決定エンジンを使用することで、重要な更新プログラムの適用による Windows 10 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に基づくアクセス制御の設定など、一般的なタスクの自動化と最適化の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エコシステムの活用

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実現するには、成長と進化を続け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に信頼関係が確立されている必要があります。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、トラスト フレームワークを提供します。これらの API によって、多彩なセキュリティ ソリューションで構成されるエコシステムと Workspace ONE との通信が可能になり、セキュリティと管理の簡素化に不可欠な環境全体の統合的な可視化が可能になります。

サイロ化されたセキュリティ ソリューション間を橋渡しすることにより、VMware のお客様は既存の投資を活用しつつ、継続的な監視とリスク分析を大幅に向上させ対応時間の短縮を実現することで、傾向やパターンに基づくスケーラブルで予測型のセキュリティ戦略を確立できます。

VMware のお客様は既存の投資を活用しつつ、継続的な監視とリスク分析を大幅に向上させ対応時間の短縮を実現することで、傾向やパターンに基づくスケーラブルで予測型のセキュリティ戦略を確立できます。

企業では、業務環境の境界の消滅に伴い、デジタルワークスペースに新しいセキュリティ アプローチを採用することが不可欠になっています。エコシステム内のコンポーネント間で信頼関係を確立するフレームワークは、新しい従業員、新しいアプリケーション、新しいデバイス、新しいネットワークにも対応します。このフレームワークは、リスクの低減、企業ブランドの保護、コストの削減、俊敏性の向上、すべてのデバイスでのコンシューマー製品のようなシンプルな操作性などを実現しながら、企業をデジタル エンタープライズへと迅速に進化させる基盤となります。

保護、検出、修正：8 つの必須機能

vmware Workspace ONE™ Trust Network	
機能	**重要な理由**
単一のオープン プラットフォーム アプローチ	プラットフォーム、アプリケーション、ユーザー プロファイルにまたがるテクノロジーのサイロ化を排除することによってコンプライアンスの適用を簡素化し、リスクを低減します。
情報漏洩防止対策（DLP）ポリシー	格納されている場所に関係なく、デバイスのワイプ、リモート ロック、アプリケーション単位のセキュリティ ポリシーでデータを保護します。
コンテキストベースのポリシー	条件に基づいたアクセス ポリシーの適用により、承認されたユーザーにのみ機密情報やリソースへのアクセスを許可します。
アプリケーションの保護	アプリケーション レベルの DLP ポリシーで、リソースにアクセスできるユーザーと、アクセスの対象となるリソースを制御することで情報を保護します。
アクセス管理	ユーザー ID に基づく多要素認証またはシングル サインオンによるすべてのアプリケーションへの一括認証を実現することで、データの保護を強化します。
暗号化	データの送受信時に意図しない第三者によるデータの受信を防止することで、機密データを保護します。
マイクロセグメンテーション	ワークロードとトラフィックを分離することで組織の攻撃対象領域を削減します。
分析	アクションを可能にするインサイト、アプリケーションの分析、オートメーションによって、セキュリティ状態とコンプライアンスを改善します。

詳細情報

デジタルワークスペースによって従業員の作業効率の向上を支援することで、従業員とビジネスの両方に大きなメリットがあります。IT セキュリティの問題によって生産性と効率性が損なわれるようなことがあってはなりません。Workspace ONE Trust Network のアプローチでは、動的なサイバー脅威が拡大し、従来の境界の外にある新しい脆弱性が狙われるなか、デジタルワークスペース戦略の拡大と進化に合わせて機密データを保護するための包括的なセキュリティの実装を可能にします。アクセス、デバイス、アプリケーションの管理と分析機能を組み合わせ、エコシステム全体でトラスト フレームワークを活用し、収集したデータから得た情報に基づいて適切なセキュリティ上の意思決定を行うことで、デジタルワークスペースを保護します。

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

本資料は原題「A COMPREHENSIVE APPROACH TO SECURITY ACROSS THE DIGITAL WORKSPACE」の翻訳版です。

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

Copyright © 2018 VMware, Inc. All rights reserved. 本製品は、米国および国際的著作権法および知的財産法によって保護されています。VMware 製品は、http://www.vmware.com/go/patents のリストに表示されている 1 件または複数の特許対象です。VMware は、米国およびその他の地域における VMware, Inc. およびその子会社の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。

アイテム No.：VMW-WP-CMPRHENSIVE_APPROACH_SECURITY_WRKPLC-A4_103
E:2018/03 J:2018/06