VMware Workspace ONE

ユーザーが求めるシンプルさと企業が求めるセキュリティを実現

概要

VMware Workspace™ ONE™ は、シンプルかつセキュアなエンタープライズ プラットフォームで、任意のスマートフォン、タブレット、ラップトップに、あらゆるアプリケーションを提供し、管理できます。ID 管理、リアルタイムでのアプリケーション提供、エンタープライズ モビリティ管理を統合することで、ユーザーにデジタル ワークスペースを提供するほか、データ漏えいの脅威を軽減し、モバイル クラウド時代に向けて従来の IT 運用を刷新します。

主なメリット

- SaaS およびモバイル アプリケーションをセキュアに利用できると同時に、既存のエンタープライズ アプリケーションもサポートできます。
- データ セキュリティとコンプライアンスを適切に維持すると同時に、ユーザーが柔軟にツールを選択して作業できるようにすることで、優秀な人材の確保と活用が可能です。
- モバイル デバイス用に設計されたものと同じ、最新の管理フレームワークを使用することで、Windows 10 の導入を促進します。
- 適応性に優れ、条件に基づいたアクセスを提供する機能により、認証の強度、データの機密性、ユーザーの場所、デバイスの状態に基づいて適切なセキュリティ レベルを確保します。

主な市場動向

最新のアプリケーション（SaaS アプリケーション、モバイル アプリケーション）が迅速に導入できるようになったことに加え、安価に購入できる強力なモバイル デバイスが急増したことで、作業環境に新たな課題が発生しています。

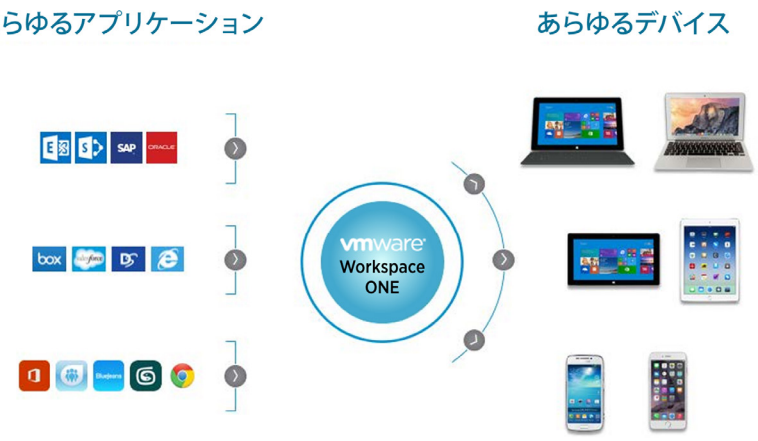
ユーザーは、時間や場所を問わず作業できる環境を求めており、柔軟性の低い従来のポリシーに準拠しない場合があります。企業は重大な転換期を迎えており、意図しないセキュリティ違反が発生する恐れのある状況を無視するのではなく、新たな管理フレームワークを活用して新しい働き方に対応する必要があります。

Workspace ONE について

VMware Workspace™ ONE™ は、シンプルかつセキュアなエンタープライズ プラットフォームで、任意のスマートフォン、タブレット、ラップトップに、あらゆるアプリケーションを提供し、管理できます。ユーザーは、クラウド、モバイル、Windows の各アプリケーションにシングル サインオンでセルフ サービス アクセスでき、業務用の E メール、カレンダー、ファイル、およびソーシャル コラボレーション ツールが効果的に組み込まれています。

VMware Identity Manager や AirWatch エンタープライズ モビリティ 管理ソリューションなどにより、条件に基づいたアクセス ポリシーをリスクに応じて詳細に適用することができるため、ユーザーが使用するデバイスと必要な管理レベルを自身で選択するような BYOD プログラムをスムーズに導入することができます。

Workspace ONE では、従来型のデバイス登録と、ラップトップおよびモバイル デバイスの構成を自動化し、アプリケーションのライフサイクルをリアルタイムで管理でき、従来のクライアント / サーバ型エンタープライズ アプリケーションと、モバイル クラウド時代のアプリケーションのどちらにも対応します。



主な機能

コンシューマ製品のような使いやすさで、ユーザーがクラウド、モバイル、Windows のアプリケーションにアクセス可能に

新しいアプリケーションの追加や新しいユーザーへの対応が、これまでにないほど容易になります。ユーザーは、VMware Workspace ONE のアプリケーションで一度認証されると、カスタマイズされたエンタープライズ アプリケーション カタログに即座にアクセスでき、ほぼすべてのモバイル アプリケーション、クラウド アプリケーション、Windows アプリケーションを利用できるようになります。また、組み込みの VMware Identity Manager を使用すると、業界初のワンタッチでのモバイル シングル サインオンで、デバイスから簡単にアプリケーションにアクセスできます。

機能	説明
最新のモバイル クラウド アプリケーションから従来のエンタープライズ アプリケーションまで、**あらゆるアプリケーションを提供**	あらゆるデバイスに適切なアプリケーションを提供するためのエンタープライズ アプリケーション カタログには、次のようなアプリケーションおよび機能が含まれます。 • セキュアなブラウザとシームレスな VPN トンネルを利用した社内の Web アプリケーション • SAML ベースの SSO とプロビジョニング フレームワークを利用した SaaS アプリケーション • パブリック アプリケーション ストアから購入したネイティブ パブリック モバイル アプリケーション • ビジネス向け Microsoft Windows ストアから購入した最新の Windows アプリケーション • MSI パッケージで提供された従来の Windows アプリケーション • Horizon Air を使用してデータセンターまたはクラウド プロバイダにホストすることで、HTML5 プロキシの内側にある、機密性の高い記録用アプリケーションのシステムを保護 • Horizon Air を利用して、クラウドまたはオンプレミスのデータセンターで管理対象のデスクトップをすべて仮想化 • Citrix XenApp ホスト型アプリケーションをサポート
新しいユーザーへの対応を変革する**セルフ サービスのアプリケーション カタログ**	Windows、iOS、または Android に Workspace ONE のアプリケーションをダウンロードするだけで、セルフ サービスの完全なエンタープライズ アプリケーション カタログをユーザーに提供できます。このカタログは、IT 部門で容易にカスタマイズおよびブランディングすることが可能です。
非常に複雑なオンプレミスの Active Directory トポロジーとも連携する**シングル サインオン**	ユーザー、デバイス、および企業間で信頼関係を確立することで、複雑なログインは不要になり、一度で認証できます。 シームレスな生体認証またはその他の多要素認証の方法を採用することで、より機密性の高いアプリケーションに対応します。 Workspace ONE と Identity Manager を組み合わせることで、SAML および WS-Fed（Web サービス フェデレーション）をサポートするアプリケーション向けにエンタープライズ クラスの ID プロバイダを使用できるほか、すでに使用している既存のサードパーティ製 ID プロバイダとも連携できます。
業界初のワンタッチでのモバイル SSO による、デバイスの信頼性と PIN / 生体認証のタイムアウト設定を活用した認証	ユーザーが PIN 認証サービスまたは生体認証サービスを利用して、認証済みで一意の登録済みデバイスのロックを解除することで、多数のアプリケーションのセキュリティを容易に確保できます。一度ロックを解除すると、ユーザーは、認証が有効な間はアプリケーションをタッチするだけで利用できます。Workspace ONE、VMware Identity Manager、および AirWatch を組み合わせることで、デスクトップ、Web、およびモバイル全体で、業界をリードするシームレスなユーザー環境を実現でき、パブリック モバイル アプリケーションへの SSO は、ユーザー、デバイス、アプリケーション、企業間で信頼関係を確立する、特許出願中の Secure App Token System（SATS）によって実現できます。
認証ブローカーによる新規および既存のサードパーティ認証形式の活用	Workspace ONE と Identity Manager を組み合わせると、RADIUS、Symantec、RSA SecurID、Imprivata Touch、Go などのサードパーティの認証サービスをサポートする認証ブローカーを利用できます。

個人または企業が所有する任意のデバイスを選択可能

現在展開しているアーキテクチャは、まだ開発途上のデバイスへの対応も求められます。ウェアラブル デバイスから 3D グラフィック ワークステーションまで、ユーザーの生産性を維持するということは、時間と場所を問わずアプリケーションを利用可能にする必要があるということです。

これらのデバイスの一部は、企業が所有し、IT 部門がライフサイクルを構成および管理する必要がある場合がありますが、今後多くのデバイスはユーザー個人が所有するものになっていきます。VMware Workspace ONE では、ユーザーがそれぞれのワークスタイルに合わせて、利便性、アクセス、セキュリティ、および管理のレベルを選択でき、IT 部門がデバイスに関わることなく、BYOD プログラムをスムーズに導入することが可能です。

機能	説明
新しいデバイスのプロビジョニングにより、オペレーティング システム管理インターフェイスを活用し、ラップトップ、スマートフォン、およびタブレットをユーザー自身で構成して即座に業務用に使用可能	VMware Workspace ONE の統合管理プラットフォームを使用して、新しいデバイスをセルフ サービスでプロビジョニングできます。 AirWatch のデバイス管理には、Apple iOS および OS X、Microsoft Windows 10、Google Android、および耐衝撃性デバイス向けのさまざまな専用プラットフォームのエンタープライズ モバイル管理 API を利用して、アプリケーションとデバイスのプロビジョニング、構成、および保護を実行します。 また、デバイスは、オペレーティング システム提供者から配信されるパッチにより、脆弱性に即座に対応できます。構成およびアプリケーションは引き続き IT 部門が管理します。

セキュアな業務用アプリケーション：メール、カレンダー、ドキュメント作成、およびチャット機能

Workspace ONE には、ユーザーが必要とする E メール、カレンダー、アドレス帳、ドキュメント、チャット、およびエンタープライズ ソーシャル アプリケーションが含まれます。添付ファイルなどの編集方法や共有方法を制限することで、セキュリティ対策が意識されることなく、企業のデータ漏えいを防止します。

チームでのチャット、打ち合わせ、質疑応答、コンテンツへのアクセス、およびその他のソーシャル ツールなどを、すでにユーザーが使用しているアプリケーションやツールに統合することで、部門間のコミュニケーションを促進し、リアルタイムで共同作業ができるようになるため、生産性だけでなく、真の意味でユーザーの意欲を向上させることができます。




機能	説明
コンシューマ製品のような E メール アプリケーションをビジネス向けに設計	Gmail、Exchange、Outlook、Yahoo、Hotmail、iCloud、Office 365、IMAP および POP3 のメール アカウントをサポートする、高速かつスマートでセキュアな E メール アプリケーションを提供します。Dropbox、Box、Evernote などのお気に入りのサービスと連携することで、管理も非常に容易に行うことができます。
カレンダーとの連携によって、E メールで容易にミーティングを設定可能	E メールとカレンダーを連携させることで、ミーティングの招待を受け取ったときに、E メール アプリケーションから移動する必要がなくなります。アプリケーション間を移動することなく、数回のクリックで、ミーティングの確認や返信をしたり、予定を確認して時間の変更を提案することができます。
E メールの添付ファイルに対する高度なセキュリティ機能でデータ漏えいを低減	AirWatch Secure Email Gateway を使用することで、E メールと添付ファイルのセキュリティを確保できます。エンタープライズ クラスの暗号化の適用、ワイプ、および「プログラムから開く」操作を制御して添付ファイルのセキュリティを確保します。
コンテンツ管理アプリケーションにより、事業部門でのデバイスへのセキュアなコンテンツのプッシュおよび管理が可能	AirWatch Content Locker のモバイル アプリケーションを使用することで、社内のリポジトリや外部のクラウド ストレージ プロバイダからファイルを直接デバイスに送ることができるため、ユーザーは最新の情報にアクセスすることが可能です。
ビジネス向けチャット機能によるユーザーの業務効率の向上	企業向けのセキュアなチャット プラットフォームは、記録システムと既存のエンタープライズ アプリケーションとを連携させると同時に、カスタマイズ可能なモバイル ファーストのチャットおよび通知機能を提供します。

条件に基づいたアクセスによるデータ セキュリティと端末のコンプライアンス

特に重要な機密情報を保護するために、ID とデバイスの管理を組み合わせてアクセスを制御します。これは、認証の強度、ネットワーク、場所、デバイスのコンプライアンスなど、さまざまな条件に基づいて行われます。

機能	説明
ID とモバイルの管理を組み合わせる**コンプライアンス チェックと条件に基づいたアクセス** ポリシーの適用	モバイル、Web、および Windows アプリケーションに対して、条件に基づいたアクセス ポリシーをアプリケーションごとに適用できます。この設定方法には、Identity Manager を使用して認証の強度を適用し、ネットワークの範囲でアクセスを制限する方法と、AirWatch でデバイスに制限をかける方法（Root 化されたデバイス、アプリケーションのブラックリスト、地理的要因など）の 2 通りがあります。
AirWatch による**デバイス管理とコンプライアンス**	デバイスのコンプライアンスを自動化し、データ漏えいに対する高度な保護機能を提供します。これには、Root 化されたデバイスまたはジェイルブレイクされたデバイスからの保護、ホワイトリストおよびブラックリストのアプリケーション、「プログラムから開く」機能の制限、カット / コピー / ペーストの制限、ジオフェンス、ネットワーク構成、および AirWatch のポリシー エンジンで適用されるさまざまな詳細な制限とポリシーに対する保護が対象となります。
アプリケーションおよびデバイスの分析によるリアルタイムな情報提供	アプリケーション、デバイス、およびコンソールのイベントを記録してシステム監視の詳細情報を取得し、コンソールでログを表示したり、事前に定義したレポートをエクスポートすることができます。
インテリジェントなネットワークと VMware NSX との連携	追加機能として VMware NSX を AirWatch トンネルと一緒に使用することで、トラフィックをアプリケーションからデータセンター内の特定のワークロードへさらに分離します。これにより、企業に大きな脅威を与える可能性があるマルウェア / ウイルスの攻撃要因が大幅に低減します。

リアルタイムでのアプリケーションの提供と自動化

Workspace ONE は、Windows 10 の新しい機能を最大限活用し、業界をリードする AirWatch のモバイル管理システムを利用することで、デスクトップ管理者がアプリケーションの提供とアップデートを即座に自動化できるようにします。高い実績を誇る Horizon の仮想化テクノロジーと組み合わせ、アプリケーション提供プロセスを自動化することでセキュリティとコンプライアンスを強化することも可能です。

機能	説明
リモートの構成管理により、ユーザーは、新しいデバイスをどこからでもプロビジョニング可能	Workspace ONE と AirWatch を組み合わせた構成により、ラップトップのイメージ作成が不要になり、シームレスにユーザーがすぐに使用できる環境を提供できます。 動的なスマート グループに基づいて構成を管理でき、デバイスの情報とユーザー属性を考慮し、変更に応じて自動でアップデートが行われます。
AirWatch を使用した **Windows ソフトウェアの提供**でソフトウェアのライフサイクル管理を自動化	AirWatch のソフトウェア提供により、IT 部門は、ソフトウェア パッケージを自動でインストール、アップデート、および削除できます。また、スクリプト作成機能とファイル管理ツールも提供されます。ソフトウェア、アプリケーション、ファイル、スクリプト、コマンドの自動ワークフローを作成して、ラップトップ上にインストールすることもでき、このインストールは、追加時またはオンデマンドで設定できます。 AirWatch を使用すると、パッケージを設定して、ネットワークの状態や指定したスケジュールなどの条件に基づいてインストールすることもできます。また、ソフトウェア アップデートを自動で展開し、アップデートの発生時にユーザーに通知できます。
Horizon の**仮想アプリケーションおよびデスクトップ**によってセキュアなホスト型デスクトップとアプリケーションを提供可能	高い実績を誇るセキュアなホスト型仮想アプリケーションおよびデスクトップを提供する Horizon により、ユーザーは企業データに影響を与えることなく、非常に機密性の高い情報にアクセスすることができます。 ユーザーは、使用している場所やデバイスの種類を問わずに仮想アプリケーションやデスクトップにアクセスできるため、場所を問わずに作業をすることができます。
資産追跡機能により、企業が管理するデバイスの所在場所に関係なく、1 つの画面で確認可能	管理者は、Workspace ONE と AirWatch を組み合わせることで、企業ネットワークに接続されたすべてのデバイスをリモートで監視および管理できます。AirWatch はマルチテナントに対応しているため、地域、事業部門、またはその他の区分に関係なく、すべてのデバイスを 1 つのコンソールで管理でき、ユーザーの役割ごとのアクセス コントロールにより、管理を定義および委任できます。
リモート アシスタント機能によりユーザーのサポートを簡素化	Workspace ONE と AirWatch のリモート アシスタント機能を組み合わせることで、エンド ユーザーに、リモートからのサポートとトラブルシューティングを提供します。デバイスに関する情報を収集するには、デバイス クエリを実行して、最新のプロファイル リスト、デバイスの情報、インストールされているアプリケーション、および証明書を集めることができます。トラブルシューティングをサポートする場合は、ファイル システムのログと構成ファイルにリモートでアクセスし、問題を診断します。IT 管理者は、リモート ビュー コマンドを使用して、ユーザーにデバイスの画面共有をリクエストすることも可能です。

詳細情報

VMware Workspace ONE の詳細については、http://www.vmware.com/go/jp-workspace-one を参照してください。

VMware Workspace ONE またはその他の VMware のビジネス モビリティ ソリューションの購入については、次の製品 Web サイトをご覧ください。

http://www.vmware.com/jp/products

製品の仕様およびシステム要件の詳細については、製品のオンライン ドキュメントを参照ください。

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

アイテム No.：VMW9528-DS-VMW-ID-MGR-DGTL-WKSPC-A4-101 2016/02