ivanti

Windows 10 でユーザー ワークスペース管理がこれまで以上に必要な 5 つの理由

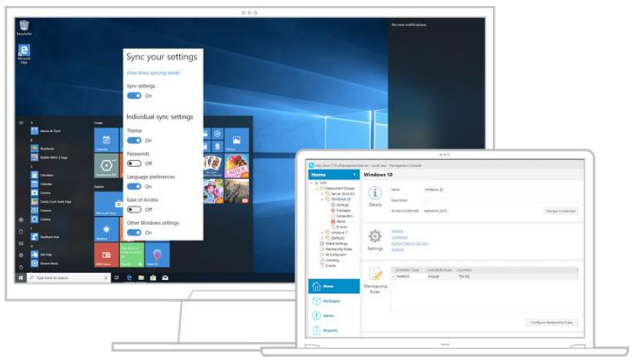
Windows 10 にエンタープライズレベルの機能が次々と追加されていることから、ユーザー エクスペリエンスの向上やエンドポイントの保護にまだサードパーティのソリューションが必要かどうかを検討すべき時が来ています。ここでは考慮すべき 5 つの点を紹介します。

1. パーソナライゼーション機能は無料か?

Windows 10 には組み込みの「設定の同期」機能が搭載されており、一見、パーソナライゼーション機能が「組み込みで」提供されているように見えます。その目的は、ユーザーがコンピューター間でローミングを行う際に、デスクトップとアプリケーションの設定が一緒にローミングされるようにすることです。どの設定をユーザーと一緒に移動するかについては、基本的な制御をある程度行うことができます。

消費者にとっては、設定が自分の Microsoft アカウントで Microsoft Cloud に同期されるという点で素晴らしい機能です。その Microsoft アカウントで新しい Windows 10 デバイスにサインオンするたびに、主な設定の多くが自動的に同期されます。しかし企業では、状況はもう少し複雑です。オンプレミスの Active Directory だけを使用している場合は、ADFS によって Microsoft アカウントのフェデレーションと同期を行い、「設定の同期」機能を使用することができます。Azure AD を使用している場合はこの機能が無効になるため、Enterprise State Roaming を使用する必要があります。機能的にはとても似ていますが、Enterprise State Roaming では企業アカウントを使って設定を Azure AD に保存します。IT 部門にとっては、このすべてが問題となります。

まず 1 つ目は、オンプレミスの AD を使用していて、各ユーザーの Microsoft アカウントに同期している場合、パスワードなどの機密情報が IT 部門の管理外の場所に保存されるようになる点です。このため、特に GDPR の導入により、セキュリティ、プライバシー、および規制の面で影響が出るかもしれません。ユーザーは退職しても Microsoft アカウントを保持します。この問題は Enterprise State Roaming を利用すれば回避できますが、そのためには Azure AD Premium のサブスクリプションが必要になり、別途コストがかかります。



2 つ目は、Microsoft アカウントと Enterprise State Roaming への両方の同期が適用されるのが、ユニバーサル Windows プラットフォーム (UWP) アプリ (モダン アプリ、Windows ストア アプリ、Metro アプリ、さらには WinRT アプリ) というまれな種類のアプリのみという点です。Windows 10 に組み込まれるそれらのアプリの数は (Edge、電卓、付箋、さらにはスタート メニューと) 増えつつあるとはいえ、企業で使用されているアプリの 99% が Win32 API をベースとしているため、それらのアプリで「設定の同期」機能は役に立ちません。

3 つ目は、たとえ UWP アプリであっても、アプリの開発者はこの方法を使用して設定を Microsoft Cloud に保存することを選択するよう求められます。また、必要な設定が含まれていない場合、サードパーティのソリューションを使わないとその設定を追加することはできません。

Office 365 には特定の Office 設定を Microsoft Cloud に取り込むローミング設定機能が別途用意されていますが、ドキュメントが限られており、Office 2016 向けに更新されていません。Windows 10 の「設定の同期」機能のように、Microsoft アカウントか Azure AD アカウントの使用が求められ、どの設定を保存するかを制御することはできず、ロールバックやアーカイブ

の制御機能もありません。また、他の Win32 アプリケーションに拡張することもできません。

ここでいつものようにサードパーティのソリューションが活躍します。サードパーティのソリューションを使えば、Windows デスクトップとアプリケーションのすべての設定を全面的かつ柔軟にカバーし、完全な IT 統制とデータ プライバシーを実現できます。

2. エンドポイントでのセキュリティ

Windows 10 はこれまでの Windows の中で最も安全なバージョンです。Device Guard (Windows Defender Application Control の構成可能なコードの整合性と仮想化に基づくセキュリティ) や Credential Guard といったテクノロジが、従来型の攻撃を防ぐための新たな手段を提供します。どちらも実際にはさまざまなテクノロジの集合体であり、極端な例では、Device Guard を使用して PC を電話や Apple/Android 風のタブレットのようなものに変え、Windows ストアのアプリか、IT 部門が専用のシグネチャを作成して明示的に許可したアプリしか実行できないようにすることも可能です (なおこれは、アプリの変更が行われるたびに再作成する必要があります)。言い換えれば、Device Guard の完全版はアプリケーション実行制御の極端な形であり、望ましくない実行可能ファイルが実行されるのを防ぐ反面、基幹業務アプリの既存資産を実行することも非常に難しくなり、それらのいずれかが変更されるたびに IT オーバーヘッドが必要になります。

Microsoft が推奨するもう 1 つのアプローチは、既存の Win32 アプリを UWP アプリに (デスクトップ ブリッジを使って) 変換することによって、管理者特権なしでアプリを実行し、ラップして保護できるようにする方法です。残念ながら、その変換プロセスは単純とはいえず、ほとんどの場合は Win32 アプリのコードを変更する必要があります。これは、旧式のアプリや外部ベンダーのアプリでは不可能です。Device Guard は後にマーケティング寄りの用語に調整され、Windows Defender ブランドでさまざまなテクノロジに対応するようになりました。

一方、Credential Guard は、ハードウェアによって保護された Hyper-V 仮想マシン内の LSA (ローカル セキュリティ機関) Windows サブシステムを保護します。当然、Credential Guard には厳しいハードウェア要件があり、LSA とやり取りするサードパーティ アプリは Windows 10 向けに更新されるまで動作しない可能性がありますが、有効なセキュリティ機能であり、多数の攻撃ベクトルを阻止します。

それでも、ユーザーの特権昇格やローカル管理者の制御、ブラウザーやアプリケーションのネットワーク アクセスといった問題は、サードパーティ ベンダーを使った方がはるかに簡単に管理できます。また、ファイルのメタデータや他のパターンマッチング機能を使用して、より柔軟にアプリケーションの実行を制御することもできます。そのため、アプリにマイナー更新が行われるたびに IT オーバーヘッドが発生することはありません。先述の Windows 10 の各機能により、これらのソリューションの価値が損なわれることはありません。

3. データ ストレージ

OneDrive は消費者にとって素晴らしいサービスであり、Windows 10 と Office 365 は OneDrive との統合のしやすさを新たなレベルへと引き上げます。OneDrive for Business では、IT 部門は Microsoft Cloud と同期するユーザーのファイルやフォルダーをより細かく制御できますが、それでも多くの組織は、ユーザー データが自組織のデバイスやデータ センター内に保持されるようにする必要があります。オンプレミスのストレージが必要で、かつオフライン フォルダーでは不十分な場合は、サードパーティのソリューションを利用することで、選択的同期や、ファイルの種類とバックグラウンド転送のきめ細かな制御、ファイル配置の完全な監査が可能になるほか、OneDrive と同じクロスプラットフォーム アクセスのメリットも得られます。

また、ユーザー ファイルをクラウドに保存しても問題ない組織の場合、Office 365 ではユーザーごとに 1TB のストレージが提供されますが、ユーザー データは IT 部門の目が届かない場所で管理されることになります。IT 部門にとって、ファイル アクセスの監査や、同期および保存するファイルの種類に対するポリシーの設定、またはオンプレミスとクラウドのストレージが混在する環境に対するアクセスの制御を簡単に実行できる方法は存在しません。このような場合も、サードパーティのブローカーなら、シームレスなユーザー エクスペリエンスを提供し、Office 365 でユーザーごとに提供される 1TB のストレージを活用しながら、IT 部門による制御を確実に保持できます。

4. Windows 7 と 10 間、および Windows Server 2008 と 2016 間での移行とローミング

ほとんどの組織が Windows 8 と 8.1 の導入を見送り、またデスクトップ エクスペリエンスが Windows 8 風であるという理由から、RDSH/XenApp/Terminal Server の展開環境では 2012 と 2012 R2 の導入も見送りました。2020 年の Windows 7 のサポート終了を受け、ようやく企業での Windows 10 の導入が加速しています。また、ユーザーは共有された仮想デスクトップやセッションに Windows 10 のエクスペリエンスを期待しているため、Windows Server 2016 への移行が (多くの場合、Citrix XenApp へのアップグレードとともに) 求められています。

とはいえ、企業のデスクトップの 70% 以上は今も Windows 7 です。つまり、ユーザーは、バージョン 2

(Windows 7)、バージョン 5 (初期の Windows 10 と 2016)、およびバージョン 6 (それ以降の Windows 10 と 2016) のプロファイル間を行ったり来たりすることになると思われます。x86 と x64 の CPU アーキテクチャについては言うまでもありません。Windows の既定のプロファイル ローミング機能ではそれに対応できません。異なるプロファイル バージョン間でのローミングが可能なサードパーティ ツールを利用しなければ、ユーザーがクリーンなエクスペリエンスを得ることはできません。

5. どのように導入状況を追跡するか?

ドメイン上の誰が Windows 10 を使用しているか挙げることができますか。意図的に展開したマネージドデバイスについては既に把握していると思いますが、ユーザーがネットワークに接続するすべての BYOD デバイスや COPE デバイスについてはどうでしょうか。ある程度の情報は Active Directory ツールから得られるかもしれませんが、ネットワーク上に存在するデバイスのエージェントレス検出は今もサードパーティの領域です。ご期待のとおり、Ivanti では、どのデバイスが Windows 10 を使用しているかだけでなく、ライセンス バージョンやビルド、デバイスの種類まで追跡できる幅広いツールを提供するとともに、お客様の移行プロジェクトの進捗に合わせてインタラクティブなダッシュボード、アラート、およびレポートを作成することができます。Windows 10 移行ソリューションの詳細については、Ivanti の Web サイトをご覧ください。

まとめ

Windows 10 には素晴らしい機能と拡張機能が数多く搭載されていますが、どのような規模の企業であっても、IT 部門がユーザーのセキュリティとエクスペリエンスを制御し保護したいと考えている場合には、やはり以下のような機能を備えたサードパーティ ソリューションが不可欠です。

1. デスクトップとアプリケーションの設定のローミングと回復
2. アプリケーション制御と最小特権のセキュリティ
3. データの同期と回復
4. Windows 10/2016 とそれ以前の Windows バージョンとの間でのローミング
5. Windows 10 の導入および展開状況の追跡

www.ivanti.co.jp

(03) 5226 5960

Contact@ivanti.co.jp