PIQUE SOLUTIONS

Windows 10 と macOS

ラボ環境における機能比較: Windows 10 と macOS のセキュリティおよび管理

PIQUE SOLUTIONS

2016 年 7 月

このホワイト ペーパーは、マイクロソフトの後援により作成されました。本書の基盤となっているラボ環境でのテスト、調査、分析は、Pique Solutions が単独で実施したものです。

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

目次

要旨

サイバー脅威防止は、組織が攻撃される可能性を低減することを目標とするものですが、一方でサイバー脅威からの回復 (サイバー レジリエンス) とは、リスク管理を通じ、こうした攻撃によって生じる影響を軽減することを目指しています。サイバー レジリエンス プログラムでは、攻撃を検出・防止する技法を考慮しつつも、侵害は起こり得るものであることを前提としています。このアプローチで重視されるのは、予測力、機動力、適応力です。

サイバー レジリエンスで最優先されるのは、資産に対して適切なセキュリティ機能を活用することです。セキュリティ スタックは、さまざまな脅威、特にビジネス資産に影響を及ぼす脅威から、企業を保護する必要があります。しかし現状では、セキュリティに関する意思決定に活用できるデータが不足しているために適切なセキュリティが利用されておらず、企業がそれに気付いていないことが少なくありません。また、サイバー脅威に直面した際の回復力の強化に活用できるテクノロジやアーキテクチャ関連のプラクティスは数多く存在していますが、それらを利用することでメリットを得られる反面、コストもかかります。

Pique Solutions では、マイクロソフトの Windows 10 と Apple の macOS 10.11 (旧 OS X) の回復機能の比較分析をラボ環境で実施しました。この分析では、回復機能が組織にもたらす保証レベル、回復機能の実用性、ユーザー エクスペリエンスへの影響を評価しました。

マイクロソフトは、Windows 10 を通じて、PC、タブレット、スマートフォンのオペレーティング システムを単一の OS に統合しました。Windows 10 のエディションはすべて共同開発されており、同一のコアと同一のアプリ モデルを共有し、同一のストアにアクセスします。Windows 10 にはさまざまなエディションが用意されていますが、このホワイト ペーパーでは Windows 10 Pro と Windows 10 Enterprise を検証しました。基盤のチップセットによって特別な機能 (x86 プロセッサ上での仮想化のサポートなど) が提供される場合や、コアに関連する特別な機能 (Windows 10 Mobile のテレフォニーなど) が装備されている場合がありますが、その点を除けば、ユニバーサル Windows プラットフォームに組み込まれているセキュリティ、管理、アプリは、PC、タブレット、モバイル デバイス全体で共通です。本書では、このオペレーティング システムを「Windows 10」と呼びます。

この分析ではセキュリティ保証とユーザビリティを主要な基準として測定し、その結果 Pique Solutions は Windows 10 の方がセキュリティ保証のレベルが高く、ユーザビリティに対する影響は低いと結論付けました。Windows 10 は、モバイル デバイス、タブレット、PC にコスト効率の良い 2 要素認証を提供し、ユーザー パスワードを排除して ID を保護することで、資格情報の盗難に起因する侵害発生のリスクを軽減しています。Windows 10 では、ユーザーにとって透過的な方法で企業データが保護され、ユーザーは同一のアプリを個人的なタスクにも仕事にも使用できます。また Windows 10 は、デバイスの正常性構成証明に基づいて企業リソースへの条件付きアクセスを提供します。デバイスの種類にかかわらず、統合された 1 つの OS アーキテクチャとアプリ開発プラットフォームを活用することで、重要なセキュリティ更新プログラムや修正プログラムの配布を含むデバイスとアプリのプロビジョニングを合理化しています。

macOS は高度なデスクトップ機能を備える柔軟なオープン プラットフォームを提供していますが、認証と暗号化のためのハードウェアの信頼のルートが存在せず、企業データの管理と保護を効率化するネイティブ機能もありません。また iPhone と iPad の成功によって、Apple は macOS の強化の手を緩めているようです。現在、Apple のデスクトップまたはノート PC で、認証用の指紋センサーやその他の生体認証リーダーを装備している製品はありません。macOS の次期リリースで提供が約束されている Apple Pay 機能でも、対応する iPhone や iPad に搭載されている TouchID センサーが使用されます。

Apple は攻撃からの回復力に優れているという評価が聞かれますが、macOS がその評判に値するかどうかははっきりとしていません。市場シェアが 10% に満たない macOS は、これまで Windows ほどの注目は集めていませんでしたが、最近 iOS と macOS に過去最大の数の脆弱性が発見されました。Bit9 + Carbon Black の調査で、2015 年は過去 5 年間の合計数の 5 倍以上の Mac マルウェアが検出されたことがわかっています。マイクロソフトは、長年にわたって攻撃に脆弱だという批判に耐えながら、製品やサービスが企業に広く普及しているために発生した非常に多くの攻撃と戦ってきました。マイクロソフトが開発した Windows 10 は、現在最も回復力が高い OS であり、高度な認証、ハードウェア整合性チェック、データ保護、包括的な管理といった機能を備えています。

豊富な資金を持つ攻撃者によって実際に執拗な標的型攻撃が仕掛けられている現在の環境では、デバイスの高度なセキュリティ保証レベル (SAL) に関する要件として、基本的な企業セキュリティ機能を満たすだけでは十分と言えなくなりました。Windows 10 は、最も厳しいセキュリティ要件および企業管理要件を満たす回復性の高いデバイスを提供できます。しかも、エンド ユーザーにとって透過的に、生産性を低下させるどころか高める方法でこうした制御を実現します。

テスト手法

Pique Solutions によって開発された総合的なテスト手法を以下に示します。

1. デバイスから企業リソースへのアクセスに関するリスクを低減するために必要なセキュリティ特性とセキュリティ機能を特定する (情報の保管、共有、使用といった機能を含む)。
2. ディレクトリ サービスなど、大半の組織に共通するコンポーネントを含む、簡易なエンタープライズ アーキテクチャをシミュレートする環境を構築する。
3. Windows 10 と macOS の評価に使用するデバイスと管理システムを選定する。
4. 選定したデバイスがテスト フレームワークに定義されたタスクをどのように実行するかを手作業で確認する。
5. 結果の詳細な評価を公表する。

業界で認知されている標準と定義を使用して Windows 10 と macOS を評価するために、Pique Solutions では、アメリカ国立標準技術研究所 (NIST) 発行のサイバー セキュリティ プラクティス ガイド Special Publication (SP) 1800-4b に記載されているセキュリティ特性と必要な機能を参考にしました。NIST は、NIST SP 800-124、NIST SP 800-164、米国家安全保障局

モバイル機能パッケージ、適切な米国家情報保証パートナーシップ プロテクション プロファイルなどに記載されている複数の標準の内容と概念を分析して、必要なセキュリティ特性を導き出しています。Pique Solutions は、参考にした NIST のセキュリティ特性を適宜変更、更新することによって、不足している機能に対応すると共に、セキュリティ特性とベンダーが主張する機能を相関付け、本書全体の内容と流れを改善しました。

わかりやすく説明するために、セキュリティ機能を次の 4 つの領域に分類しました。

ID と承認

- 認証: デバイスとアプリに対するユーザーのローカル認証、ユーザーのリモート認証、デバイスのリモート認証
- 信頼モデル: 認証のためのユーザーとデバイスのロールの使用、資格情報およびトークンの保管と使用
- 生体認証のサポート: 方法、格納、使用

情報保護

- ストレージの保護 – 保存中のデータ (DAR): デバイス暗号化、安全なキー格納、ハードウェア セキュリティ モジュール
- 通信の保護 – 転送中のデータ (DIT): 仮想プライベート ネットワーク (VPN)、アプリごとの VPN
- 作業中のデータ保護 – 使用中のデータ (DIU): 保護された実行環境、データ管理、データ共有

脅威対策

- デバイス整合性: ブート/アプリ/OS/ポリシー検証、信頼された整合性レポート
- アプリケーション保護: サンドボックス、メモリ隔離、信頼された実行
- ブラウザー保護: サンドボックス、プラグイン/拡張機能、URL ブラックリスト

デバイス/アプリ管理

- デバイス登録: 検出、証明書、プロビジョニング
- デバイス構成とサポートされるポリシー: ネットワーク、デバイス リソース、ジオフェンシング
- アプリ管理: 配信、更新、構成、アプリのブラックリスト/ホワイトリスト
- リモート管理: 資産管理、OS とセキュリティの更新プログラム、紛失したデバイス、リモート ワイプ
- 診断/監視: 異常な動作の検出、コンプライアンス、原因の検出

テスト環境では、世界中の企業で広く利用されている一般的なソフトウェア、具体的には Microsoft Windows Server、 Microsoft Active Directory、 Office 365 (ドキュメントと電子メール)、「企業アプリ」(企業が提供するアプリをシミュレートするための、機能が制限された軽量アプリ)、「個人用アプリ」(個人用アプリをシミュレートするための、機能が制限された軽量アプリ)、および OneDrive を使用しました。

モバイル デバイス管理 (MDM) システムは、マイクロソフトのツールおよび MobileIron と統合された Microsoft Intune を使用しました。

使用したデバイスは次のとおりです。

1. MacBook Pro 13 ― macOS 10.11
2. Surface Pro 3 ― Windows 10 Enterprise

テスト環境とデバイスの構成、定義されたすべてのシナリオの実行、およびこの比較分析の発行は、テスト スペシャリストが担当しました。Pique Solutions では、OS 管理機能を実際の環境でテストするために MDM ベンダーを活用しました。同等の機能と比較するために、Pique Solutions は幅広い企業に導入されている独立系 MDM プロバイダーである MobileIron を選定しました。MDM の分析は、この調査プロジェクトの当初の意図および範囲には含まれていません。

OS の回復力の評価では、ISA-99.01.01 で導入された概念である SAL に照らしてセキュリティおよび管理の機能の分析を行いました。以下に SAL の説明を示します。

> セキュリティ レベルは、ゾーンのセキュリティに対処する定性的なアプローチを提供します。セキュリティ レベル定義は定性的な手法であるため、組織内の複数のゾーンに対するセキュリティの比較と管理に適用できます。利用できるデータが増加し、リスク、脅威、セキュリティ インシデントの数学的表現が開発されれば、この概念は、セキュリティ レベル (SL) の選択および検証の定量的なアプローチに移行するでしょう。セキュリティ保証レベルは、エンド ユーザー企業だけでなく、産業用オートメーションおよび制御システム (IACS) やセキュリティ製品のベンダーも利用できるようになります。また、ゾーン内で使用する IACS デバイスと保護対策の選定や、さまざまな業界セグメントのさまざまな組織においてゾーンのセキュリティの特定と比較にも使用されるでしょう。

ISA99 では、定性的に 4 つの SAL が定義されています。

- SAL1 – 不用意または偶発的な侵害からの保護
- SAL2 – 単純な手段を利用した意図的な侵害からの保護
- SAL3 – 高度な手段を利用した意図的な侵害からの保護
- SAL4 – 幅広いリソースと高度な手段を利用した意図的な侵害からの保護

スコア付けでは、SAL に数値が割り当てられ、組織のセキュリティに対する機能の実用性に基づいて重み付けされています。実用性とは、その機能が組織に必要な特性を提供しているかどうかを意味します。合計スコアは、OS の総合的な回復力レベル、つまり OS がどれだけ効果的に、どのレベルまで攻撃に対抗できるかを表しています。Pique Solutions は、セキュリティがユーザビリティにもたらす影響も評価しました。メトリックには、タスク完了までの時間、エラー率、ユーザー満足度が使用されました。情報セキュリティは、優れたユーザー エクスペリエンスを提供できなければ、必ず人為的なエラーを招くことになります。

主な結果

Pique Solutions がラボ環境で実施した Windows 10 と macOS のセキュリティおよび管理性に関する機能の比較評価を通じ、Windows 10 は macOS よりも優れたソリューションを企業に提供していることがわかりました。この結論は、以下に示す主な結果に基づいて導き出されました。

ID と承認

- Windows 10 は、企業向けに Fast ID Online (FIDO) 2.0 をサポートした初の主要 OS である。
- macOS は 2 要素認証をネイティブ サポートしておらず、サード パーティ製の生体認証またはスマート カードが必要になる。
- Windows 10 ではパスワードの代わりに生体認証機能が採用され、セキュリティとユーザビリティの両方が向上している。
- macOS は、暗号化と認証のためのハードウェア ベースのキー ストレージを提供しない。

情報保護

- Windows 10 の Windows Information Protection (WIP) は、重複するワークスペースやアプリを必要とせずに重要なデータを保護し、セキュア コンテナーやアプリのラッピングが不要である。
- macOS はネイティブなデータ管理機能を提供しないため、データ保護テクノロジへの追加投資が必要になる。

脅威対策

- Windows 10 のメジャー ブートは、ハードウェアを使用してシステム ブート プロセスの整合性を測定する。
- macOS には、暗号化や整合性検証のためのハードウェア セキュリティ モジュールがない。
- Windows 10 は、強力なメモリ制御を包括的な整合性検証機能と共に提供する。Apple は、システム整合性保護を提供してこの機能をエミュレートしようとしているが、再起動してリカバリ モードにすることで無効にできる。

管理

- Windows 10 は、1 つのステップでドメイン認証、プロビジョニング、管理を行うことができる。
- macOS は機能を強化する柔軟性を備えているが、機能を強化するには Apple 拡張サポートを使用してサード パーティ製ツールと統合する必要がある。Apple は、独自プロトコルの範囲を超えてこれらの統合ツールをサポートする単一ソースの役割は果たさない。

- ⊕ Windows 10 は、リモート正常性構成証明に基づいて、デバイスのコンプライアンス状態を確保し、条件付きアクセスによって非準拠デバイスのアクセスを制限する。

テストのスコア

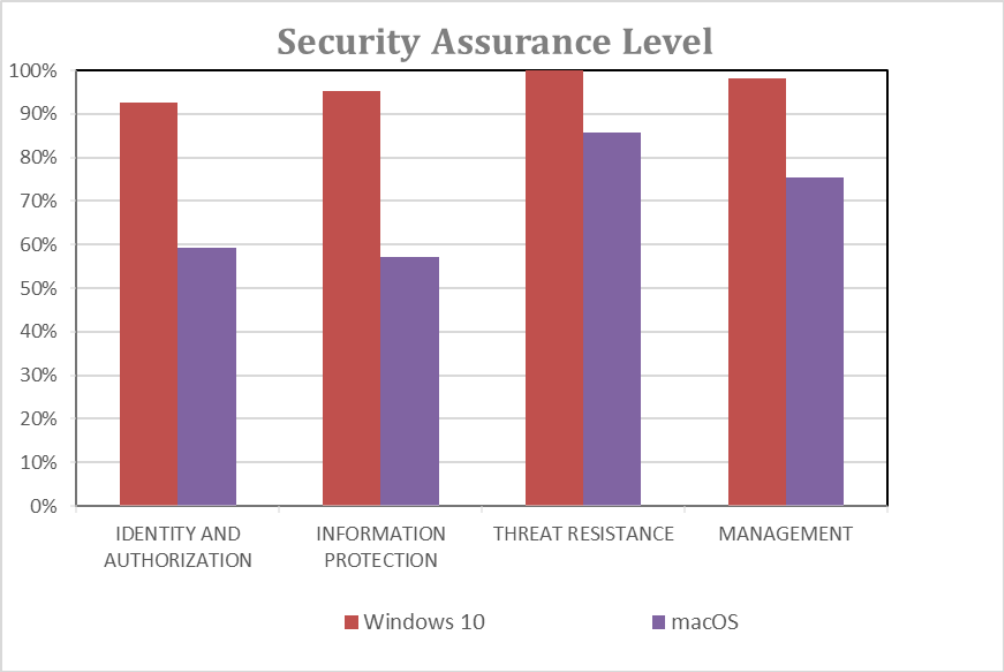

図 1.Windows 10 と Apple macOS のセキュリティ保証に関するラボ テストのスコア

総合すると、Windows 10 は測定されたすべてのカテゴリで一貫して macOS よりも高いスコアを記録しました。データ保護では、Windows 10 がデータに適用する暗号化と制御機能は masOS よりも効率的であり、ユーザー エクスペリエンスに対して透過的であることがわかりました。脅威対策としては、Windows 10 にはリモート構成証明で整合性を検証するためのハードウェアの信頼のルートが備わっています。管理面では、Windows 10 は非常に幅広い OS 管理手法と、ドメイン アカウントを使用した合理的なデバイスのプロビジョニングおよび構成のプロセスを提供しています。

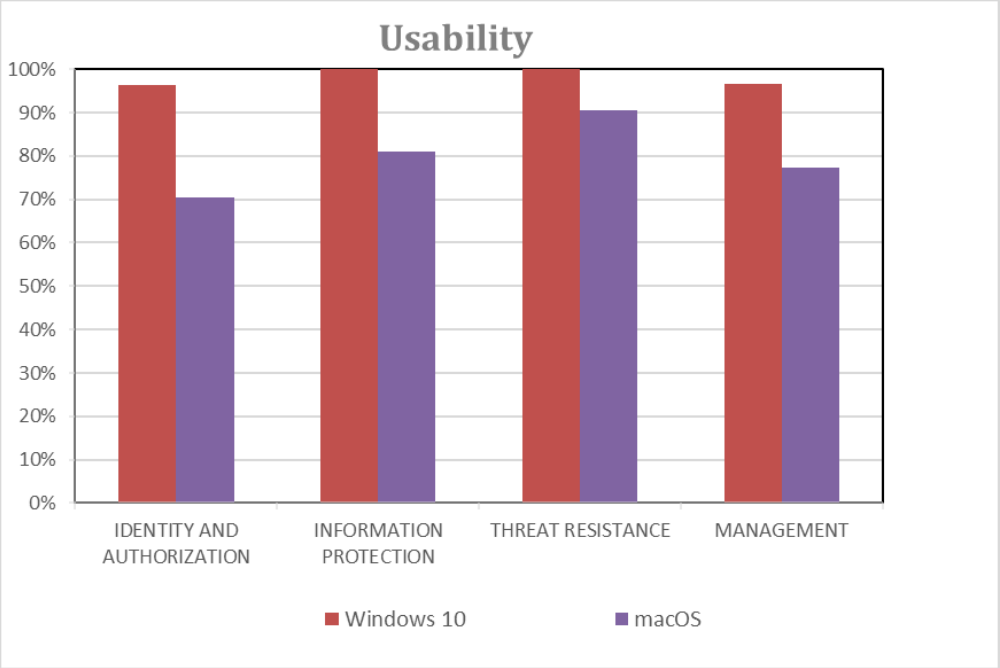

図 2.Windows 10 と Apple macOS のユーザビリティに関するラボ テストのスコア

ID と承認

ID とアクセスの管理 (IAM) は、必要とするユーザーに必要なときに適切なすべてのリソースへのアクセスを提供する機能です。企業は、ユーザーがさまざまなデバイスにアクセスする分散システムを管理する際に機動力を実現できる IAM 機能を必要としています。IAM は、IAM インフラストラクチャのコストを考慮しながら、各ユーザーの ID の整合性と信頼性を保証する必要があります。さらに重要なこととして、IAM は認証制御の強力さとユーザーにとっての使いやすさを両立する必要があります。

最も一般的な ID の形態は、ユーザー名とパスワードです。大半のユーザーは、平均して 3 つ以上のパスワードを記憶しておく必要があるため、非常に複雑なパスワードを設定してしまうと、多くのユーザーは記憶しようという気が起こらず、実際にも記憶するのが困難です。しかし複雑なパスワードを用意しても、最新のコンピューターを使用すれば、数秒とは言わずとも、数分で侵害される可能性があります。ユーザーの資格情報を知っているだけで、第三者がそのユーザーになりすますことができるのです。シンプルで低リスクの個人デバイスと思われていたモバイル デバイスは、利便性を考慮して単純な 4 桁 PIN で標準化されたため、複雑さの要素が大幅に少なくなっています。パスワードと PIN は、強力とは言えませんが、比較的便利で、実装しやすく、ユーザーにとって個人的なものであるという理由から現在も使用されています。多要素認証戦略の一環として、パスワードと PIN は効率的かつ便利に活用できる可能性があります。より効果的な方法として、生体認証を活用すれば、ユーザー ID は一意性が高まり、個人との結び付きが強くなり、ユーザーと企業にとって便利なものなります。

認証

Windows 10 は、ユーザーからデバイスやアプリへのリモート エンタープライズ ドメイン認証に対して 2 要素認証を提供します。Windows Hello は、パスワードに取って代わるテク

ノロジで、特定のデバイスと生体認証ジェスチャまたは PIN の組み合わせを利用します。Windows Hello は、Microsoft アカウント、Active Directory (AD)、Azure AD、または FIDO 2.0 認証に準拠したサード パーティのサービスもサポートしています。Windows 10 は、エンタープライズ環境で FIDO 2.0 を活用する初の OS であり、FIDO 2.0 の採用は大きな前進と言えます。FIDO 2.0 は、非対称キーをハードウェア ベースの構成証明と組み合わせてキーの正当性を検証することで、多要素認証に対応しています。

登録時に行われる最初の 2 段階検証の後、ユーザーはデバイスに Windows Hello をセットアップし、ID を検証するためのジェスチャ (生体認証または PIN) を設定します。トラステッド プラットフォーム モジュール (TPM) チップは、デバイス上で認証キーを生成し、デバイスにバインドします。これにより、デバイスはエンタープライズ ドメイン アカウントに関連付けられた ID の 1 つになります。非対称キー暗号化では、企業アプリやオンラインの企業リソースへのアクセスを許可する前にユーザーが認証されます。これは、スマート カードを使用して証明書ベース認証を強化する方法や、携帯電話によってネットワークを検証する方法に似ていますが、追加のハードウェアは必要ありません。また、Windows 10 では、デバイス上にある個人の Microsoft アカウントを Azure AD や社内 AD ドメインに参加させる必要はありません。

Windows 10 Enterprise は、Credential Guard と呼ばれるアクセス制限された仮想コンテナー内で認証を実行することによって、認証システムの保護を強化します。すべてのアクセス トークンとチケットをこのコンテナーに格納し、最大長のハッシュで完全にランダム化して管理することで、ブルートフォース攻撃を回避します。

macOS は、生体認証リーダー、スマート カード、2 要素認証用トークンの使用を含む、ローカルおよびネットワーク ベースの認証をサポートしています。macOS は、ネットワーク ベースのディレクトリ ドメインとして主にオープン ディレクトリを使用しますが、Kerberos を介した AD サーバーの相互認証もサポートします。macOS における承認は、/etc/authorization に格納されているポリシー データベースによって制御されます。SecurityAgent プラグインは、ポリシー データベース (/etc/authorization) から要件を収集して、すべての認証要求を処理します。

macOS はキーチェーン アプリを使用して、暗号化されたパスワード、証明書、その他のプライベート値を格納します。ユーザーは認証 (パスワード、デジタル トークン、スマート カード、生体認証リーダーを使用) を通じてキーチェーンを解除できます。アプリは、このキーチェーンを使用してパスワードなどのデータの格納と取得を行います。既定では、ユーザー アカウントごとに、ユーザーのログイン パスワードを使用して 1 つのキーチェーンが作成されます。このパスワードによって、ユーザーが macOS にログインするときにキーチェーンのロックが解除されます。キーチェーン アクセスに対して別の認証を強制するには、ユーザーはキーチェーン パスワードを変更する必要があります。キーチェーンは、キーチェーンにアクセスできるアプリを管理するためのアクセス制御リストもサポートしています。スマートカードのような外部デバイスに格納されている場合を除き、キー ストレージに対するハードウェア ベースの保護は提供されません。総合的に見ると、macOS のキー ストアは、システム アクセスを通じて容易に取得できます。リモートのハードウェアに実装することもできますが、その場合は利便性が低下します。

生体認証のサポート

Windows Hello は、Windows 10 で生体認証サインイン オプションを使用するための拡張フレームワークです。ユーザー固有の生体認証 ID によってデバイスへのアクセスを認証します。現在 Windows Hello は、指紋、顔認識、虹彩スキャンをサポートしていますが、現在サポートされている生体認証が新しいハードウェアによって拡張される可能性があります。

Windows 10 は、生体認証とデバイスの他のセキュリティ コンポーネントを統合します。Windows Hello で使用されるユーザーの生体認証データは、ユーザーのデバイス以外の場所に移動されることも、クラウドに一元的に格納されることもありません。Windows 10 は、センサーによって取得された生体認証イメージをアルゴリズム形式に変換します。元のイメージは破棄され、復元できなくなります。このアルゴリズム形式のイメージは、すべての Windows 10 デバイスに必須で搭載されている TPM に格納されます。生体認証イメージが格納されないため、他のデバイスから企業リソースへの不正なアクセスにこれらのイメージが使用されるリスクが排除されます。また、組み込みのスプーフィング対策や生体検知機能により、偽の生体認証データ (ユーザーの目の写真など) を使用してデバイスにアクセスすることはできません。

macOS は、AuthPlugin フレームワークを使用するサード パーティの生体認証をサポートしており、アプリはサード パーティの認証手法に要求を送信できます。セキュリティ サーバーは、アプリと認証ツールの間の認証トランザクションを管理しますが、認証以外の保護レベルは提供しません。なお、脅威対策の評価を目的としたサード パーティ製生体認証システムのテストは、この分析の対象範囲外です。ただし、サード パーティ製システムを利用すると、オペレーティング システムは特定の生体認証プロバイダーの保証とユーザビリティのレベルの影響を受けます。

テストのスコア

ID 管理	SAL	ユーザビリティ
Windows 10	**89**	**93**
macOS	**59**	**70**

Windows 10 は、認証に関連する測定可能なすべての機能で、macOS よりも高いスコアを記録しました。Windows 10 は、パスワードもトークンのようなセカンダリ デバイスも必要としない 2 要素ドメイン認証を提供します。さらに、ローカル認証向けにドメイン アカウントをサポートします。Windows 10 Enterprise の場合は、キーがハードウェアに格納されます。これにより、アクセスが制限され隔離された仮想コンテナーに認証資格情報が格納され、追加の保護レイヤーが提供されます。Windows 10 は、FIDO を含む最新の認証方式をサポートする統合フレームワークを提供します。Windows 10 の生体認証は、強力なスプーフィング対策保護も行います。macOS の ID 管理システムは、単純な方式を使用した悪質な意図に対する保護以外のセキュリティ保証レベルを備えていません。サード パーティ ツールがサポートされていなければ、企業向けの認証システムとしては不適切です。

情報保護

データ損失防止では、データのライフサイクルに対応する 3 つの機能グループでデータを制御するように定義されています。その 3 つとは、デバイスや他の形式のメディアに格納されているデータを指す DAR、ユーザーと情報共有手段の間で共有されているデータを指す DIT、デバイス上のアプリ、ドキュメント、システム メモリ内にあり、作成または操作されているデータを指す DIU です。どのようなデータ保護戦略でも、制御はできるだけデータの近くに配置されます。最も効率的なデータ保護手法は、制御をデータ上に配置する方法、次いで管理アプリ上に配置する方法、デバイスおよびネットワーク上に配置する方法です。これらすべての場所に制御を配置すれば、データのライフサイクル全体にわたる包括的な管理を行うことができます。

ストレージの保護 (DAR)

デバイスの紛失、盗難、不正使用に起因する機密情報の損失や侵害を防止する主要な手段として、暗号化が使用されます。暗号化に使用される暗号化キーは、ソフトウェア、ファームウェア、またはハードウェア内の保護された場所に格納する必要があります。最も高度な保護を提供するのはハードウェアです。改ざん防止機能付きハードウェアも暗号化処理によく使用されています。

Windows 10 は、OS、データ ストレージ パーティションを含むディスク全体を暗号化する BitLocker を備えています。BitLocker は、ポリシーで指定されている場合やユーザーが Windows 設定で有効にしている場合に、自動的に暗号化を適用します。Windows 10 は、デバイスのパフォーマンス低下を回避するために、プロセッサ拡張機能を使用して暗号化を高速化します。Windows 10 Enterprise は 128 ビットおよび 256 ビットの XTS-AES をサポートしており、暗号化されたテキストを操作してプレーン テキストに予測可能な変更を発生させるタイプの攻撃からも暗号を保護します。

macOS の FileVault 2 フル ディスク暗号化機能は、128 ビット XTS-AES 暗号化を使用して起動ディスクとユーザーのホーム ドライブを暗号化します。すべての FileVault 承認済みユーザーのホーム ディレクトリが、macOS の既定の構成である起動ディスク以外のボリュームにある場合、FileVault 2 は機能しません。ディスクへのアクセスが許可されているすべてのユーザーは、認証されるとドライブ全体にアクセスできます。また、FileVault 承認済みユーザーは、最初のログインだけで暗号化の解除も行うことができます。FileVault 2 は、キー保護のために専用ハードウェアを使用しません。攻撃者は、物理的にデバイスにアクセスできれば、パスワード ハッシュを抽出し、オフラインでブルート フォース攻撃を実行して暗号化用のパスワードを復旧できます。復旧には、Apple で保管されている (3 つの質問でのみ保護) か、ユーザーが指定した場所に格納されたファイルとして保管されている 24 文字のパスワードが使用されます。

通信の保護 (DIT)

DIT 制御の目的は、ユーザーがデバイスと信頼される企業リソースや企業アプリとの間で、保護された接続を確立できるようにすることです。通常は VPN が使用されます。VPN のメ

リットは、デバイスのインターネット接続を暗号化してリモートから企業に安全にアクセスできることです。VPN を使用するとネットワーク パフォーマンスに影響がありますが、最新のネットワークでは感知されない程度です。一方で、VPN アクセスを使用すると、組織のリソースがデバイス上の他のアプリに不必要に公開されてしまいます。そのため VPN アクセスは、特定のアプリにアクセスを限定するようにきめ細かく設定できる必要があります。

Windows 10 は、次の 2 つのタイプの VPN 接続を提供する VPN プラットフォームを備えています。

- インボックス プロトコル
  - IKEv2、PPTP、L2TP (L2TP は PSK と証明書の両方) をベースとした VPN がサポートされています。
  - インボックス VPN は認証に EAP を使用します。以下の EAP メソッドがサポートされています。
    - MSCHAPV2
    - TLS (Windows Hello、仮想スマート カード、証明書などの証明書ベース認証を使用)
    - TTLS (外部メソッド)
      以下の内部メソッドを使用できます。
      - PAP/Chap/MSCHAP/SCHAPv2
      - EAP MSCHAPv2
      - EAP TLS
    - PEAP
      以下の内部メソッドを使用できます。
      - EAP MSCHAPv2
      - EAP TLS
- TLS/SSL 向け VPN プラグイン プラットフォーム
  - サード パーティ開発者は、VPN プラグイン プラットフォームを使用して、ストアからダウンロード可能な VPN アプリを作成できます。現在ストアでは、Pulse Secure、Cisco、SonicWALL、Check Point、MobileIron、F5 製のアプリが提供されていますが、2016 年後半にさらに多くのアプリがリリースされる予定です。

Windows 10 は、VPN 接続の簡略化と保護のために、多くのオンデマンド手法と強制適用手法をサポートしています。「常時オン」では、ユーザーがスマートフォンの電源を入れたときやネットワークに変更があったときに自動的に VPN 接続が行われます。「ロックダウン VPN」は、VPN トンネルを介したネットワーク トラフィックのみを許可することでポリシーを強化します。「アプリ トリガー VPN」では、アプリの起動時に自動的に接続が開始されます。「トラフィック フィルター」を利用すると、アプリごとに動作を管理できるため、許可されたアプリからのトラフィックのみを VPN に転送できます。またトラフィック フィルターは、追加レイヤーとして、ホスト宛先属性に基づいてトラフィックをフィルターすることができます。ルールは、アプリ ベースとトラフィック ベースの両方を指定できます。

macOS には、L2TP over IPSec と PPTP をサポートするユニバーサル VPN クライアントが含まれています。どちらのプロトコルもデジタル証明書と、RSA または CRYPTOcard のワンタイム パスワード トークンを認証に使用できます。また、L2TP VPN クライアントは、Kerberos 認証と VPN オンデマンドをサポートしています。このクライアントは、Cisco Group Filtering と DHCP over PPP もサポートしています。アプリに関して言うと、macOS はアプリごとの VPN 接続をサポートしています。

作業中のデータ保護 (DIU)

作業中のデータ保護の目的は、個人のアプリやサービスとの企業データの共有を制限し、データ損失を防止することです。この目的は、データの暗号化、アプリ管理、セキュア コンテナーなど、複数の方法で達成できます。この 3 つの方法の中で、システム リソースとユーザビリティに与える影響が最も小さいのは、データ暗号化です。セキュア コンテナーとアプリの分離は影響が大きくなります。アプリ内の企業データを管理する手法に加え、メモリ内のデータを保護されたメモリ領域で実行することも必要です。

Windows 10 の Windows Information Protection (WIP) は、きわめて効率的にデータを保護する手段を提供します。WIP は OS に統合されているため、セキュア コンテナーを利用する必要も、アプリを複製する必要もありません。WIP は定義済みの企業ポリシーに基づいてデータを動的に暗号化します。アプリの種類にかかわらず、企業データの管理に焦点を当てることにより、個人のユーザー エクスペリエンスに影響を与えずに、企業データの可視性と制御を実現します。WIP は、データとアプリを個人用か業務用に分類し、ビジネス データにアクセスできるアプリを判断できます。この分類によって、どのデータを暗号化し、ユーザー間でどのように共有するかも決定されます。AppLocker は、MDM で使用される構成サービスの一部であり、許可するアプリと許可しないアプリを指定できます。アプリの分類は AppLocker によって管理されるので、SDK を使用したアプリの修正やアプリ ラッピングは不要です。管理者が企業情報をワイプするときも、分類されたアプリをデバイスに追加または削除する必要はありません。また、WIP によって既存の個人アプリやデータに変更が加えられることもありません。

信頼されたアプリとは、業務で使用できるように指定され、保護されている業務データと個人データにアクセスできるアプリです。信頼されたアプリのリストに含まれないアプリは、デバイスや社内共有に格納されている企業情報にアクセスできません。企業情報は、USB ドライブや個人のクラウド ストレージ アカウントなどの信頼されない場所に保存されると、暗号化されたままになります。また、キーは組織で制御されているため、ユーザーが退職する際には無効化され、ユーザーはデータの格納場所にかかわらずデータの暗号を解除できなくなり、組織のリソースにリモートからアクセスすることも不可能になります。WIP の重要な機能の 1 つは、Windows 10 アプリ (People (連絡先)、Outlook など) が個人データと業務データの両方を同時にサポートできるようにし、業務データには必要な制御や暗号化を提供できることです。たとえば、Microsoft Word の業務用ドキュメントではコピーと貼り付け操作を制限し、個人用ドキュメントでは共有を許可することができます。

IT 部門は WIP を使用して、企業リソースにアクセスするデバイスに次の 4 つの保護レベルを設定できます。

- **ブロック:** WIP は不適切なデータ共有を検出すると、ユーザーによる操作を停止します。
- **オーバーライド:** WIP は不適切なデータ共有を検出すると、操作のポリシー違反についてユーザーに警告します。この保護レベルでは、ユーザーはポリシーを無視してデータを共有でき、その操作が監査ログに記録されます。
- **サイレント:** WIP はサイレント モードで実行されます。ユーザーが不適切な操作を行うと、データを暗号化してログに記録しますが、ユーザーへの通知や操作のブロックは行いません。
- **オフ:** WIP がオフになり、デバイス上のデータは保護されません。

企業は、許可されていないデータ共有 (コピーや貼り付けなど) を完全にブロックするか、監査下での共有を許可するかを選択できます。監査下での共有を許可する場合、ユーザーは WIP 定義の制限をオーバーライドできますが、ユーザーが未許可のデータ共有を試みると、警告がユーザーに表示され、EMM システムによってこの行動がログに記録されます。ユーザーは、この操作を続行するかキャンセルするかを選択できます。新しいドキュメントを作成する際、許可されているアプリ内では、分類を業務用から個人用に手動で変更できます。新しいドキュメントを個人用に分類すると、企業のドキュメントからこの新しい個人用ドキュメントに情報をコピーして貼り付けることはできません。分類イベントはログに記録され、レビュー対象になります。

Office 365 にバンドルされている Microsoft Rights Management (RMS) を使用して、WIP の機能を拡張できます。印刷の許可、ドキュメントや電子メールの転送制御などの RMS による制御を使用して、WIP のアプリ制御、コピーと貼り付けの制御を補完できます。こうした制御は、Windows 10 に加え、macOS を含むその他のオペレーティング システムにも拡張できます。

macOS には、ファイル システム アクセス制御以外に、データ管理のためのネイティブのデータ保護機能がありません。データ管理に対応するには、サード パーティ製管理テクノロジへの投資が必要になります。マイクロソフトでは、macOS 上の Office 365 向けに RMS ドキュメント管理機能を提供しています。

テストのスコア

情報保護	SAL	ユーザビリティ
Windows 10	**95**	**100**
macOS	**57**	**81**

Windows 10 は、暗号化にハードウェア セキュリティ モジュールを使用すること、また WIP を通じてセキュア コンテナーやアプリのラッピングを必要とせずにビジネス データを管理できることから、情報保護の面で macOS よりも優れていると言えます。macOS は、ハードウェア ベースの暗号化管理機能を備えておらず、ネイティブなデータ管理機能も提供しません。macOS でビジネス情報を安全に管理するには、エンタープライズ クラスのデータ保護機能に対して追加投資を行う必要があります。

脅威対策

どのようなシステムであっても、欠陥がなく、あらゆる外部の脅威から保護されていると考えるのは現実的ではありません。攻撃者は、マルウェアを使用して脆弱性を悪用し、デバイスを感染させます。その手段となるのが、プログラムのエラーと、意図された機能です。プログラム エラーは、攻撃者がアクセス制御を回避して不正なコードをシステムに送り込む手段を提供するため、攻撃者はリモートからシステムにアクセスできるようになります。こうした不正コードは、その後このエラーを悪用して他のマルウェアをダウンロードして実行し、ネットワーク内のシステムに伝搬します。意図された機能は、意図されない用途で使用されてしまいます。たとえばブラウザーは、ローカル オペレーティング システムでのコードの実行を許可します。この手段によって、ウイルスやワームなどの脅威がシステムへのリモート アクセスを取得できるようになります。

セキュリティ侵害されたシステムにおけるデータ損失とマルウェア伝搬の影響を低減するために、オペレーティング システムは回復力を備えるだけでなく、新しいアプリや不明のアプリから、デバイスのディスクやデバイスで実行中のアプリに格納されたファイルへの広範なアクセスや完全なアクセスが不当に取得されないように設計されている必要があります。

デバイスの整合性

Windows 10 デバイスは、セキュア ブート付きの Unified Extensible Firmware Interface を通じ、デバイス、ファームウェア、ブートローダーの整合性を検証します。すべてのブート コンポーネントには、暗号によって検証済みのデジタル署名が含まれているため、承認済みのコードだけがデバイスの実行と初期化、Windows オペレーティング システムの読み込みを行うことが保証されます。このプロセスによって、デバイス ハードウェアやファームウェアから OS にまで拡張される信頼チェーンのルートが確立されます。

OS ローダーの起動後、トラスト ブートによって残りの Windows ブート関連コンポーネントの信頼性と整合性が検証されます。続いて、Windows カーネルが Windows スタートアップ プロセスの他のすべてのコンポーネント (ブート ドライバー、スタートアップ ファイルを含む) を検証します。改ざんされたファイルがあればトラスト ブートが検出し、Windows の起動前に既知の有効な構成への復元を試みます。

トラスト ブートを実行するには、OEM ドライバーやウイルス対策ソリューションなど、オペレーティング システム内のすべてのコードにマイクロソフトの署名が必要です。これがもう 1 つの整合性検証レイヤーとして機能します。すべての Windows 10 アプリには、Windows ストアまたは信頼されたエンタープライズ ストアのデジタル署名が必要です。

マイクロソフトは、「メジャー ブート」という 2 つ目のハードウェア支援プロセスによって、1 つ目の整合性検証プロセスを拡張します。メジャー ブートでは、TPM ハードウェアを使用して、ファームウェア、Windows ブート コンポーネント、ドライバーなどの重要なスタートアップ関連コンポーネントのベースラインを測定します。TPM は、ベースライン データを切り離して、改ざん攻撃から保護します。Windows 10 は、条件付きアクセスのシナリオで、このベースライン データと共に追加のセキュリティと構成基準を活用します。条件付きアクセスでは、Windows 正常性構成証明 (DHA) クラウドベース サービスをデバイ

スの完全な整合性を証明する手段として利用します。DHA サービスを使用する管理システムは、このチェックに基づいてリソースへのデバイス アクセスを許可または拒否します。この機能は、高度でない整合性制御を回避できるルート化されたデバイスを検出するうえで特に重要です。

macOS には、あらゆる整合性検証の基盤となるハードウェアの信頼のルートが存在しません。ブート プロセスに関しては、ファームウェアのパスワードによって、攻撃者がブート プロセスを変更することは困難になりますが、物理的にデバイスにアクセスできれば侵害するのは簡単です。

macOS では、アプリの署名を使用して ID と整合性を検証できます。すべてのネイティブ macOS アプリは Apple によって署名されています。開発者は、各自のアプリにデジタル署名するための一意の開発者 ID を Apple から付与されます。macOS のペアレンタル コントロール、管理対象設定、キーチェーン、ファイアウォールでは、アプリケーション署名を使用して管理対象アプリケーションの整合性 (キーチェーンの資格情報の要求など) を検証します。ペアレンタル コントロールと管理対象設定では、署名を使用して、アプリが変更されずに実行されていることを確認します。アプリケーション ファイアウォールは、署名を使用して、ネットワークへのアクセスを提供されているアプリの整合性の特定と検証を行います。ペアレンタル コントロールとファイアウォールの場合、システムはアドホック ベースでアプリに署名してアプリを識別し、変更されていないことを検証します。

システム整合性保護は、ルート アカウントに制約を課し、ルート ユーザーがシステム レベルおよび macOS ファイル システム内のネイティブ アプリ ディレクトリで実行できる操作を制限します。また、特定のプロセスからシステム レベル プロセスへの接続も防止します。その目的は、macOS への悪質なコードの侵入を阻止することです。システム整合性保護は、Apple によって署名され、システム ファイルへの特別な書き込み権限を与えられたプロセス (Apple ソフトウェア アップデートや Apple インストーラーなど) に対してのみ、保護されている部分への変更を許可します。Mac App Store からダウンロードするアプリは、既にシステム整合性保護に対応しています。これらのシステム レベル ディレクトリを呼び出す一部のアプリ、ユーティリティ、スクリプトは、sudo 権限があっても、ルート ユーザーが有効化されていても、管理者アクセスが許可されていても、機能しません。

アプリの保護

Windows 10 では、すべてのアプリとオペレーティング システムの一部が、AppContainer と呼ばれる専用の分離されたサンドボックス内で実行されます。AppContainer のセキュリティ ポリシーでは、AppContainer 内からアプリがアクセスできる機能が定義されています。その機能とは、地理位置情報、カメラ、マイク、ネットワーク、センサーなどの Windows 10 デバイス リソースです。アプリは互いに分離されており、事前定義された通信チャネルとデータ型を使用してのみ相互に通信できます。

多くの不正コードとマルウェア攻撃は、メモリ内のどこに特定のプロセスやシステム関数が存在するかを把握しなければなりません。Address Space Layout Randomization (ASLR) 機能は、実行可能コード、システム ライブラリ、関連プログラミング構成要素のメモリ アドレスをランダム化することで、不正コードによってコードとデータの場所が把握される可能

性を低減します。マイクロソフトでは、Windows 10 の ASLR 実装を以前のバージョンよりも強化しており、メモリ空間の予測がさらに難しくなっています。TPM を活用すると、デバイス間での ASLR メモリのランダム化の一意性が高まり、あるシステムで機能している不正コードが別のシステムで機能することは困難です。ASLR はアプリ向けの機能ですが、Windows 10 は OS 全体に ASLR を適用してサンドボックスが回避されるリスクを低減します。

Windows 10 には、ユーザーが書き込み可能なメモリ領域に配置されたコードの実行を拒否するデータ実行防止、保護されたランダム ヒープ メモリ割り当て、メモリ管理アルゴリズムが実装されています。この一連のテクノロジによって、脆弱性が悪用の成功につながる可能性をさらに低減しています。こうした防御メカニズムに対抗するために、攻撃者は Return Oriented Programming (ROP) を通じて、システムで既に使用可能なコードを利用します。Windows 10 は OS として初めて、メモリに読み込まれたアプリの制御フローを強制的にロックダウンする、制御フロー ガード (CFG) と呼ばれる手法を実装しました。CFG はブラウザーにとって非常に重要な機能です。Microsoft Edge では CFG が有効になっています。これらの一連のテクノロジには、世界で最も多くの企業とコンシューマーに使用されている OS である Windows プラットフォームが数十年にわたって繰り広げてきたマルウェアとの戦いの経験と成果が活かされています。

Microsoft Edge は、AppContainer ベースのサンドボックスを使用して脆弱性からシステムを保護します。Microsoft Edge は、Microsoft ActiveX、Java、Silverlight、ブラウザー ヘルパー オブジェクトなどの従来のバイナリ拡張を実行しないため、リスクが大幅に低減されます。SmartScreen は、フィッシング対策 URL フィルターを提供するほか、アプリケーション評価を使用してダウンロードをチェックし、ドライブバイ攻撃の防止にも効果を発揮します。SmartScreen は、サイトで悪質なコンテンツを検出したとき、そのサイト自体をブロックでき、状況によってはページ内の特定のコンテンツのみをブロックすることもできます。

macOS のサンドボックスでは、カーネル レベルで実装されている強制アクセス制御が使用されます。サンドボックス内で実行されるアプリごとにサンドボックス プロファイルが存在し、どのリソースがアプリにアクセス可能かが正確に記述されています。mDNSResponder (Bonjour の基盤ソフトウェア) や Kerberos KDC など、ネットワークと日常的に通信するシステム ヘルパー アプリの多くはサンドボックス化され、システムにアクセスしようとする攻撃者の不正行為から保護されています。また、信頼されていない入力 (任意のファイルやネットワーク接続など) を定期的に受け付けるその他のプログラム (Xgrid、クイック ルック、Spotlight のバックグラウンド デーモンなど) もサンドボックス化されています。

64 ビット チップ上で動作する macOS は、メモリと実行可能ファイルの保護をサポートしています。メモリと実行可能ファイルの保護によって、特定のタイプの悪質なソフトウェアは、メモリ割り当てや実行方法を悪用してプロセッサに他のプロセスのメモリ領域から任意のコードを実行させることができなくなります。また XD (実行無効化) 機能により、データ用のメモリ領域と実行命令用のメモリ領域の間に強力な壁が形成されます。macOS は、カーネルによって使用されるメモリに ASLR が実装されています。macOS は、NX (no-

execute) スタック、NX データ、NX ヒープという 64 ビット保護機能も備えています。NX スタックは、32 ビット アプリと 64 ビット アプリで利用できます。64 ビット プロセスに対しては、macOS はヒープとスタック両方のデータ領域でコード実行防止機能を提供します。また、ライブラリのランダム化も行います。ライブラリのランダム化では、システムが起動するたびに変更される OS プロセスのメモリの場所を使用します。

Safari では、不正なサイトの検出機能が強化されています。また、セキュリティと安定性を高めるために、多くのブラウザー プラグインを独立したプロセスとして実行します。Safari、Mail、iChat は、ダウンロードされたファイルに、ファイル、URL、ダウンロードの日付と時間が含まれたメタデータでタグ付けします。ダウンロードの検査担当者は、このメタデータを使用して悪質なタイプのファイルが意図せず開かれるのを防ぎます。Safari には、Google が提供する既知および疑わしいマルウェア転送サイトとフィッシング サイトのブラックリストを使用して、不正サイトを検出する機能も搭載されています。さらに Safari は、拡張機能の管理と、ブラウザー上での不必要なコード実行の無効化を、完全に制御することができます。

テストのスコア

脅威対策	SAL	ユーザビリティ
Windows 10	**100**	**100**
macOS	**86**	**90**

Windows 10 は、macOS よりも優れた 2 つの脅威対策を提供します。まずはリモート正常性構成証明です。ハードウェアの信頼のルートを使用することにより、ルート化されたデバイスの強力な検出など、現在のデバイスの状態に応じて、信頼された企業ネットワークへの条件付きアクセスをデバイスに提供します。もう 1 つは CFG などの新しいメモリ保護機能で、攻撃者によるメモリ攻撃を通じたシステムの侵害を防止できます。これらの機能はどちらもエンド ユーザーに対して透過的に実行されますが、アクセスが拒否された場合にはユーザーに通知されます。

管理とレポート

個人所有デバイスの使用が一般化しているモバイル領域とは異なり、デスクトップは通常、企業所有の管理対象デバイスです。ノート PC は個人所有の割合が増加している一方で企業所有も混在しており、その大半は MacBook が占めています。このような各種カテゴリ内では、さらに管理要件は組織によって大きく異なります。ごく軽度な管理で済むデバイスもあれば、きめ細かい制御が必要なデバイスもあります。

マイクロソフトは、System Center Configuration Manager の非常にきめ細かい制御機能を通じて、macOS 環境では比較的新しい機能であるデスクトップおよびノート PC の管理機能を長年にわたって提供しています。これらのツールは、多くの組織に数十年もの間利用されており、Windows 10 にもこれまでどおりに搭載されたに過ぎません。

Windows デバイスには昔から管理機能が装備されており、Windows 10 にもその機能が受け継がれています。Apple は、2011 年に Lion (macOS 10.7) リリースで macOS に API ベースの管理機能を追加しました。そして今度はマイクロソフトが Windows 10 にその機能を追加しました。管理 API は Windows 10 に組み込まれていますが、System Center Configuration Manager で macOS デバイスをサポートするためのダウンロードも提供されています (ただし、macOS 10.11 (El Capitan) はまだサポートされていません)。

マイクロソフトは、グループ ポリシー、AD、System Center Configuration Manager などのテクノロジを通じて、強力な管理とセキュリティの機能も提供しています。「モバイル ファースト」、「クラウド ファースト」の環境向けには、Microsoft Enterprise Mobility Suite のクラウド ベース デバイス管理ソリューションを使用する最新のシンプルな管理機能を提供しています。これらの機能は、Microsoft Intune、Azure AD、Azure Rights Management Service、Office 365、ビジネス向け Windows ストアなどのクラウド サービスによって補完されています。

デバイスの登録

管理ツールの最新バージョンは、Windows 10 を実行するあらゆるタイプのデバイスを管理できます。グループ ポリシー、Windows Management Instrumentation、PowerShell スクリプト、Orchestrator Runbook、System Center ツールなどの既存のエンタープライズ管理ツールは、引き続き PC 上の Windows 10 で使用できます。Windows 10 を実行するデバイスにも、デバイスの登録と管理のために MDM エージェントが組み込まれています。MDM ベンダーは、Windows 10 デバイスとの通信に Microsoft MDM プロトコルを使用し、Windows 10 デバイスは Open Mobile Alliance の Device Management プロトコル 1.2.1 をサポートしています。MDM クライアントは、ポリシー設定の構成、アプリと更新プログラムの展開、その他の管理タスクの実行を MDM に許可します。MDM は、MDM クライアントを通じて構成要求を送信し、インベントリを収集します。

macOS デバイスの場合、MDM は Apple Push Notification Service (APNS) を使用して公衆ネットワークとプライベート ネットワークの両方でデバイスとの永続的な通信を維持します。MDM では、デバイスと通信するための APNS 証明書、安全に通信するための SSL 証明書、構成プロファイルに署名するための証明書など、多くの証明書が必要です。組織は、毎年 APNS 証明書を更新する必要があります。証明書が失効すると、MDM ソリューションは組織が証明書を更新するまで Apple デバイスと通信できなくなります。

個人所有の Windows 10 デバイスには、職場の Microsoft アカウントを使用します。これは企業による管理とリソース アクセス専用のデバイスのサブ アカウントとして機能します。企業所有デバイスは、プライマリ デバイス認証としてドメイン アカウントを使用して企業に登録されます。Azure AD との統合によって、メール、Word、OneDrive、Azure AD Web アプリを含むネイティブ アプリへのシングル サインオンが可能になります。また Azure AD に参加することで、オンプレミス リソースへのシングル サインオンと、ビジネス向け Windows ストアの認証も可能になります。管理者がプロビジョニング パッケージを作成し、適用してからデバイスをユーザーに配布することも、ユーザーが初期構成時にプロビジョニング パッケージを適用することもできます。

macOS は、MDM のプロビジョニング パッケージをサポートしており、電子メールの添付ファイルまたは Web ページのダウンロードを介して配布できます。また macOS の MDM では、暗号化署名、プロビジョニング パッケージの暗号化、パスワード ベースのユーザー アクセスがサポートされています。MDM では、メールやその他のユーザー アカウントを自動的にセットアップできます。ユーザー名、メール アドレス、認証と署名のための証明書 ID もアカウント ペイロードにあらかじめ入力しておくことができます。macOS デバイスは、通常 Simple Certificate Enrollment Protocol を使用して組織のサービスの認証用に一意の ID を作成します。一方で、Windows 10 の単一ステップによる MDM 検出、プロビジョニング、登録と同様のメリットが得られるように、macOS は、Microsoft Certificate Authority (DCE/RPC を使用)、Active Directory 証明書プロファイル ペイロード、AD 認証の使用をサポートしています。

デバイス構成

Windows 10 では、組み込みの MDM クライアントを使用することで、MDM で管理された制限を複数の項目に適用できます。MDM では、デバイス パスコードの要求と要件の指定、内部ストレージ暗号化の強制、SD カード使用の有効化と無効化、開発者アンロックの無効化を行うことができます。また MDM によって、モバイル データとデータ ローミングにおける VPN の許可、ActiveSync 設定の構成と配布、ルート証明機関 (CA) や発行者証明書など各種証明書の構成も実行できます。さらに、カメラ、Cortana、位置情報データ、利用統計情報、Bluetooth、インターネット共有、Microsoft アカウント以外のアカウントの追加の制限に加え、検索での位置情報の使用の禁止、Microsoft アカウントの接続認証の拒否、複数のデバイス間での [設定を同期] の禁止、Windows ストア以外のアプリの制限などもサポートされています。

macOS は、デバイスの MDM プロファイルをサポートしています。macOS では、このプロファイルを通じて、MDM にセキュリティ ポリシーのプロビジョニング、企業アカウントへのアクセスの提供、証明書の管理、ノート PC 設定の構成を許可します。MDM プロファイルを使用して、パスコードと暗号化の要件の設定、Wi-Fi アダプターとイーサネット アダプターの構成、ネイティブ メール アカウントと Outlook アカウントの管理、ネットワーク プリンターの構成、ソフトウェア更新の防止、ドックと壁紙設定によるユーザー エクスペリエンスのカスタマイズも実行できます。プロファイルは時間ベースの設定も可能で、自動的に、またはオンデマンドで展開するように構成できます。

アプリケーション管理

Windows 10 は、アプリの展開のためにビジネス向け Windows ストアのサブスクリプションと MDM の統合をサポートしています。MDM システムを使用してデバイスに基幹業務 (LOB) アプリを直接展開するには、すべてのソフトウェア パッケージが証明機関によってデジタル署名されている必要があります。企業は最大 20 個の自己署名付き LOB アプリを Windows 10 Mobile デバイスに配布できます。組織のデバイスが Windows 10 Mobile Enterprise を実行していれば、20 個以上のアプリを配布できます。Windows 10 の WIP で、許可するアプリと許可しないアプリを指定し、アプリ ラッピングやアプリの変更を必要とせずにアプリの分類を管理できます。管理者は、企業情報をワイプするときも、分類され

たアプリをデバイスに追加または削除する必要がありません。WIP によって既存の個人アプリやデータに変更が加えられることはありません。アプリ管理では、Windows ストア、プライベート ストア、自動更新、サイドローディングを制限したり、同一アプリで複数のユーザーがデータを共有したりすることも制限できます。

管理対象アプリの配布のために Apple Volume Purchase Program (VPP) と統合すると、MDM を通じて、商用企業アプリと LOB アプリをアップロードし、macOS に配布できると共に、アプリの説明、イメージ、カテゴリを定義することもできます。MDM では、アプリを配布することも、ユーザーがデバイスの登録を解除したときにアプリを削除することも可能です。Apple によって検証され、デジタル署名された商用アプリは App Store から入手できます。ユーザーが個人的に使用するアプリを Apple Store からインストールしないように制限することはできません。Apple ID で購入されたアプリは、同一の Apple ID で構成されている他の macOS デバイスでも使用できます。

リモート管理

MDM は、Windows 10 デバイスに、ハードウェア インベントリ、デバイス名、ユーザー名、メール アドレス、オペレーティング システムとバージョン、証明書、位置情報、Wi-Fi MAC アドレス、デバイス ID、所有者の指名、基本入出力システム、画面の解像度、OS の言語、Windows ストア アプリとそれ以外のアプリのインベントリを照会できます。

macOS デバイスでも、ハードウェアのシリアル番号、デバイス名、Wi-Fi MAC アドレスなど、同様のさまざまな情報を照会できます。また、デバイスのバージョンと制限事項、デバイスにインストールされたアプリのリストなど、ソフトウェア情報も照会できます。

Windows 10 には、Windows 10 as a Service という、過去の Windows リリースよりも速いペースで OS 機能の更新を提供するモデルが導入されています。以前は、新しい Windows が 3 年ごとにリリースされてきました。現在はリリースの頻度が高くなり、絶えず進化するセキュリティの脅威に対処すると共に、定期的に新しい機能を求めるユーザーの期待に応えることを目的としています。マイクロソフトは、定期的に更新プログラムを提供し、新機能も継続的にリリースする予定です。Windows 10 は Windows Update から直接ソフトウェア更新を取得します。Windows 10 Enterprise では、広範囲のユーザーに配布する前に、企業が更新プログラムの選定と検証を行うことができます。

Apple はソフトウェアやセキュリティの更新スケジュールを公開していませんが、通常は定期的に macOS のメジャー バージョンの更新を行っています。macOS は、リモート更新の手法やセキュリティ更新プログラムのみを取得する手法を提供していません。

デバイスの紛失または盗難が発生した場合、Windows 10 では MDM を通じてデバイスの検索と階層リンク履歴の確認、盗難/紛失/非準拠デバイスの選択的ワイプまたはフル ワイプ、デバイスの手動での使用停止の制限を行うことができます。macOS は、リモートからのデバイス ロックをサポートしています。macOS をロックすると、デバイスがシャットダウンされ、EFI パスコードがインストールされるため、パスコードを入力しないと起動できなくなります。macOS デバイスのワイプを実行すると、すべてのユーザー データが削除されます。

診断と監視

Windows 10 は、問題の追跡や修復操作の実行に役立つ監査情報を提供します。この情報により、デバイス構成を組織の標準に準拠させることができます。Windows 10 のリモート デバイス正常性構成証明は、測定されたブート データを使用してデバイスの正常性状態を検証します。MDM はこの正常性状態を活用し、クライアント ポリシーと関連付けて、デバイスの現在の状態に基づいて条件付きアクセスを許可します。デバイスは、マルウェアに感染していないこと、セキュリティ ツールがアクティブであること、最新のパッチ レベルまで完全に更新されていることを証明する必要があります。証明できなければ、指定のリソースへのアクセスが拒否されます。

macOS では、同様のリモート構成証明機能を提供していません。管理者による macOS ログの監視は、デバイス上でローカルで行うか、サード パーティ製のリモート管理ツールを使用する必要があります。

マイクロソフトは、Windows 10 の利用統計情報を定期的に収集しています。利用統計情報は、Connected User Experience and Telemetry コンポーネントによってアップロードされるシステム データです。これは、基本的には OS の診断とユーザー エクスペリエンスの向上のために使用される匿名データです。Windows 10 Mobile で利用統計情報機能を無効にするには、Windows 10 Mobile Enterprise エディションにアップグレードする必要があります。Windows 10 Mobile Enterprise では、企業は、「セキュリティ」レベルなど、サポートされる 4 つのレベルで利用統計情報を構成できます。「セキュリティ」レベルでは、最新のセキュリティ更新プログラムで Windows デバイスの安全性を維持するために必要な利用統計情報のみが収集されます。Windows からマイクロソフトにデータが送信されないようにするには、Windows Defender 利用統計情報と悪意のあるソフトウェアの削除ツールのレポートを無効にし、Microsoft サービスへのその他のすべての接続を無効にします。

Apple にも、製品とサービスの向上に使用される匿名技術データを収集する機能があります。このデータは、デバイスとアプリに関する匿名情報を送信する診断および使用状況プログラムで使用されるオプトイン プロセスです。データを送信するにはユーザーが明示的に同意する必要があります。ユーザーはデバイス上で送信されるデータを確認でき、いつでも送信をやめることができます。

テストのスコア

管理	SAL	ユーザビリティ
Windows 10	**93**	**93**
macOS	**75**	**77**

macOS は、複数の構成オプションを提供する柔軟なオペレーティング システムですが、エンタープライズ プラットフォームとしては現在も開発段階にあります。総合的に見て、Windows 10 の方が企業向けのリモート管理をサポートする優れた機能を装備しています。

大半の MDM は企業ドメイン認証をサポートしていますが、Windows 10 ではドメイン アカウントを使用して単一ステップでデバイスの検出、プロビジョニング、構成、管理を行うことができます。macOS では、まず構成ファイルを通じてデバイスの管理と構成を行う必要があります。そうすることで、ビジネス アプリがドメイン アカウント認証をサポートできるようになります。Windows 10 は、リモート正常性構成証明に基づいた条件付きアクセスも提供していますが、macOS にはこの機能はありません。Windows 10 は、はるかに包括的な企業アプリ管理機能と更新戦略を提供するだけでなく、管理エクスペリエンスも優れています。

結論

この分析ではセキュリティ保証とユーザビリティを主要な基準として測定し、その結果 Pique Solutions は Windows 10 の方が macOS よりもセキュリティ保証のレベルが高く、ユーザビリティに対する影響は低いと結論付けました。Windows 10 は、モバイル デバイス、タブレット、PC にコスト効率の良い 2 要素認証を提供し、ユーザー パスワードを排除して ID を保護することで、資格情報の盗難に起因する侵害発生のリスクを軽減しています。さらに重要なのは、Windows 10 では、ユーザーにとって透過的な方法で企業データが保護され、ユーザーは同一のアプリを個人的なタスクにも仕事にも使用できることです。また Windows 10 は、デバイスの正常性構成証明に基づいて企業リソースへの条件付きアクセスを提供します。Windows 10 は、デバイスの種類にかかわらず、統合された 1 つの OS アーキテクチャとアプリ開発プラットフォームを活用することで、重要なセキュリティ更新プログラムや修正プログラムの配布を含むデバイスとアプリのプロビジョニングを合理化しています。

macOS は高度なデスクトップ機能を備える柔軟なオープン プラットフォームを提供していますが、認証と暗号化のためのハードウェアの信頼のルートが存在せず、企業データの管理と保護を効率化するネイティブ機能もありません。さらに、現在 Apple のデスクトップやノート PC には、認証用の指紋センサーやその他の生体認証デバイスが装備されておらず、サード パーティ製のアドオンに依存しています。

Windows 10 は、認証に関連する測定可能なすべての機能で、macOS よりも高いスコアを記録しました。Windows 10 は、パスワードもセカンダリ デバイスも必要としない 2 要素ドメイン認証を提供します。さらに、ローカル認証向けにドメイン アカウントをサポートします。Windows 10 Enterprise の場合は、キーがハードウェアに格納されます。これにより、アクセスが制限され隔離された仮想コンテナーに認証資格情報が格納され、追加の保護レイヤーが提供されます。Windows 10 は、FIDO を含む最新の認証方式をサポートする統合フレームワークを提供します。Windows 10 の生体認証は、強力なスプーフィング対策保護も行います。macOS の ID 管理システムは、単純な方式を使用した悪質な意図に対する保護以外のセキュリティ保証レベルを備えていません。サード パーティ ツールがサポートされていなければ、企業向けの認証システムとしては不適切です。

Windows 10 は、暗号化にハードウェア セキュリティ モジュールを使用すること、また WIP を通じてセキュア コンテナーやアプリのラッピングを必要とせずにビジネス データを管理できることから、情報保護の面で macOS よりも優れていると言えます。macOS は、ハード

ウェア ベースの暗号化管理機能を備えておらず、ネイティブなデータ管理機能も提供しません。macOS でビジネス情報を安全に管理するには、エンタープライズ クラスのデータ保護機能に対して追加投資を行う必要があります。

Apple は攻撃からの回復力に優れているという評価が聞かれますが、macOS がその評判に値するかどうかははっきりとしていません。市場シェアが 10% に満たない macOS は、これまで Windows ほどの注目は集めていませんでしたが、最近 macOS に過去最大の数の脆弱性が発見されました。マイクロソフトは、長年にわたって攻撃に脆弱だという批判に耐えながら、製品やサービスが企業に広く普及しているために発生した非常に多くの攻撃と戦ってきました。

Windows 10 は、macOS よりも優れた 2 つの脅威対策を提供します。まずはリモート正常性構成証明です。ハードウェアの信頼のルートを使用することにより、ルート化されたデバイスの強力な検出など、現在のデバイスの状態に応じて、信頼された企業ネットワークへの条件付きアクセスをデバイスに提供します。もう 1 つは CFG などの新しいメモリ保護機能で、攻撃者によるメモリ攻撃を通じたシステムの侵害を防止できます。そして最も重要なのは、両方の機能がユーザーに対して完全に透過的に実行されることです。

豊富な資金を持つ攻撃者によって実際に執拗な標的型攻撃が仕掛けられている現在の環境では、デバイスの高度な SAL に関する要件として、基本的な企業セキュリティ機能を満たすだけでは十分と言えなくなりました。Windows 10 は、最も厳しいセキュリティ要件および企業管理要件を満たす回復性の高いデバイスを提供できます。しかも、エンド ユーザーにとって透過的に、生産性を低下させるどころか高める方法でこうした制御を実現します。