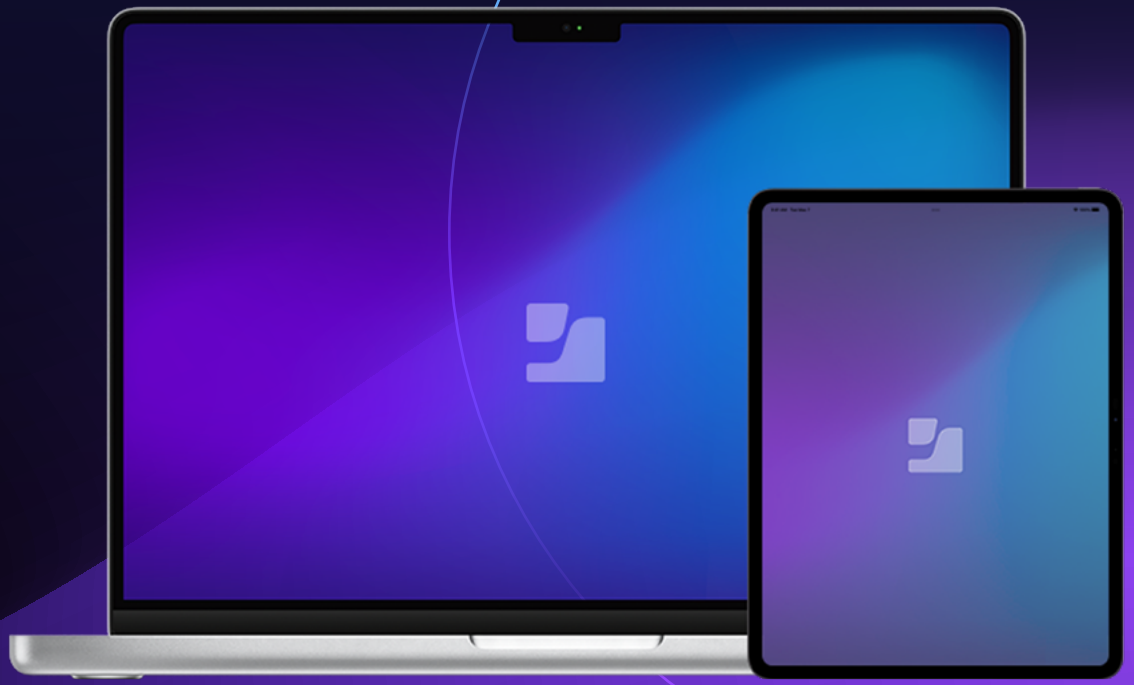
jamf



不確かなコンプライアンス確保：クロスプラットフォーム環境における

Appleセキュリティとコンプライアンス

はじめに

Macデバイスのコンプライアンスギャップは Windows デバイスのものと同じに見えますが、おそらくお使いのツールはそのギャップを確認できる設計になっていません。デバイスが混在する環境を相手にしているIT部門やセキュリティ部門は、一連の問題に繰り返し悩まされています。クロスプラットフォームコンソールではMacに関する報告がWindowsの概念に変換して行われ、誤検知（もっと悪い場合には検出漏れ）としてテレメトリギャップが表面化し、監査サイクルでは既存のツールに存在するApple製品固有の死角が露見します。

すべてを「単一の画面」にまとめたいと考えるのは当然の流れですが、多くの場合はその代償として、macOS、iOS、iPadOSのポリシーの適用方法に対応していない汎用的な制御フレームワークでApple セキュリティを管理することになります。

「Jamfが選ばれる理由」シリーズの第3弾となる本ガイドでは、そうしたトレードオフなしにこのギャップを解消する方法を説明します。MacおよびiOS/iPadOSネイティブのコンプライアンスメカニズムを利用する形でデバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティを統合する方法を見ていきます。管理層の主張ではなくデバイス自体によって署名された証拠を確保し、規模が拡大しても監査レポートを適切に用意し、IT部門が可視性とセキュリティを天秤にかける事態を廃止できます。

概要

ほとんどの企業向けコンプライアンスプログラムはWindows向けで、Appleデバイスは後回しにされていました。デバイスが混在する環境でコンプライアンスを確保する場合、この扱いの違いが原因でよく見られる非常に危険な失敗パターンに陥ります。それは、「グリーンダッシュボードの罠」です。すべてのエンドポイントはコンプライアンスが確保されていると報告し、すべての検査に合格し、すべての設定が問題なく完了していても、監査やインシデントによってMac、iPhone、またはiPadについて検証したとされていた項目が実はまったく検証されていなかったと判明するのです。

これは、IT部門の怠慢ではなく、アーキテクチャの問題です。別のオペレーティングシステム（OS）向けのツールは、macOS、iOS、iPadOSがセキュリティ状態を適用および報告するために利用する統合型のネイティブメカニズムにアクセスできないため、エンドポイントのテレメトリデータが欠如するか、得られたとしても不完全なものになります。そのため、主張は、証拠ではなく推測に基づくことになります。ダッシュボードも、監査人も、CISOもこの状況を把握できないため、リスクは静かに高まっていきます。

こうしたギャップを解消するには、デバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティを統合したAppleネイティブのコンプライアンス基盤が必要です。こうした基盤では、デバイスレベルの証拠で主張の裏付けを行い、監査での立証能力を全プラットフォームで確保し、デバイスでWindows、macOS、iOS、iPadOSのいずれが稼働していても同じ基準を適用できます。

Jamfが解決するコンプライアンスプログラムの課題

クロスプラットフォームツールにはAppleネイティブの制御機能がない：Jamfのソリューションはプラットフォームssoを介してMDM、宣言型デバイス管理、AppleのEndpoint Securityフレームワーク、Secure Enclave内の鍵に対して直接機能します。

アクセスの許可が検証済みのデバイスの状態ではなく、ユーザからの要求に応じて行われる：Jamfのソリューションは、デバイスの状態をOkta Device Trust、Microsoft Entra条件付きアクセス、Zscalerに結び付けるため、証拠ベースでアクセスが許可されます。

ダッシュボードは状態を報告しているが、監査人は証拠を求めている：スマートコンピュータグループによりデバイスがリアルタイムに分類されます。APIを利用してCSVをエクスポートすると、監査およびリスク管理システムに直接取り込まれます。

デバイス数が増加するにつれて標準構成が崩壊する：Jamfのソリューションは、MITRE ATT&CKにマッピングされた挙動分析を利用してベースラインを継続的に適用します。セキュリティ状態に逸脱があると、スマートグループポリシーが自動的に適用されます。

検証可能なベースラインがないため、「堅牢化」が主観にすぎない：mSCPをベースにしたJamfコンプライアンスベンチマークは、監視のみまたは強制モードでCIS、NIST 800-53/171、DISA STIG、CMMC 2.0、CNSSI-1253、Indigoに照らして評価します。

PCベースのツールがMacを見逃す理由

コンプライアンスツールの役割は1つです。それは、デバイスの真の状態を報告することです。PCベースのツールは、Windowsネイティブのメカニズム（レジストリクエリ、WMI、Win32 APIなど）に対応するよう設計されています。これらのメカニズムはAppleプラットフォームには存在しません。このツールをMacやiPhoneに使用した場合、かろうじて見つかった表層的なシグナルを利用することになり、結果として、主張は確からしく見えても不完全な証拠に基づいたものになります。

Apple製品では以下の3つの主要メカニズムが公開されており、コンプライアンスツールはこれらにアクセスする必要があります。

MDM（モバイルデバイス管理）：個々のデバイスやユーザチャネルをまたいで構成やポリシーの適用を実行します。その上にDDM（宣言型デバイス管理）が自律的できめ細かい制御を重層的に展開します。登録、プロファイル、ペイロードはすべてこのスタックを通過します。

ESF（Endpoint Securityフレームワーク）：プロセスの実行、ファイルシステムのイベント、認証などに関するリアルタイムのテレメトリを提供するApple製のユーザ空間APIです。Appleが発行した権限のもとでカーネルレベルの許可/禁止が適用されます。

Secure Enclave：メインCPUから独立した、Apple シリコン上の専用サブシステムです。不変のハードウェアによる信頼の基点をブートROM内に実装し、内蔵のAESエンジンで暗号化操作を実行し、専用のメモリ保護エンジンを介してメモリを保護します。

ここでミスマッチが生じます。PCベースのツールはMacでFileVaultが有効になっていることを報告できますが、FileVaultの暗号鍵がSecure Enclaveにハードウェアで紐付けされていることは検証できません。**これがアーキテクチャ由来のサイレントグリーンの原因です。**主張の検証に必要な証拠を構造的に収集することができないのです。

Jamfが選ばれる理由

Jamfは、Appleのエコシステム全体でmacOS、iOS/iPadOS、tvOS、watchOS、visionOSのネイティブ同日サポートの提供を続けているだけでなく、10年以上にわたってこの機能を一貫して提供しています。ベータリリースのサポートを確立することで、最新のオペレーティングシステム、機能、アップデートを、当社ではなくお客様のタイミングでテストできるよう支援しています。

デバイスの堅牢化とベースラインの適用

ベースライン自体が定義されていなければ、堅牢化は失敗します。立証可能なベースラインを用意するには、使用しているOSとバージョン、インストールされているアプリとその理由、利用しているクラウドサービス、役割ベースで許可されている権限、組織が満たす必要のあるガバナンス要件を盛り込む必要があります。このインベントリがなければ、「堅牢化」の基準は直近に関与した管理者の独断にすぎません。

ベースラインは規制だけでは確立できず、以下の段階分けが必須です。

- フレームワークで目標を設定する
- 基準で具体的な制御を定義する
- ベンチマークでベストプラクティスに照らしてパフォーマンスを測定する

基準とベンチマークはOSに依存します。コンプライアンスを策定、適用、文書化するには、各制御をネイティブに管理しているOSのメカニズムを調査する必要があります。

再度FileVaultの例を取り上げます。NIST SP 800-53 Rev. 5 control SC-28では、保存中の情報の保護について検証します。CMVP（Cryptographic Module Validation Program）では、FileVaultで使用されているmacOSの暗号化モジュールがFIPS 140-2/140-3（および国際的にはISO/IEC 19790と24759）に準拠しているか検証します。また、macOSのCISベンチマークでは、実際のデバイスの状態、つまりFileVaultがオンになっていて、無効化が禁止されているかどうかを検証します。対応する層は検証によって異なり、それぞれにmacOSへのネイティブアクセスが必要です。

PCベースのツールを使用している場合、ここで問題が起こります。ソフトウェアレベルの状態をまったく読み取ることができなかったり、FileVaultが有効になっていることはわかっても、鍵がSecure Enclave内に保持されているか確認できなかったりします。**どのような場合でも、監査責任は変わりません。**制御の状態を検証できないと、裏付けとなる証拠のないまま、コンプライアンスを確保できていると誤解してしまうことになります。

Jamfが選ばれる理由

Jamfコンプライアンスベンチマークは、mSCP（macOSセキュリティコンプライアンスプロジェクト）をベースにしています。Jamfのソリューションに含まれており、NIST、DISA STIG、CMMC、CISのベースラインに直接マッピングします。管理対象デバイスに目的の構成を適用し、基盤となる制御状態をタイムスタンプ付きで記録し、合否確認ではなく、セキュリティ部門が監査に対応するために必要となる検証可能な証拠を生成します。

ポリシーの継続的な適用によるコンプライアンスの自動化

監査は、ある1日のコンプライアンスを証明するものです。監査後、デバイスの状態は日々変化します。その間に立証は不可能になります。火曜日に監査に合格しても金曜日にはコンプライアンスから逸脱するケースや、何ヶ月も前からコンプライアンスから逸脱した状態が続いていたのにまったく気が付かないケースが起こり得るからです。

逸脱は常に起こります。設定はアップデートで変わり、管理者は変更を手作業で行い、脆弱性が表面化し、ユーザはユーザらしく振る舞います。エンドポイントの状態に関する継続的な証拠がないと、監査レポートは特定の瞬間を証明するだけで、残りのライフサイクルにおけるプロビジョニング、構成、監視、アップデート、廃棄は闇の中です。

Apple製品へのコンプライアンス適用で失敗が起きる領域は以下の3つです。

検査間のネイティブテレメトリがない。

PCベースのツールは、監査間のコンプライアンスを証明するAppleネイティブのシグナルを継続的に収集できません。インシデントが発生した場合や、監査人から審査対象期間全体の制御履歴を求められた場合、IT部門にできるのは前回の検査のタイムスタンプを示すことだけです。

MDMのチェックイン周期は過去のもの。*

MDMは定期的なチェックインを前提に設計されていますが、運用担当者はサーバ負荷を抑えるためにその間隔を広げるものです。間隔が広くなるとデータが古くなるので、インシデント対応を古い情報に基づいて手動で行うことになり、事後対応のセキュリティ態勢を余儀なくされます。

アイデンティティとセキュリティの運用をまとめてではなく、並行して行う。

コンプライアンス違反のデバイスが自分で申告することはありません。アイデンティティおよびアクセス制御においてデバイスの状態を絶えず監視できないと、コンプライアンス違反のエンドポイントが保護対象リソースにアクセスできる状態のままになり、そうしたアクセスがないと証明する監査証跡が記録されることはありません。

***今後の動向：Appleは従来のMDMモデルの廃止を進めている**
WWDC 2025で、Appleは従来のMDMのソフトウェアアップデートコマンド（ScheduleOSUpdate、OSUpdateStatus、com.apple.SoftwareUpdateペイロード）をiOS 26、iPadOS 26、macOS 26（Tahoe）で廃止すると発表しました。これらのメカニズムは26以降のOSリリースで削除されます。ソフトウェアアップデートは、MDMコマンドからDDMへの切り替えで廃止される最初の機能に過ぎません。これを皮切りに、DDMの成熟度合いに合わせて置き換えが進んでいきます。この移行はコンプライアンスプログラムに直接的な影響をもたらします。従来のMDMメカニズムはもはや安定した基盤ではなく、利用を続けることは推奨されません。

Jamfが選ばれる理由

Jamfのソリューションには、デバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティが1つのシステムとして統合されています。MDM、宣言型デバイス管理、Endpoint Securityフレームワーク、Secure Enclaveによって保護されたアイデンティティなどのAppleネイティブのメカニズムはテレメトリを継続的に提供します。そのため、過去、現在、および監査期間のエンドポイントの状態を確認できます。

パッチ管理とソフトウェア脆弱性対策

Appleの配信モデルには、緊急セキュリティ対応（RSR）、App Storeからの配布、OSの差分、メジャーアップグレードがあり、ネイティブチャネルであるMDM、宣言型デバイス管理、Apple Business Managerを通じて実行されます。クロスプラットフォームツールは、それらのチャネルの言語を着実に学んでいます。

流暢さはまちまちですが、次の3つの要因が「導入可能」と「監査で立証可能」を分かちます。

RSRの可視性とバージョンレポート：Appleの緊急パッチは、一刻を争う無防備な状態を解消するためのものです。難しいのは、それらを許可または禁止することではなく、組織内のデバイスへの適用状態を把握することです。デバイスごとのRSR固有の追加ビルドバージョンのインベントリ作成、全デバイスへの導入状況の可視化、コンプライアンスレポートへのそのシグナルの取り込みの各機能は現在、プラットフォームによって異なります。大半はRSRのオン/オフを切り替えられますが、何がどこに展開されたかを証明できるものはごくわずかです。

サードパーティアプリケーションの大規模なパッチ適用：App StoreアプリはVPPを介してアップデートされます。他のすべて（つまりブラウザ、生産性向上スイート、PDFツール、セキュリティエージェント）は、管理プラットフォーム自体で管理されます。審査済みのパッチをまとめたカタログがないと、新しいバージョンがリリースされるたびに管理者が手作業でアップロードすることになります。

監査対応の証拠：パッチを展開するのは難しいことではありません。課題は、各適用期間内に各エンドポイントにそれぞれのパッチがインストールされたことを証明するデバイスレベルの証拠をタイムスタンプ付きで生成することです。OSレベルのレポートはどのプラットフォームでもきちんと文書化されますが、通常、サードパーティアプリケーションの更新履歴やRSRのバージョン履歴はそうではありません。

実際のデバイスの状態を読み取ることができないツールでは、インストールされているパッチを確認することも、監査人に対してコンプライアンスを証明することも、リスクにさらされているデバイスをIT部門に通知することもできません。監査に対応したタイムスタンプ付きのパッチに関する証拠が必須条件となる規制の厳しい環境では、推測は証拠になりません。

Jamfが選ばれる理由

Jamfのソリューションは、インシデントを追いかけるのではなく、全デバイスで一貫した状態を維持します。構成のベースラインにより、導入時にエンドポイントの健全性基準を設定します。宣言型デバイス管理により、OSアップデートを展開し、緊急セキュリティ対応の状態を明らかにし、全デバイスの追加ビルドバージョンとRSRの導入を追跡します。そのため、セキュリティ部門はパッチの状態を推測するのではなく、把握することができます。Jamf App インストーラは、App Storeからの配布では対応できないギャップを解消します。ライフサイクルのすべての段階が、タイムスタンプ付きのデバイスレベルの証拠に記録されます。導入記録は監査人に対する主張ではなく、それを裏付ける証拠となります。

この脅威が広まった背景

Jamfの2026年版セキュリティ360レポートでは、150,000台以上のMacデバイスを分析した結果、評価対象のMacデバイスの73%に少なくとも1つの脆弱なアプリケーションが入っており、58%の組織が致命的に古いバージョンのOSを搭載したMacデバイスを利用していることを突き止めました。これは、単一の調査期間内において10,000台のMacデバイスのうちおよそ7,300台に少なくとも1つの脆弱なアプリが入っており、5,800社のOSがリスクにさらされていたということです。

プロアクティブな脅威防御とテレメトリ

異なるデバイスが混在する環境でのセキュリティ運用において、Macのテレメトリは厄介な問題となる傾向があります。その理由はApple製品ではなく、ツールにあります。macOS、iOS、iPadOSは、AppleのESF（Endpoint Securityフレームワーク）、MDMチャネル、Secure Enclaveを通じてリアルタイムの詳細なセキュリティシグナルを送信します。このシグナルが存在しても、どれほど詳細な情報を取得できるか、どのくらいきめ細かく構成できるか、どれほど正確にSIEMに到達するかはすべて、ツールのそうした面がどのように設計されているかに左右されます。

影響が顕在化するのは、事態が逼迫したときです。インシデントが発生すると、調査担当者は状況を再現するためにテレメトリ（つまり、プロセスの実行、ファイルアクセス、ネットワークアクティビティ、認証、システム動作）を遡って分析します。そうした連続性のある情報の中に抜け落ちているものがあると、タイムラインが途切れてしまいます。何が起きたかはわかっても、なぜ起きたかは十全に説明することはできません。この2つの答えが揃わないと、その隙を突いて次の侵害が発生します。

推測と完全なAppleテレメトリを分ける要因は次の3つです。

Appleのネイティブイベントの発生場所をまたいだ広範な収集：最新のエンドポイントツールではEndpoint Securityフレームワークを利用するものが増えていますが、プロセスの実行、ファイルシステムのアクティビティ、アイデンティティイベント、永続化、一元化されたログの統合への対応状況はまちまちです。そうした連続性のある情報の中に抜け落ちているものがあると、調査の相関付けが破綻します。

構成のカスタマイズ性およびコンプライアンスの整合性：収集ポリシーを一括でオン/オフするしかないツールと、カテゴリごとに細かく指定して例外を設定し、NIST、PCI DSS、HIPAA、EO 14028などのフレームワークへ明示的にマッピングできるツールには、テレメトリがただ存在するだけか、証拠として利用できるかという違いがあります。

SIEM対応のストリーミングとスキーマの忠実性：Apple対応のパーサーと正規化されたイベントスキーマを備えSplunk、Microsoft Sentinel、Elastic、お客様所有のデータストアとの事前構築済みの統合があるかどうかが、「送信されたイベント」と「クエリ可能なイベント」を隔てる要因です。

完全なデータがなければ、脅威検出は事後対応モードに追い込まれます。インシデントは本来の兆候ではなく影響が出てから表面化し、セキュリティプログラムはダッシュボード上では完璧に見えても、SIEM内にあるそのことを正当化する証拠は不完全です。

Jamfが選ばれる理由

Jamf Protectは、Endpoint Securityフレームワークを基盤に、アプリケーションやプロセスからApple セキュリティツールやシステムイベントまで9つのカテゴリに対応し、クラッシュレポートなどを提供します。収集はカテゴリごとに構成でき、例外の設定や、コンプライアンスフレームワークへの明示的なマッピングにも対応しています。イベントは、デバイスが接続を失っても収集を継続する専用のオフライン導入モードを使用して、正規化されたスキーマでSIEM（またはお客様が所有するデータストア）に取り込まれます。これにより、包括的なシグナルが手に入ります。調査担当者はタイムラインを再現でき、CISOはプログラムが設計通りに動作していることを証明でき、監査人は主張の裏付けとなる証拠を確認できます。

アイデンティティ+セキュリティ：ゼロトラストポリシーと最小権限アクセス

ゼロトラスト（別名「絶対に信頼せず、必ず検証」）の強度は、取り込むテレメトリの精度に左右されます。条件付きアクセスポリシーは、ユーザが誰であるかを確認するだけではありません。ユーザが使用しているのはどのデバイスか、そのデバイスがポリシーに従っているか、アクセスの許可を支持する証拠があるかも確認します。デバイスの状態が実際に検証されないと、「検証」は推測になります。

一般的には、以下の2つの失敗パターンがよく見られます。

不完全なデバイスの状態に基づいたアイデンティティの判断：IdPの背後にあるセキュリティツールがパッチレベル、構成逸脱、コンプライアンスベースライン、脅威の存在など、実際のデバイスの状態を継続的に通知しない場合、IdPは古いシグナルや表層的なシグナルに基づいて許可または拒否することになります。条件付きアクセスはIdPが把握できる範囲で適用されます。把握が十分でないと、推測に基づいて適用することになります。

ネットワークレベルのアクセスにアプリレベルのアクセスも含まれている：従来のVPNはトンネルを暗号化し、ネットワーク全体へのアクセスを許可します。1つのエンドポイントまたは認証情報が侵害されると、影響範囲は環境全体に及びます。アクセス権の取り消しは大ざっぱで、アクセスを全面的に遮断するか、データ漏洩を許容するかということになります。リソース層ではなくネットワーク層にアクセスされた場合、その中間の選択肢はありません。

これらが重なると、本ガイドで取り上げているのと同じ監査の問題が生じます。アクセスの可否はその時点では適切に見えても、プログラムはそのときのデバイスの実際の状態を証明できず、特定のリクエストが許可された理由を明らかにできず、その裏付けとなる証拠を監査人に提示できません。

Jamfが選ばれる理由

Jamfのソリューションは、デバイス管理、アイデンティティ管理、エンドポイントセキュリティを統合するため、ユーザからの要求ではなく、検証済みの証拠に基づいて条件付きアクセスが実行されます。Jamf ProおよびJamf Protectからのリアルタイムのデバイスの状態はOkta Device Trust、Microsoft Entra条件付きアクセス、Zscaler統合に取り込まれるため、IdPは監査人が確認するのと同じ証拠に基づいてアクセスを許可します。ZTNA（ゼロトラストネットワークアクセス）は、ネットワーク全体にわたるトンネルではなく、アプリごと、リソースごとのアクセス管理を実現します。そのため、侵害はリソース層で食い止められ、アクセス権をきめ細かく取り消すことができます。アクセスの可否はすべて、その基になったデバイスの状態と共に記録され、プログラムが設計通りに機能していることをガバナンスが証明するために必要な監査証跡が生成されます。

インシデント対応と運用の自動化

インシデント対応の成否は証拠によって決まります。侵害時点のシステムの状態はどうだったか、インシデントはいつ起こったか、どのデバイスが影響を受けたか、どのようにして起こったか、なぜ起こったか、責任者は誰か、という調査担当者が答えなければならない質問はすべて同じ問題に収束します。つまり、証拠が存在するかしないかです。証拠が存在しない場合、対応は推論に基づくことになります。

Appleのフォレンジックアーティファクトは Windowsのものとは異なる場所に存在します。その場所は、一元化されたログ、FSEvents、システム機能拡張のアクティビティ、TCCデータベースの変更、構成プロファイルの履歴、MDMコマンドの履歴、Endpoint Securityのイベントです。これらの場所に対応できるよう設計されていないツールでは、全体像ではなく、断片しか捉えることができません。

以下の3つの失敗パターンが複合的に発生します。

不完全な証拠：重要なイベントストリームが欠落していると、タイムラインの再現が不完全になります。インシデント対応後レポートには説明できないギャップが存在することになり、規制やサイバー保険の証拠保持要件を満たすことはできません。

手作業の収集：証拠の自動収集が導入されていない場合、対応部門はデバイスごとに収集を進め、多くの場合、物理的にアクセスすることが必要になります。手作業のステップごとに対応時間が延び、ヒューマンエラーのリスクが高まり、データの完全性が低下したり、損なわれたりする可能性があります。

遅い解決：封じ込め、修復、ベースラインへの復帰のすべてにおいて証拠の収集がボトルネックになります。事態の把握に時間がかかるほど、業務の中断が長引き、その後に規制当局、監査人、保険引受人に提示する正当化可能な報告書を生成することが困難になります。

Jamfが選ばれる理由

Jamfのソリューションは、事後的ではなく、継続的に証拠を収集します。Jamf Protectの9つのイベントカテゴリのテレメトリを、Jamf Protectからの管理対象の状態およびJamfのZTNAからのアクセス可否と組み合わせて、インシデントが発生する前にフォレンジック記録を生成します。ポリシーベースの対応自動化により、しきい値に達した瞬間に封じ込めと修復のワークフローが開始され、JamfのAIアシスタントが得られたデータの分析を加速します。その結果、インシデント対応がクローズドループになります。対応が自動化され、解決までの時間が短縮され、インシデントがクローズした時点から立証に利用可能で包括的な証拠一式を利用できるようになります。

モバイルデバイスもアクセス層

モバイルデバイスは、ノートパソコンと同じ企業リソース（つまり、E メール、コラボレーションプラットフォーム、社内アプリケーション、顧客データ）にアクセスしますが、多くのコンプライアンスプログラムではモバイルデバイスはおまけのような扱いです。規制の厳しい業界やBYOD環境では、監査時にそのギャップが表面化し、ノートパソコンと同じデータにアクセスするiPadやiPhoneに同じ制御が適用されていると証明するために必要な証拠が存在しないことが判明します。

以下の3つの失敗パターンが繰り返されます。

- **一貫性のない制御適用：**ノートパソコンに適用されているベースライン制御（暗号化、パスコードポリシー、OSアップデート設定、限定的なアプリインベントリ）が、モバイルデバイスに部分的に適用されているか、監視されていません。
- **BYODのプライバシーとコンプライアンスの対立：**プログラムによる収集が過剰な場合、従業員の信頼を徐々に損なったり、導入の妨げとなったりする可能性があります。一方、収集が不足すると、監査の証拠が生成されません。
- **限定的なフォレンジック能力：**物理的にアクセスできず、オンデバイスAPIが制限されていると、インシデント発生後の再現が、MDMとセキュリティエージェントがインシデントの前に収集した情報に全面的に依存することになります。

Appleデバイス向けの成熟したモバイルデバイスセキュリティプログラムは、以下の3つの重要な層でコンプライアンスを確保します。

MDM基盤

登録により、管理関係と証拠の足跡が確立されます。Apple Business Managerの自動デバイス登録を通じて登録された会社支給デバイスは監視対象になり、
高度な構成や調査機能の利用が可能になります。AppleがBYODのために設計したユーザ登録により、企業データは別個の管理対象のAPFSボリュームに配置され、個人用のアプリとデータは管理対象外のままとなります。これがプライバシー境界となり、導入が維持されます。

モバイルデバイス脅威防御とWebプロテクション

iOSとiPadOSが直面している脅威の侵入経路はmacOSとは異なり、未承認の構成プロファイル、認証情報フィッシング、悪意のあるリンク、ネットワーク内攻撃、危険なアプリなどがあります。Endpoint Securityフレームワークはmacos専用でモバイルには対応しないため、対策には、オンデバイス調査、DNS層のフィルタリング、ネットワークトラフィック分析が利用されます。監査時に重要となる制御は、ツールが脅威イベント、そのときのデバイスの状態、対応アクションを、デバイスIDに紐付けされた記録に残しているかどうかです。

モバイルデバイスのフォレンジック

物理的にアクセスできない場合、モバイルデバイスのインシデント対応は、デバイスの状態、構成履歴、インストールされているアプリのインベントリ、MDMコマンド履歴、セキュリティエージェントからの脅威イベントという事前に収集されたデータに基づくことになります。リモートワイプ、アカウントの無効化、アプリの削除、証明書の取り消しなどの標準的な対応アクションにより、データが保護され、リスクが抑えられます。それぞれがいつどのデバイスに対して実行されたかを文書化して記録に残しておくと、その対応が監査可能なイベントになります。

Jamfが選ばれる理由

Jamfのソリューションは、Appleエコシステム全体に同じコンプライアンスモデルを適用します。企業支給デバイス向けの自動デバイス登録とBYOD向けのユーザ登録は同様にサポートされています。そのため、管理関係と証拠の収集は同じように開始されます。Jamfのモバイルデバイス脅威防御によって脅威イベント、デバイスの状態、対応アクションが同じ監査記録にまとめられ、ユーザ登録によるプライバシー境界によって個人用のアプリとデータは管理対象外のままになることで、プライバシーとコンプライアンスの対立が解決されます。フォレンジック証拠（つまり、デバイスの状態、構成履歴、アプリインベントリ、MDMコマンド履歴、脅威イベント）を継続的に収集できるため、インシデントの発生時点で監査証跡が既に存在し、実施した対応アクションが同じデバイス記録に残されます。

まとめ

クロスプラットフォーム環境においてAppleデバイスの運用がリスクにさらされるのは、IT部門の怠慢が原因ではありません。このリスクの原因は、ほとんどの企業向けセキュリティツールがApple以外のプラットフォーム向けの設計になっているため、パッチの検証、テレメトリの幅広さ、ハードウェアに紐付いた鍵証明、宣言型コンプライアンスの状態に不備があっても監査時にはサイレントグリーン（その証明となる証拠なしにコンプライアンスが確保されているとダッシュボードが報告すること）となってしまうことです。

この環境に別のツールを追加しても、そうした不備の解消にはなりません。問題を解消するには、Appleのネイティブメカニズムであるmdm、宣言型デバイス管理、Endpoint Securityフレームワーク、Secure Enclaveをベースとし、デバイス管理、アイデンティティベースのアクセス管理、エンドポイントセキュリティを、証拠に根差した単一のプログラムに統合する基盤となるプログラムが必要です。

これらのメカニズムをベースに構築されたソリューションが、Jamfです。Jamfは検証可能なテレメトリをリアルタイムに収集し、宣言型デバイス管理を通じて状態を適用します。そして、規制当局や監査人から、またはサイバー保険の審査で求められる傾向にあるAppleエンドポイントの証拠について、会社支給デバイスとBYODデバイス両方の最初の登録から安全な廃棄に至るまでの監査に対応した記録を生成し、提供できます。

本ガイドのポイント

- **サイレントグリーンは、及第点ではなくコンプライアンスギャップ：**現在のセキュリティスタックがApple固有の環境にどれだけ対応しているか監査します。デバイス単位で制御の証拠を提示できなければ、証明することはできません。
- **コンプライアンスの基盤は証拠：**主張ベースのレポートから、コンプライアンスを実証するタイムスタンプ付きの継続的なテレメトリに移行します。
- **構成逸脱は監査と監査の間に起こる：**ポリシーベースの自動適用を利用して、各ライフサイクルステージで起こる逸脱を検出して修復します。
- **ゼロトラストの強度はその基盤となるテレメトリの精度に左右される：**検証済みのAppleエンドポイントの健全性データをIDプロバイダに提供し、推測ではなく、証拠に基づいてアクセス許可の判断を行います。
- **インシデント対応の始まりはインシデントの発生前：**テレメトリ、MDMコマンドの履歴、エンドポイントセキュリティのイベントを発生前から収集しておくことで、対応措置を監査対応のイベントへと変換できます。
- **モバイルデバイスはおまけではなくアクセス層：**同じMDM、脅威防御、フォレンジック証拠モデルをiOSとiPadOSまで拡張します。

ぜひお試しください

トライアルに申し込む