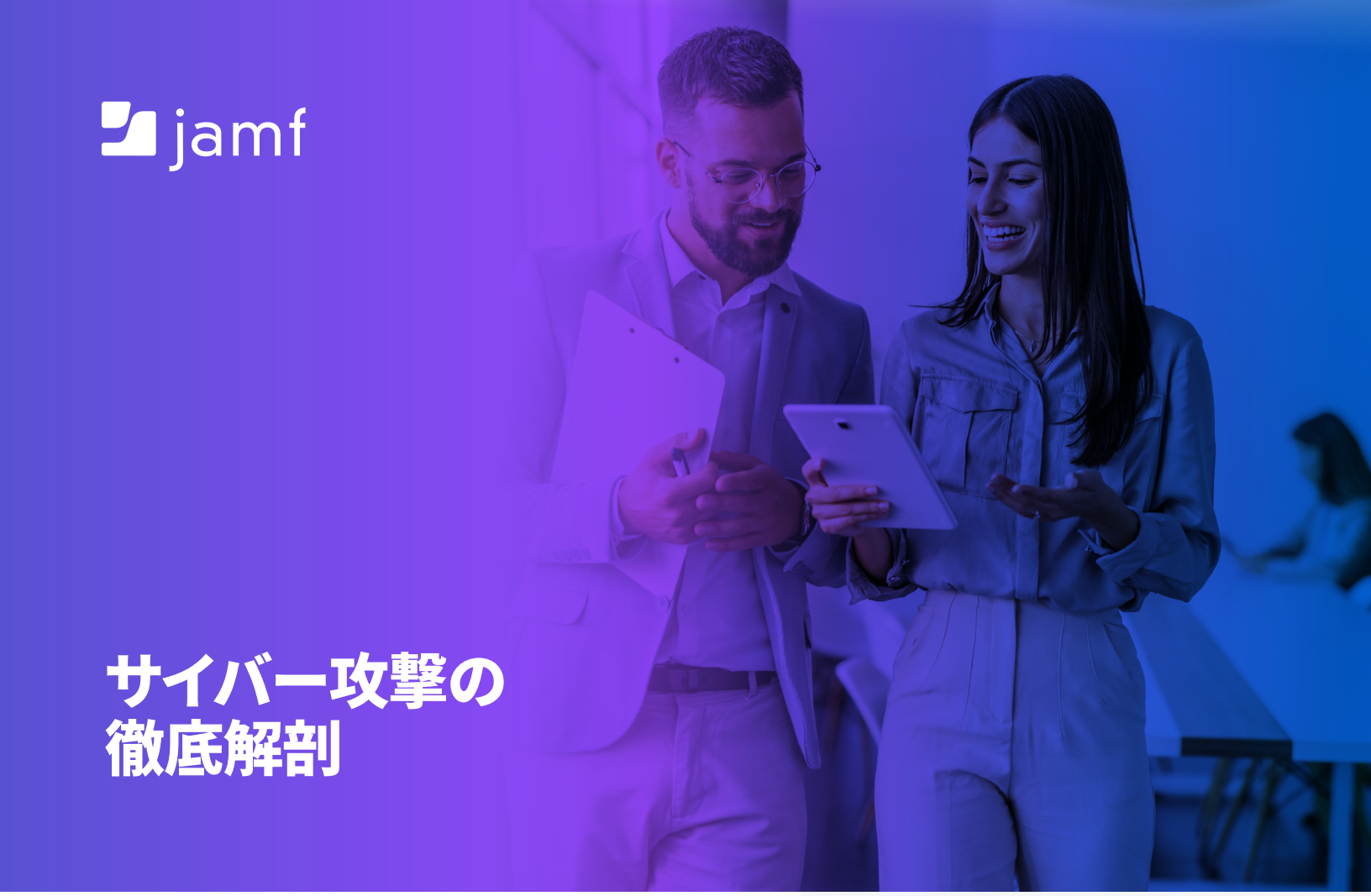


サイバー攻撃の徹底解剖

インターネットを通じて全世界がつながる現代。そのなかで、サイバーセキュリティ担当者にとって大きな仕事となっているのが、脅威アクターへの対策です。脅威アクターは、脆弱性をたった1つ発見するか、認証情報を1セット入手できれば、組織のネットワークに侵入できてしまいます。これに対して、サイバーセキュリティ担当者は、自社が抱える脆弱性を1つひとつ潰していかなければなりません。さもなければ、コンプライアンス違反のデバイスやユーザ認証情報が起点となり、データ侵害が発生するおそれがあります。

トーマス・ジェファーソンは、かつて「知は力なり」と言いました。これをサイバーセキュリティの文脈で考えてみましょう。知識は、脅威アクターからすれば、組織のセキュリティ対策を突破するための武器となり得ます。しかし、サイバーセキュリティ担当者からすれば、自社を標的としたサイバー攻撃について理解を深めるための手段にもなり得ます。

知識を組織防衛に役立てるためには、サイバーキルチェーンの各段階をしっかりと把握し、攻撃の仕組みを十分に理解しておくことが欠かせません。それこそがリスクに備え、保護を強化することにつながっていくのです。

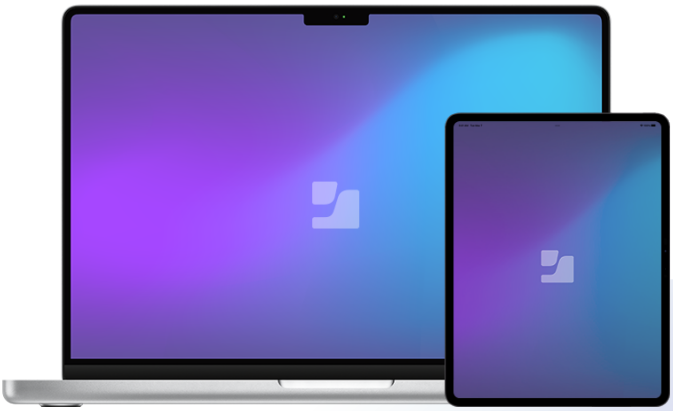
このホワイトペーパーの内容

- サイバーキルチェーンの詳細
- 攻撃の展開の一例
- 攻撃を構成する主な要素と有効な防御策
- セキュリティギャップを埋める重要性

サイバーキルチェーンを分解する重要性

攻撃のあり方は一様ではありません。攻撃者は、選んだ標的とその脆弱性に基づいて用いる脅威を変えるのが常だからです。エンドポイントのセキュリティに影響を及ぼす要素は多種多様であり、似たような脅威を利用した攻撃でも、個々の性質はまったく異なります。そのため、サイバーセキュリティを考える際には、科学から技術まで、ありとあらゆる知識を駆使して最適な対策を推測していくほかありません。

一方、攻撃を構成する脅威が多種多様であっても、どのサイバー攻撃も複数の段階に分解できることは確かです。そこで、それぞれの段階で攻撃を阻止・防御するべくLockheed Martin社が提唱を始めた手法が、「**サイバーキルチェーン**」です。サイバーキルチェーンでは、攻撃者が目的を果たすまでに（最初の準備から悪意のあるツールを実行するまでの）7つの段階があるとされます。そのため、この段階を一つひとつ分析していけば、脅威アクターに標的とされうる穴を特定し、セキュリティ対策をすり抜けられる事態を防ぐことができます。



「それが僕の戦略で、
これが僕のプラン」

– Tears For Fearsの楽曲より

攻撃者の手法を詳しく学ぶ前に、まずはサイバーキルチェーン**の7つの段階を見ておきましょう。**

1.

偵察

攻撃者が標的についてオンラインとオフラインの両方で調査を行い、標的を絞り込む。

2.

攻撃手段化

調査で収集した情報を使って、後の段階で用いるツールの開発や調達を行う。

3.

デリバリー

さまざまな悪意のあるツールを活用して、標的内部にアクセスする。

4.

エクスプロイト

標的へのアクセスに成功したら、脆弱性などのセキュリティギャップを悪用して内部に広く深く入り込む。

5.

インストール

悪意のあるコードを標的内部にインストールして、攻撃を成功させるための土台を確立する。

6.

コマンド&コントロール（遠隔操作）

攻撃の最終段階に向けて、侵害したデバイスとの通信を確立する。

7.

目的の実行

すべての準備と基礎作業の完了後、目的（個人情報の収集、データの窃取、ランサムウェアの実行など）を果たすためのツールを実行する。

さあ始めよう!

それでは、サイバーキルチェーンの各段階を詳しく見ていきましょう。このセクションでは、macOSを標的とするMaaS（Malware-as-a-Service）型脅威「**Atomic Stealer**」（AMOS）を例に攻撃を分解し、実際にこの攻撃がどのように実行されるかを見ていきます。

1.

情報収集

情報収集の段階です。脅威アクターは、もっぱら標的に関する調査を進め、標的のインフラストラクチャ、ネットワークの状況、上流および下流のサービスプロバイダに関する詳細な情報を収集します。どんな情報でも、標的のプロファイル作成に役立ちます。この段階で重要なのは、アクティブ偵察とパッシブ偵察の両方が発生する可能性があるという点です。

アクティブな情報収集

ログイン失敗の回数が過剰になる、ネットワークフィンガープリントが残るなど、侵害用のツールの痕跡が残るため、標的組織が偵察されていることを把握できる類の偵察です。

パッシブな情報収集

主に公開されている情報源から匿名で情報を収集する類の偵察です。標的組織は偵察されていることを認識できません。具体例：

- ソーシャルメディアを使って、暗号通貨業界など、収益性の高い業界から標的候補を絞り込む
- ソーシャルメディアを使って、標的組織で重要な役割を担っている従業員を特定する
- ベンダーパートナーシップを調査し、標的組織が業務に利用しているサービスを割り出す
- 従業員にソーシャルエンジニアリングを仕掛け、攻撃の成功率を高める機密情報・秘密情報を入手する

2.

攻撃手段化

偵察を終えた脅威アクターが収集した情報を整理し、攻撃の比較的早期に使用するツールをカスタマイズしていく段階です。今回例として使用するAtomic Stealerについても、攻撃手段化するための作業がいくつかあります。まず、マルウェアを開発し、DMGにアドホック署名を施します。また、ユーザにAppleのGatekeeperによる警告を回避させるようなインストール手順も用意します。このほか、実際のArcブラウザのサイトを模した悪意のあるWebサイトを作成する作業もあります。このサイトでは、訪問者に対して改ざんされたソフトウェアをダウンロードするよう促します。

注：サイバーキルチェーンの影響が表れてくるのは、ほぼ第3段階以降です。そのため、ここまでに見てきた第1段階と第2段階では、どのセキュリティソリューションもあまり大きな効果を発揮しません。『マイノリティ・リポート』の世界とは異なり、第1段階と第2段階では、攻撃は一切発生していないと考えるべきです。この2つの段階においては、脅威アクターの頭の中にアイデア、考え、仮説があるばかりです。サイバー犯罪が始まるのは第3段階からであり、私たちは脅威アクターが攻撃を試みるまで待ったうえで、その攻撃を阻止に臨んでいくことになります。

3.

デリバリー

脅威アクターが自らの調査結果を基に作戦を実行に移す段階です。

ステップ1：偽のWebサイトの運用が開始される

ステップ2：偽のWebサイトについて、正規のArcブラウザのサイトを騙るスポンサー広告が配信される

ステップ3：Atomic Stealerマルウェアでエンドポイントを侵害するソフトウェアをユーザがダウンロードし、実行する

スポンサー広告はリーチが大きく、ユーザの検索結果の上に表示されるため、比較的短期間でエンドポイントに感染が広がっていきます。この攻撃は、Webサイトを訪問する行為では直接始まらないようになっています。これは、検出を回避する狙いがあると思われます。Jamf Threat Labsが指摘しているように、Atomic Stealerの亜種を使った攻撃では、脅威アクターが多数の標的にリーチするべくE メール、SMS、ソーシャルメディアなどを駆使したフィッシングキャンペーンを展開することから、被害が急速に広まる傾向があることがわかっています。

そのような脅威からユーザを守るのに役立つのが、**Jamf Pro**、**Jamf Protect** などのソリューションです。前者は、各種のコンテンツフィルタリングによりフィッシングURLをブロックできるので、ユーザがリンクをクリックしてしまった場合の備えとして役立ちます。エンドポイントセキュリティは、デバイスの健全性を随時モニタリングし、コンプライアンスのステータスが変わった時点で管理者にアラートを送信できます。また、デバイス管理登録プロファイルを使えば、ビジネスデータを個人データとは別個の暗号化されたボリュームに保持できるため、データに強固なセキュリティが実現します。さらに、ビジネスデータに何らかの影響が及んだ場合でも、デバイスのサニタイズワークフローを自動化しておけば、被害を受けたデバイスから機密データをワイプし、漏えいを防ぐことができます。

4.

エクスプロイト

ペイロードを届ける方法には攻撃ごとに差があるものの、Jamf Threat Labsの調査で指摘されているとおり、攻撃の「目標とロジックは、究極的には変わりません」。つまり、ユーザの認証情報を不正に入手し、その機密データを窃取することこそ、攻撃者の最終目標です。

Atomic Stealerの狙いもまさにこの点にあります。つまり、自動アップデートプロセスの一環としてユーザに認証情報を入力させたうえで、データを窃取することがAtomic Stealerの究極目標であるわけですが、このデータ窃取自体は、macOSのネイティブコマンド「osascript」をベースとしたAppleScriptの呼び出しにより実行されます。

このマルウェアがバックグラウンドで実行する処理については **Jamf Threat Labs**（および「目的の実行」のセクション）で詳しく説明しています。もっとも、この悪意のあるコードをベースとした亜種のほか、時間とともに進化していくような作りの亜種まで見つかっていることを考えると、脅威アクターがユーザに侵害を気づかれないまま処理をいくらでも実行できる可能性は十分考えられます。**実際、AppleのTransparency, Consent and Control（TCC）フレームワークを回避する脅威による侵害の事例も存在します。**

Jamf Trusted Accessなら、豊富なテレメトリデータをリアルタイムで収集し、デバイスの健全性が変化したことを管理者に通知できるので、脅威アクターがフィッシングキャンペーンでユーザの認証情報の取得に成功した場合でも、以後の段階に位置する攻撃を阻止できます。さらに、修復に向けたワークフローを自動で実行することもできます。このワークフローで脆弱性のパッチを適用するアップデートを展開するなどすれば、エクスプロイトの段階自体の進展も防げます。

認証情報そのものに関しては、**Jamf Connect** でIDとアクセスを管理するのが有効です。Jamf Connectなら、インシデント対応が済むまで侵害を受けたアカウントを無効化できます。**インシデントへの対応と復旧**のスピードを上げるのであれば、Jamf Protectと統合し、**ゼロトラストネットワークアクセス**（ZTNA）を有効にします。すると、認証情報が他のアプリやサービスの侵害に利用された時点でそれを検知できるようになるため、リスクを最小限に抑えられます。また、標的となったサービスに対する脅威を隔離し、インフラストラクチャ内での横展開を防ぐこともできます。脅威の影響が及んでいないサービスは引き続き利用できるため、ユーザの生産性が保たれます。さらに、要求が発生するたびにハードウェアとソフトウェアのチェックを実行する機能も、追加の保護策として有用です。具体的には、検証ワークフローによる修復が終わり、侵害の影響が及んだデバイスのコンプライアンスが確認できるまで、問題のデバイスや認証情報による業務リソースへのアクセスを無効化しておく際に役立ちます。

5.

インストール

脅威アクターが引き続き悪意のあるコードを実行し、マルウェアを展開して持続性を確保する段階です。脅威アクターが侵害を受けたシステムにアクセスできる状態が持続し、偵察が続くため、侵害を受けたデバイスが接続しているネットワークに広く影響が拡大していきます。この段階では、コマンドラインユーティリティや悪意のあるコードなど、ネイティブツールから独自のツールまでさまざまな手段が駆使され、バックドアが作られていきます。AMOSはシステムに痕跡をほとんど残すことなくユーザの情報を一気に窃取することが目標なので、この段階はAMOSに直接関係するものといえます。そのため、AMOSがこの段階で実行するのは最小限の処理のみです。他の攻撃の場合、この段階は、現在および将来の攻撃を検知されることなく円滑に進めていくための準備に時間が費やされる傾向にあります。

この段階の防御措置としては、**可視性とセキュリティを活用**し、既知の脅威を検出、抑止、および修復してコンプライアンスを確保することが非常に重要です。デバイスの健全性を積極的に監視していれば、デバイスのセキュリティ状態の変化について管理者がアラートを受け取ることができるため、トリアージの

作業やインシデント対応のワークフローを速やかに開始できます。Jamf Protectには、悪意のある既知のコードの実行を阻止する機能が備わっており、マルウェアを実行される前に隔離および削除するなどの対応が可能です。未知の脅威については、デバイスのログを他社のSIEMソリューションに転送する機能があります。これを使えば、システム内で密かに情報収集を進める脅威の発見および削除に臨む**脅威ハンティングチーム**をサポートできます。

6.

コマンド&コントロール（遠隔操作、C2）

Atomic Stealerの狙いは、認証情報を窃取したうえで、窃取したパスワードを使ってデータをさらに盗み出すことでした。しかし、脅威アクターの目的によっては、攻撃がそれで終わらないこともあります。キーチェーンは、各種の認証情報を安全に保管し、一元管理できる便利な機能です。しかし、ひとたび侵害されると、さまざまな機能、ソフトウェア、サービスのキーが攻撃者の手に渡ってしまうリスクもはらんでいます。キーチェーンが攻撃者にとって魅力的なのは、侵害に成功した場合に以下のようなメリットがあるためです。

- データが豊富なリソースに対する強力なアクセス権が手に入る
- 横展開により攻撃の範囲を拡大できる
- 窃取したデータを販売したり、被害者を恐喝したりして、さらに金銭を得ることが可能になる

シンプルに言えば、手に入るデータが多いほど標的としての魅力が大きくなるというわけです。

対策としては、侵害を受けたデバイスとの通信を遮断することがきわめて重要です。ZTNAならエンドポイントを監視し、C2サーバーなどの悪意のあるサービスへの接続をブロックできるので、攻撃者が侵害を受けたデバイスと通信する事態を防げます。また、ZTNAではデバイスと認証情報の健全性を継続的に監視し、コンプライアンス違反を検知できるので、侵害を受けたデバイスやユーザが保護されているリソースにアクセスするのを防いだり、コンプライアンス違反のデバイスに対するアクセスを制限したりすることもできます。さらに、Jamf Proと連携し、脆弱性のあるデバイスや侵害を受けたデバイスの修復ワークフローを自動で実行する機能も備わっています。

7.

目的の実行

これが最終段階です。この段階になると、攻撃者が計画を実行に移します。具体的には、以下のような事態が発生します。

- **スパイ活動**
- データ流出
- 恐喝
- サプライチェーン攻撃
- サイバーテロ

上記は複合的に発生することもありますが、いずれにしても脅威アクターが自らの作業の成果を刈り取る段階であることは変わりません。この段階の被害を定量化することは困難です。組織のニーズがそれぞれ異なるように、攻撃者もそれぞれ目的が異なり、程度の差こそあれ、自らの目的に応じて実際の活動を変化させるからです。Atomic Stealerの場合には、前述のosascriptコマンドを使って正規のシステムアラートを模したアラートを作成します。これが正規のアラートと異なるのは、ユーザの認証情報を使用して、Apple のキーチェーンから以下のような機密データを収集するという点です。

- ユーザ名とパスワード
- ブラウザセッションの Cookie
- ユーザの機密データ
- 決済カードの詳細
- 暗号通貨ウォレット
- システムメタデータ

防御の穴を修復する

保護が不十分な状態でデスクトップオペレーティングシステムだけに着目していると、モバイルデバイスのセキュリティギャップが放置され、脅威アクターが組織のネットワークに侵入するための侵害の起点となってしまう可能性があります。

もちろん、データ侵害のリスクとなり得るものはモバイルデバイスだけではありません。しかし、脅威は常にめまぐるしく変化を続けています。モバイルデバイスが業務用としても個人用としても普及が進み、業務データにアクセスする手段としての使用頻度が高まっていることを考えると、モバイルを標的とした脅威は今後も発生が続くことが予想されます。**Jamf Threat Labsの調査**ではリスクを定量的に評価し、「モバイルユーザの40%が、既知の脆弱性があるデバイスを使用している」ことを突き止めました。デバイスに脆弱性があるとリスク要因の検査漏れが生じ、脅威アクターに以下のような攻撃を許してしまいます。

- デバイス上で悪意のあるコードを実行
- 内部のセキュリティ保護をバイパス
- 権限のないビジネスデータにアクセス
- 許可なくプライバシーデータを取得
- ユーザに無断で、あるいは同意なしに監視
- 感染デバイスからネットワークに不正侵入
- プライバシー情報だけでなく個人データやビジネスデータも窃盗

Appleはフォルム・機能・スタイルをデバイス機器に見事に融合させたことで名高いブランドです。この哲学は、セキュリティとプライバシーという、ますます重要性を増す設計要素にも反映されています。macOSとiOSベースのオペレーティングシステムには、デバイス、ユーザ、データをさまざまな脅威からハードウェアとソフトウェアの両方のレベルで守るための保護機能が標準搭載されています。

脅威アクターは、近年増加しているインフォスティーラー（情報窃取に特化したマルウェア）のような、新しい脅威やマルウェア亜種を使って攻撃を進化させています。既知の特徴しか検出できないツールによるセキュリティでは、進化するサイバー脅威への防御はかなり困難です。例えば、Dark Readingによると、Atomic Stealerなどの脅威の「進行の過程は、更新されているコアバージョンとはまったく異なる」といいます。そのため、**巧妙化した脅威はデバイスに内蔵されているセキュリティ機能を回避**し、デバイス、ユーザ、データにリスクをもたらします。

「ハッカーにとって必要なのはたった一度の成功。それを防ぐために私たちはたった一度の失敗も許されない」

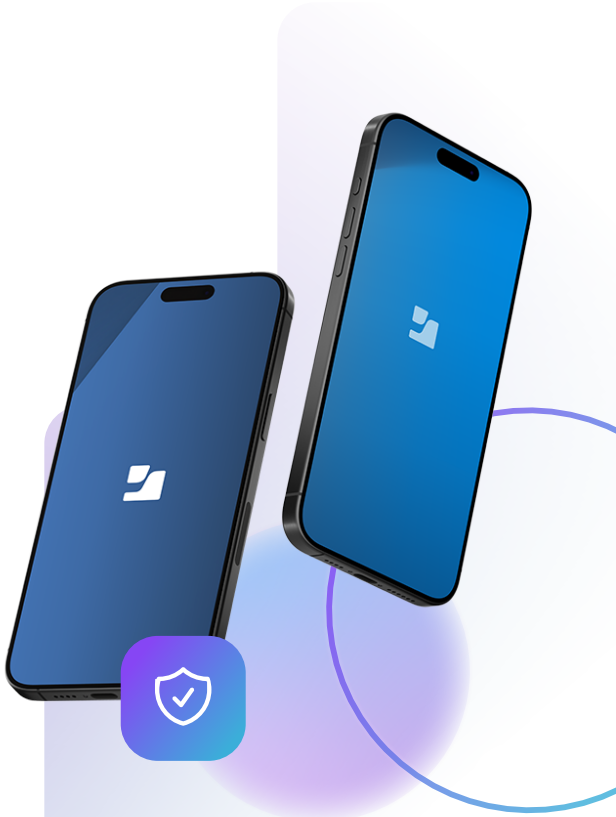
– HP社、Chris Triolo氏

解決策の1つとしては、**管理、アイデンティティ、セキュリティのすべてを1つのソリューションに統合するというやり方があります。**そうすることによって、ネットワークとデバイスの両方で、悪意のあるトラフィックを包括的にブロックするのです。さらに、ビジネスデータの窃取を予防することも、攻撃者からデータを守るうえで重要です。ZTNAは、この種の取り組みを推進するものです。具体的には、認証情報の侵害を自動で検知し、無効化することにより、保護されているビジネスサービスに対するアクセスを予防し、リスクの軽減につなげます。テレメトリデータ全体が安全に共有されるため、脆弱性の修復が済むまでの間、リスク軽減に向けたワークフローを自動で実行できます。要求されたリソースに対するアクセスは、エンドポイントのコンプライアンスが確認できてから承認されます。

最も効果的な対策は、成熟した**多層防御フレームワーク**をベースとしてセキュリティ計画を策定することです。これにより、リスクを軽減し、既知の攻撃を防止し、自動修復ワークフローでインシデントに迅速に対応して、エンドポイントのコンプライアンスを確保することができます。

多層化された統合型のソリューションがあれば、何重にも施された防御層によって包括的にリスクを捕捉および軽減し、高度な脅威にも対抗できます。これらの保護層のカバー範囲は組織全体に及ぶので、リソースやデータへのアクセスを要求するあらゆるタイプのデバイスやOSに対する第一防衛ラインにもなります。

Frost & Sullivanによる**『Frost Radar: Endpoint Security, 2023』レポート**において、Jamfは各種ソリューションで以下に挙げる優れた多層防御機能を提供していることから、エンドポイントセキュリティ分野における「リーダー」と評価されています。



悪意のあるアプリケーションやスクリプトをリアルタイムで検出し、ユーザに推奨対策を提示

お客様が複雑なコンプライアンス基準を満たすうえで役立つ、構成と監査の充実したフレームワーク

会社支給デバイスと個人所有デバイスの両方に一貫したポリシー適用とサポートを提供

ソリューション全体で統一された脆弱性管理、脅威対策、ポリシー管理

外部のログ収集や分析用ツールにエクスポートできる豊富なエンドポイントテレメトリ

デバイス管理、アイデンティティ&アクセス管理、エンドポイントセキュリティのすべての要素を組み合わせ、Appleのために構築された市場唯一のソリューションであるJamf Trusted Accessを提供

MacだけでなくmacOS、iOS/iPadOS、Androidなどのモバイルプラットフォームも対象にしたセキュリティレポートを生成。さらに、追加の脅威保護機能により、これらのプラットフォームに加え、WindowsやChromebookにまでサポートを拡張することも可能

まとめ

デバイス、ユーザ、データが脅威アクターの標的であり続けるかぎり、セキュリティ対策が不要になることはありません。リスクを最小限にとどめ、脅威が深刻なデータ侵害に移行する事態を防ぐためには、セキュリティ対策が不可欠です。

これからのセキュリティ計画で目指すべき目標

- リスクの認識とリスク許容度の設定
- リスク軽減と脅威防御のための多層的対策の実施
- デバイス管理、アイデンティティ&アクセス、エンドポイントセキュリティの各ソリューションを、相互に連携して機能するように統合
- IT部門とセキュリティ部門のサイロ化を解消し、コミュニケーションを促進してインシデント対応を迅速化
- 自動ワークフローを活用し、脅威を短時間で修復しつつ、ユーザによるエラーも最小限に抑制
- ビジネスのニーズや要件を各種の基準やフレームワークに適合させ、セキュリティ対策を強化しつつ、コンプライアンスを確保
- 初期対応部門を創設し、インシデント対応を加速（専門組織の創設が現実的に難しい場合には、未知の脅威の発見に向けてJamf Threat Labsなどの信頼できるセキュリティ専門チームの支援を得る）

Jamfは、Appleデバイスの管理とセキュリティ分野のリーダー企業です。パートナーにお選びいただければ、Jamf Threat Labsをはじめとする**セキュリティの専門知識**を活かし、お客様のセキュリティギャップ解消をサポートします。また、各種の自動ワークフローにより、高度な脅威に対するセキュリティ状態を強化するとともに、お客様のインフラストラクチャ内の保護されているリソースにアクセスするデバイスの機密データも守ります。デバイスやOSの種類も、デバイスが物理的に存在するかどうかも、使用しているネットワーク接続の種類も問いません。**私たちは、Apple製品の業務利用を力強くサポートします。**