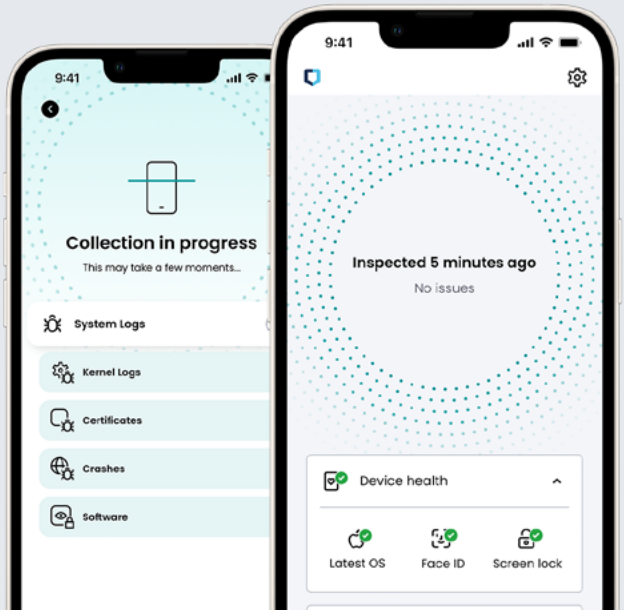
jamf

Jamf Executive Threat Protection

モバイル脅威の可視化がついに実現します。



リモートおよびハイブリッドワークが多くの組織で当たり前のものになったことで、さまざまな業務やプライベートのタスクにモバイルデバイスが頻繁に使用されるようになりました。モバイルデバイスにインストールされたアプリのおかげで、メールからミーティングまでワンタップで簡単にアクセスできます。しかし、スマートフォンには業務データやプライベートのデータが多く含まれており、さらに常にインターネットに接続されているため、ハッカーにとって格好のターゲットになります。

攻撃にはさまざまな形態があり、その中でももっとも危険なのが、ゼロクリックおよびゼロデイエクスプロイトです。これはビジネスアプリケーション、多要素認証（MFA）リクエスト、そして写真やメモまで、デバイス上のあらゆるデータへのリモートアクセスを試みるもので、ユーザの知らないところでカメラやマイクを有効にしてしまうエクスプロイトさえも存在します。そのため、デバイスが侵害された瞬間にそれを理解し、修復のためのアクションを実行してくれるツールを用意することが何より大切です。

Jamf Executive Threat Protection

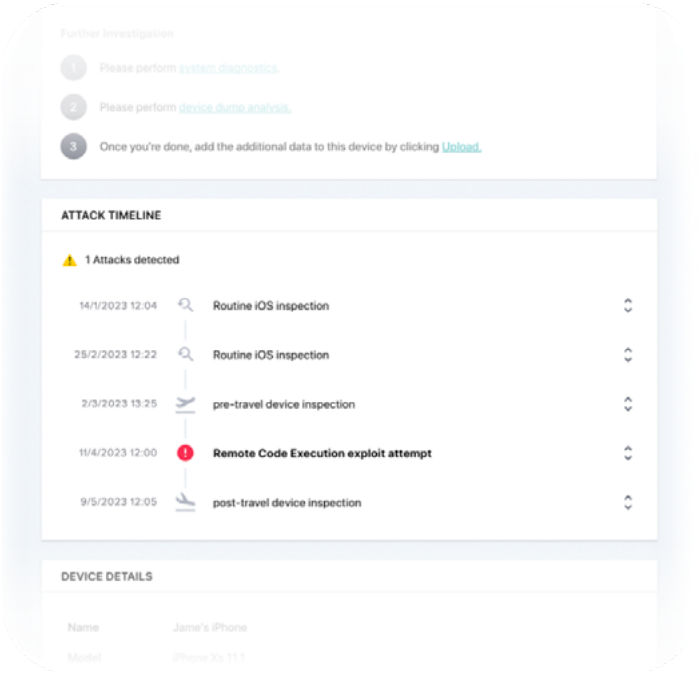
高度な検出およびインシデント対応ソリューションであるJamf Executive Threat Protectionは、モバイルデバイスに起こったことをいち早くリモートで把握するための手段や、高度な攻撃に対応するためのツールを組織に提供します。

優れたデータ収集

豊富なモバイルエンドポイントテレメトリのおかげで、どこにいてもモバイルフリートの状態を詳細に把握できるため、手動の調査にかかる時間を数週間から数分に短縮することができます。また、MDMの枠を超えたシステムログを収集し、包括的な調査を可能にします。

高度なモバイル攻撃を検出&打破

Jamf Executive Threat Protectionは、デバイスの管理とセキュアな運用の枠を超え、重要なユーザを狙った攻撃に対する優れた可視性を提供します。



より迅速な検出

攻撃者がどれほど巧妙であっても、データの痕跡は必ず残ります。大切なのはそれを見つける方法を知ることです。深層分析を実行してセキュリティ侵害インジケーター（IoC）を特定し、高度な検出データをセキュリティチームに提示することのできるJamf Executive Threat Protectionは、通常なら検出されない高度なゼロデイ攻撃をも見つけ出すことができます。

確実な修復

Jamf Executive Threat Protectionは、不審なイベントのタイムラインを自動的に構築し、デバイスがいつ、どのように侵害されたかを提示してくれます。内蔵された対応ツールを利用することにより、セキュリティチームはAPT攻撃を打破してユーザの安全を確保すると同時に、継続的な監視で脅威を排除することができます。

高度な分析とJamf Threat Labsの専門家によって厳選されたインサイトを利用してモバイルフリートの可視性を強化することに興味のある方は、ぜひ無料トライアルにお申し込みください。

jamf

www.jamf.com/ja/

詳細は公式サイトの関連ページをご覧ください。