

Appleを狙った脅威から エンドポイントを保護

サイバー攻撃を阻止し、エンドポイントのコンプライアンスを維持しながら、アクティブな脅威の検出や対応を行うためのソリューションです。



巧妙さを増した今日のサイバー脅威は、組織のデバイスやインフラに新たなリスクをもたらしています。このような状況においては、汎用的なセキュリティツールでは満足にセキュリティ攻撃の阻止やインシデントの調査・修復を行うことができず、ユーザやデバイス、セキュリティチーム、組織などを危険に晒すことになってしまいます。

そこで登場するのが**JamfProtect**です。

Jamf Protectは、Appleを狙った攻撃を阻止し、デバイスのコンプライアンスを明確に可視化するために作られたエンドポイントセキュリティソリューションです。

JamfのソリューションはAppleを狙った脅威特有の課題を解決します。

Jamf Protectを活用することにより、組織はエンドポイントやアプリケーションのサポートを強化しながら、リスク管理能力を手に入れることができます。



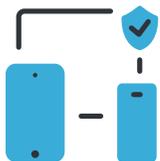
エンドポイントのセキュリティ

Jamf Protectは、Appleを狙ったマルウェアや攻撃に対抗するための包括的な検出および保護機能を提供します。また、リムーバブルストレージを管理するためのデバイス制御機能を利用して、データ損失を防ぐこともできます。



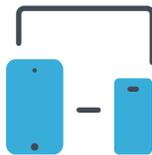
コンプライアンスと可視性

Jamf Protectは、カスタマイズ可能なベンチマークレポートや豊富なテレメトリデータの記録を通じて、組織のコンプライアンス目標の達成をサポートします。これにより、セキュリティインシデントに関する包括的なコンテキストが手に入るため、調査やインシデント対応の際に役立てることができます。



脅威防御

Jamfが独自に開発した機械学習エンジン「MI:RIAM」の力を借りてフィッシング攻撃に使われる悪意のあるドメインなどの脅威を阻止するとともに、脅威ハンティングの専門家が集まったJamf Threat Labsが未知の脅威を検出します。さらに、利用規約の徹底や危険なコンテンツのブロックを行うことにより企業データを保護します。



Appleとの連携

Jamf Protectは、Appleのデバイスやオペレーティングシステムを第一に考えて設計・構築されており、Appleによるアップデートの即日サポートやSOC 2への準拠にも対応しています。これにより、セキュリティチームは単一のツールで最新のセキュリティ脅威に対抗することができます。

エンドユーザエクスペリエンス

セキュリティツールの役目は脅威を阻止することだけではありません。エンドユーザへの影響を最小限に抑えながらそれを行うことが求められています。Jamf Protectは、カーネル拡張を必要とせず、最小限のシステムリソースだけを使用して実行されるため、Apple独自のユーザエクスペリエンスを維持することができます。

Jamf Protectは、[Jamf Threat Labs](#) (未知の脅威を調査するために結成された、経験豊富なデータ科学者および脅威調査やサイバーセキュリティの専門家から構成されるチーム) によってサポートされたソリューションです。



www.jamf.com/ja/

© 2002-2023 Jamf, LLC. All rights reserved.

Jamf Protectの機能を実際に体験してみたい方は、ぜひ**トライアル**にお申し込みください。または、お近くの販売代理店までお問い合わせください。