jamf

最先端のAppleセキュリティ体制を構築するには

無料の成熟度モデルと
90日間の実装計画 →

ほとんどのPC用ツールはMacにも対応しています。しかし、モバイルデバイス管理（MDM）、エンドポイントセキュリティのフレームワーク（ESF）、プラットフォームAPI、プラットフォームSSOといったツールについて言えば、Appleのアーキテクチャ内の適切なレベルで動作し、企業に包括的なセキュリティ対策を提供しているのは、Appleネイティブのツールだけです。

セキュリティのギャップを生まない体制は整っています？

Apple セキュリティ成熟度モデル

4段階のモデルを活用して、自社のセキュリティ体制に潜むギャップを特定しましょう。

第1段階

急場しのぎ

- 一貫性のないデバイス登録
- 手動による監査
- 限定的な可視性
- 高リスク

第2段階

定義済み

- ベースラインの導入
- パッチ適用の自動化
- コンプライアンスレポートの作成
- 基本レベルのIdP統合

第3段階

管理下

- 継続的な適用
- SIEM/SOARへのESFテレメトリの転送
- IdPとの詳細な状態の共有
- インシデント対応プレイブック

第4段階

最適化

- 予測分析
- 自動修復
- ATT&CKにおけるMacの完全網羅
- ゼロトラストの検証

90日間の実装計画の例

急場しのぎで一貫性のないデバイス登録から、自社環境に全面的に最適化された成熟度の高いセキュリティ体制へ、90日で移行できます。

1〜30日

基盤の確立

- macOS/iOSデバイスの完全なインベントリを作成
- ゼロタッチ登録を導入
- CISベンチマークレベル1のベースラインを確立
- コンプライアンスシグナリングを有効化するようIdPに接続
- デバイス監視をセットアップ

31〜60日

運用の本格化

- macOSアプリや優先度の高いアプリの自動パッチ管理を設定
- ベンチマークを規制フレームワークに拡張
- アクティブ検出とSIEM統合をセットアップ
- iOSデバイスを登録
- 不要なローカル管理者権限を削除

61〜90日

成熟に向けた最適化

- iOSの脅威防御をセットアップ
- 上位5つのMacインシデント対応シナリオに向けたSOARプレイブックを策定
- 最初の継続的コンプライアンスレポートを作成
- 成熟度の段階を評価
- 改善点を目に見える数字でリーダー層に提示

既存のツールもそれぞれの用途に関しては申し分ないものの、Mac/iOSデバイスを保護するには、Appleのアーキテクチャを理解したセキュリティ体制が必要です。

Jamfは、既存のツールを置き換えるのではなく、SIEM、SOAR、IdP、XDR、SSEといったプラットフォームとの**統合を通じて既存のツールを補完するよう設計されています。**Microsoft、Crowdstrike、Palo Alto、Zscalerと完全に統合されます。

最先端のApple セキュリティ体制の構築については、ぜひJamfにご相談ください。

トライアルに申し込む