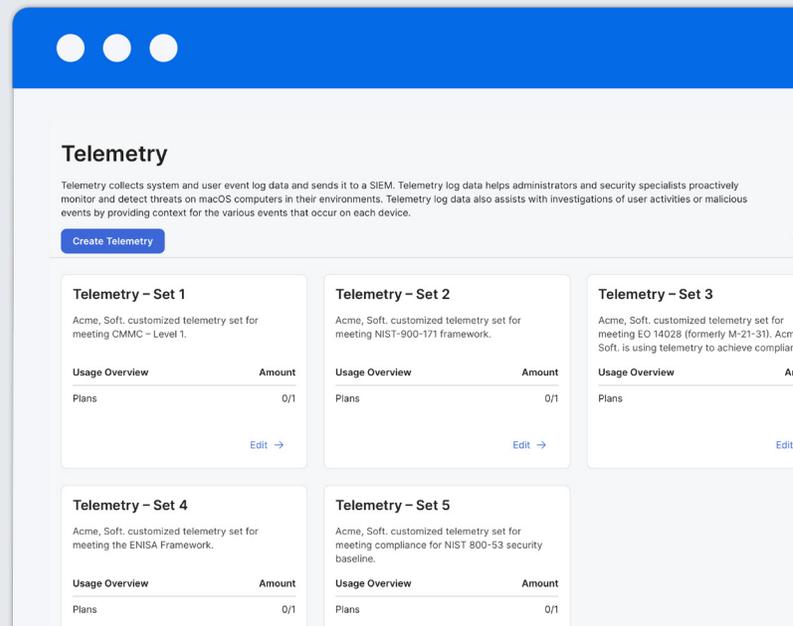




Macエンドポイントテレメトリ

Apple専門家による実用的な洞察



職場にMacを導入する企業の増加に伴って、悪意のある存在もMacへの注目や関心を高めています。

Macが他のプラットフォームと同等のコンプライアンス、セキュリティ、運用基準を満たすには、Mac向けにあつらえた可視性と防御が必要です。

Jamfが提供するMac向けのエンドポイントテレメトリ

AppleのエンドポイントセキュリティAPIを搭載し、Jamfの20年以上にわたるAppleの専門知識を投入して完成した、このテレメトリはmacOSのアクティビティの詳細な監査を可能にし、相関性のある100%トレーサブルな洞察を、セキュリティチームが日常的に使用するソリューションに提供します。

主なメリット:

- 複雑な規制フレームワークとセキュリティベースラインでコンプライアンスを徹底
- 詳細な攻撃タイムラインの再構築により、インシデント対応をスピードアップ
- 高度なmacOS脅威を検出、滞留時間を短縮、レジリエンスを強化
- 主要セキュリティベンダーと構築されたSIEM統合によるシームレスな導入



イベントデータを基にアクションを実行



次世代のエンドポイントテレメトリ

最新のコンプライアンス、セキュリティ、IT ニーズに対応した専用設計

- AppleのmacOSエンドポイントセキュリティAPIから直接取得した**忠実度の高いテレメトリ**
- macOSセキュリティアーキテクチャとの**シームレスな統合により**、耐タンパー性のある信頼度の高いデータを提供
- ユーザエクスペリエンスを維持しながら、重要なエンドポイントのアクティビティも細かく可視化する**軽量設計**



圧倒的なmacOSの可視性

Macフリートに関するかつてないほど深い洞察を提供

- プロセスの実行、認証、特権アクション、ユーザアクセス、権限昇格、永続化、ビルトインのセキュリティイベント**など**、あらゆる角度から**アクティビティを監査**
- **macOSに特化したデータモデルにより**、Appleデバイスでのコンプライアンス監査、脅威検出、調査に最適な洞察を提供
- **mac向けの洞察**: macOSに特化したデータモデルが、Appleデバイスでのコンプライアンス監査、脅威検出、調査に最適な洞察を提供



調査を迅速化

macOS 脅威のためにApple専門家が設計したテレメトリ

- 追跡可能なプロセスとテレメトリの総合的な相関付けにより、**インシデントタイムラインを再構築**
- 異常、レアイベント、living-off-the-land (環境寄生型) などのmacOS攻撃テクニックの洞察を基に**攻撃者を検出**
- 細かく文脈化されたテレメトリが迅速な調査と対応を可能にし、**セキュリティに関する意思決定を迅速化**



エフォートレスな統合

導入は数分で完了

- Splunk、Microsoft Sentinel、Elastic、Google Security Operations、その他のSIEMをプラグ&プレイでサポートし、SIEMソリューションのメリットを**最大化**
- SIEMのデータモデルにテレメトリを合わせ、macOSの脅威シナリオを基に設計した専用パーサーにより、**チームの負担を軽減**
- セキュリティチームとITチーム向けの広範なドキュメントで**シームレスな実装を約束**

JamfでMacのエンドポイントを完全可視化

Macエンドポイントテレメトリは、[Jamf Threat Labs](#) (未知のAppleセキュリティ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/

© 2025 Jamf, LLC. All rights reserved.

詳しくは、Jamf担当者にお問い合わせください。
[ぜひトライアルへの申し込みをご検討ください。](#)

または、お近くの販売代理店までお問い合わせください。