概要

Cisco プラットフォームについて

プラットフォームは主にサーバーから、インフラストラクチャ全体にわたって収集された豊富なトラフィックテレメトリを使用して、包括的に多くのデータセンターを動作させ、セキュリティの課題に対応するように設計されています。このプラットフォームは、アルゴリズム的アプローチによる高度な分析を実行し、アプリケーションに対して一貫性のある許可リストポリシーを適用します。このアルゴリズム的アプローチには、人手を介さない機械学習技術や動作分析が含まれています。このプラットフォームには、すぐに使用可能なソリューションが用意されています。プラットフォームでは、次の機能を提供します。

- 許可リストポリシーの生成を自動化する動作ベースのアプリケーションの洞察
- 効率的で安全なゼロ信頼実装を有効にするアプリケーションのセグメンテーション
- オンプレミスデータセンターおよびプライベートクラウドとパブリッククラウドにわたる一貫したポリシーの適用
- プロセスの動作の違い、ソフトウェアの脆弱性、および攻撃対象領域を削減するための公開の識別
- アプリケーションの動作の変更やポリシーの遵守違反をほぼリアルタイムに特定
- 実用的な情報を短時間で提供する、異種環境における包括的なテレメトリ処理のサポート
- 詳細なフォレンジック、分析、およびトラブルシューティングのデータを長期間保持

プラットフォーム内でケースの様々な使用事例をサポートするため、プラットフォームではデータセンターインフラストラクチャ全体からの一貫したテレメトリデータが必要です。複数のアプローチを使用してテレメトリデータを収集するサポートにより、このプラットフォームは既存と新しいデータセンターインフラストラクチャの両方をサポートするように設計されています。これらのインフラストラクチャのオンプレミスまたはパブリッククラウドにあります。

テレメトリの収集に対する主なアプローチは、ソフトウェアセンサーです。ソフトウェア（ホスト）センサーは任意のエンドホスト（仮想化、ベアメタルまたはコンテナ）サーバーにインストールできます。これらのセンサーは、プラットフォームが生成するアプリケーションのセグメンテーションポリシーのエンフォースメントポイントとして動作します。このアプローチを使用して、プラットフォームは、パブリック、プライベート、およびオンプレミスでの導入全体で一貫性のある適用を実現します。センサーはネイティブのオペレーティングシステム機能を使用するポリシーを適用し、データパスにセンサーを置く必要がなく、フェールセーフなオプションが提供されます。さらに、プラットフォームがプロセスと通信の動作の違いとソフトウェアの脆弱性を追跡する機能を有するため、包括的なワークロード保護機能を提供します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。