FORESCOUT

Forescout 8.2 最新情報

“2023年までに、世界各地で「つながる」IoTデバイスの総数は352億個を超えるだろう”

IDC社「Worldwide IoT Forecast, 2019-2023」

我々は、過去10年のサイバー攻撃から「ネットワーク上にたったひとつでも脆弱な箇所があると、組織全体が侵害にさらされてしまう」ことを学びました。デジタルトランスフォーメーションを推進すべく、エンタープライズネットワークに接続するIoTその他の非管理デバイスが増え続ける今、イノベーションと同じく重要な「デバイスのセキュリティおよびネットワークの保護」という目的を両立させることが喫緊の課題となっています。

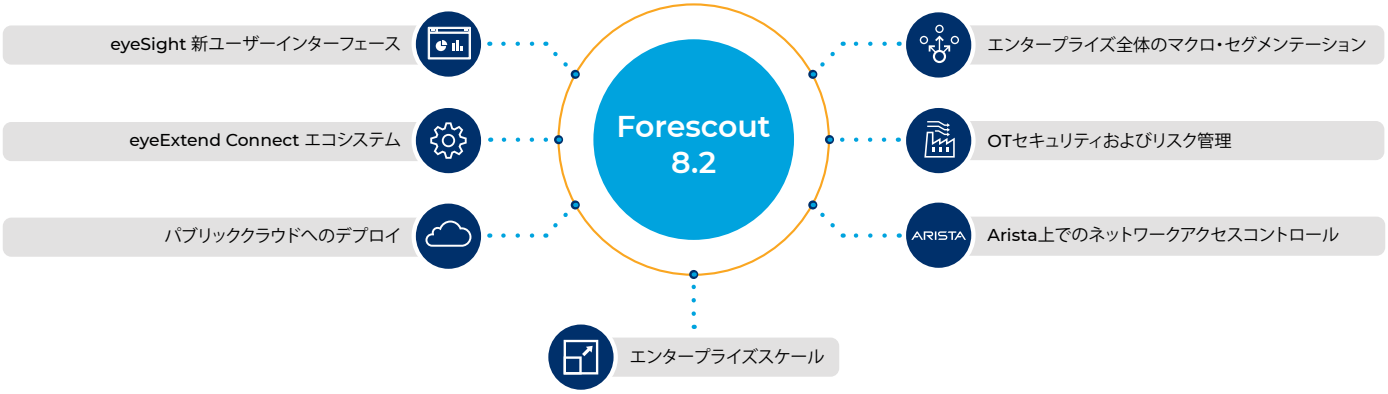
ネットワークドメイン全体の接続デバイスの全体像がなければ、リスク緩和策を迅速に実行できません。レガシー/脆弱なデバイス、コンプライアンス違反/設定違反のエンドポイント、IoTやオペレーショナルテクノロジー(OT)など、あらゆるモノを検出するだけでなく、相互接続するネットワークやロケーションすべてのリスクも常に評価する必要があります。すべてを可視化することが、「素早い」行動につながります。

Forescout 8.2: 検出から対応までをスピードアップ

Forescout 8.2は、企業ネットワーク上のあらゆる接続デバイスやコンプライアンスギャップ/リスクの迅速な検出を支援します。セキュリティのエクスポージャーに迅速かつ確実に対処し、拡張エンタープライズネットワーク全体での対応までの平均時間(MTTR)を短縮します。

Forescout 8.2の主な特長：

- eyeSightに搭載されたユーザー視点に立った新ユーザーインターフェース経由で、実行可能なデバイスコンテキスト情報を提供。リスクのピンポイント検出、優先順位付けおよびプロアクティブな緩和対応を支援します
- eyeExtend Connect（新たなコミュニティーベースのアプリ開発エコシステム）により、当社のお客様やパートナーは当社プラットフォームとの連携アプリを簡単に開発・利用・共有できます
- AWSおよびMicrosoft Azureのパブリッククラウド環境で当社アプライアンスのデプロイをご検討中の「クラウドファースト」のお客様向けに柔軟なデプロイ方法を提供し、価値の早期実現を支援します
- eyeSegmentによるエンタープライズ全体のセグメンテーション機能により、複数のネットワークドメインおよび散在するエンフォースメントポイント全体で、ポリシーを確実に設計・適用していただけます
- ForescoutSilentDefenseTMおよびIT/OT一体型センサー内蔵アプライアンスにより、IT/OTドメイン全体での可視性を統合します（IPレンジが重複するクローンネットワークも含む）
- Aristaのインフラとの直接連携により、ITおよびIoTデバイスへのエージェント無しで、802.1X認証にも依存しないネットワークアクセスコントロールを実現します。



新たなユーザーインターフェース

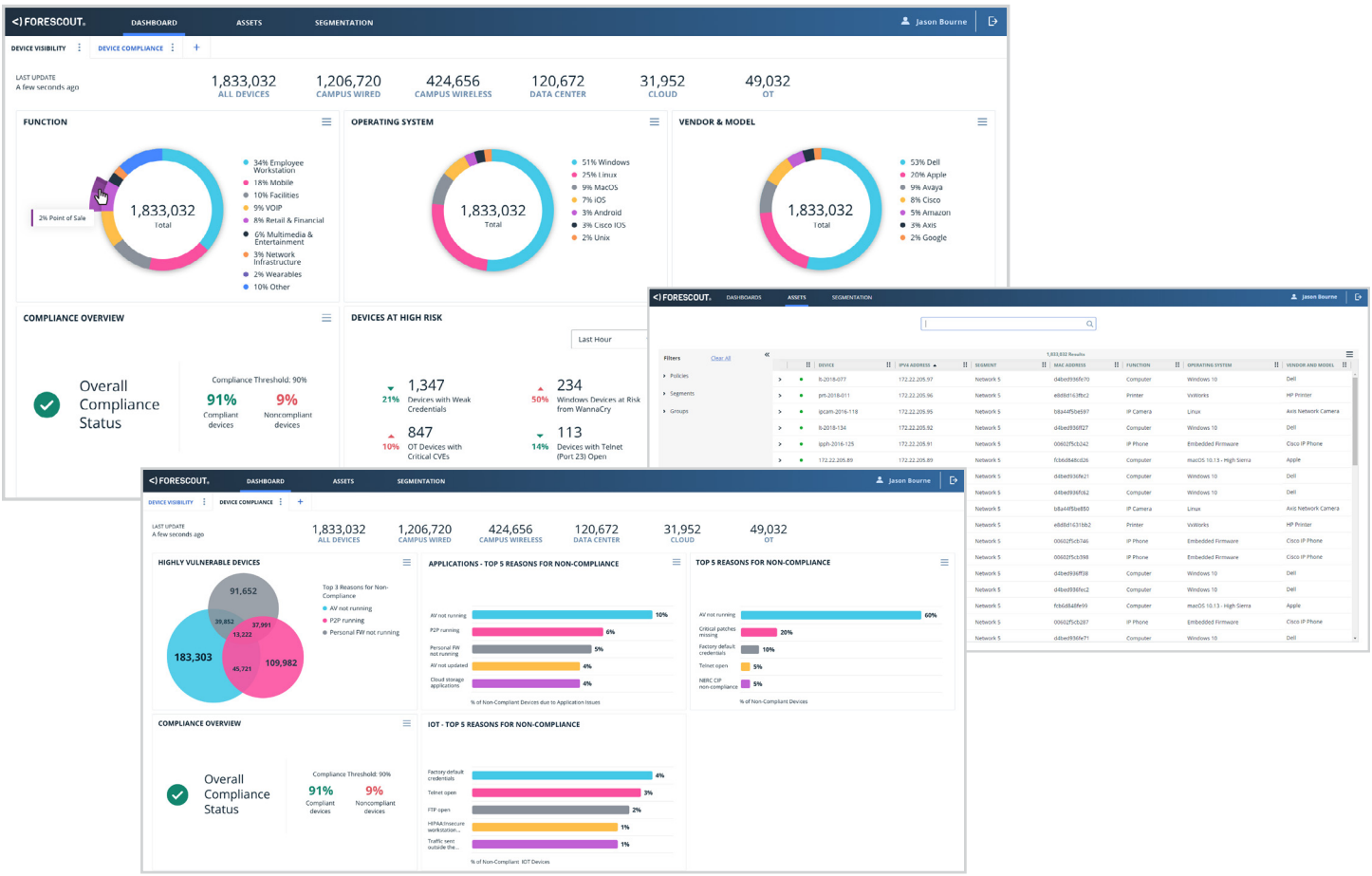
新たなWebベースのユーザーインターフェース経由で、ユーザー視点に立ったコンテキスト情報や、実行可能なインサイトをあらゆるステークホルダーに提供します。当社のダッシュボードで接続デバイスを可視化し、最もリスクの高いエリアやコンプライアンス目標の進捗状況などを担当チームに通知できます。詳細ドリルダウン機能を搭載したリアルタイムのデバイスインベントリにより、運用担当者は迅速にデバイスを検知でき、常に脅威を先回りしてエンタープライズ環境を維持できます。カスタマイズやオプション共有も簡単にできるため、IT部門全体でリスク情報を共有しやすくなり、対応のスピードアップを実現できます。

インサイトを素早く取得： 標準のデバイス可視化・コンプライアンスダッシュボードにより、以下を実現できます。

- 自社の接続デバイスすべてに関する機能、OS、ベンダー/モデルを識別
- コンプライアンスの閾値を設定し、稼働中のポリシーすべてに照らして現状を監視
- 以下をはじめとする高リスクデバイスをピンポイントで検出：
  - 脆弱な認証情報をもつIoTデバイス、オープンポートその他の設定不備
  - セキュリティ更新を怠っている、または脆弱性を有するWindowsデバイス
  - セキュリティエージェントが稼働していない、または不正アプリを実装したデバイス
  - クリティカルな共通脆弱性識別子(CVE)をもつOTデバイス
- もっとも頻度の高いポリシー違反のほか、複数のポリシーに違反しているデバイス（ファイヤーウォールやウィルス対策なしでP2Pアプリを実行中、など）を識別

プロアクティブなギャップ対応： Webベースのアセットビューを活用し、以下をスピードアップできます。

- キャンパス、データセンター、クラウド、OTにまたがるデバイスインベントリ全体の検索
- ポリシー、ネットワークセグメント、デバイスプロパティ別のフィルター検索
- デバイスロケーションをピンポイントで特定し、対応平均時間（MTTR）を短縮



eyeExtend Connectのアプリケーションエコシステム

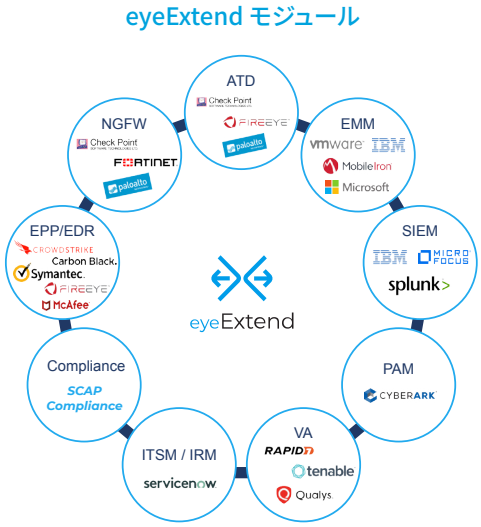
当社プラットフォームを、サードパーティー製IT/サイバーセキュリティシステムと統合することで、デバイスコンテキストの共有、ワークフローのオーケストレーション、対応の自動化を実現できます。当社の最新eyeExtend製品モジュール群は、25種類以上の主要製品と標準で統合可能なため、既存システムへの投資価値を高めることができます。Forescout 8.2では、当社が開発・サポートする自社製品に加え、当社コミュニティの参加者が共同開発可能なアプリケーションのエコシステムを新たに提供します。これにより、さらに多くの外部システムとの連携アプリを構築できます。

eyeExtend Connectはクラウドソーシングの力を活用するため、お客様およびパートナーの皆様は当社プラットフォームとの連携用アプリを迅速に開発、利用、共有できます。デバイスコンテキスト情報を外部ツールと簡単に共有し、ワークロードの自動化およびアクションの実行が可能なため、システム全体での機動性を高め、平均対応時間(MTTR)を短縮できます。

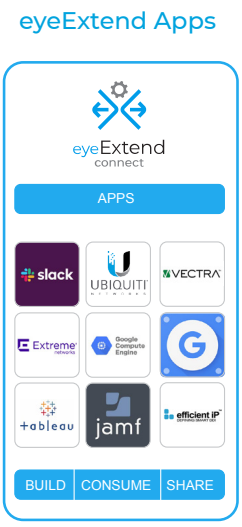
容易なアプリ開発:標準的なPythonスクリプトやJSON Data Exchangeスタンダードにより独自アプリを柔軟に開発し、価値を早期に実現

操作性:当社コミュニティが開発した各種アプリのなかから、ネットワーク環境全体でのデプロイ/カスタマイズ/移植性にすぐれたアプリを選択可能

簡単に共有:当社コミュニティへの貢献/ベストプラクティスの反映、同僚とのアプリ共有、クラウドソーシングの活用により、既存のIT投資効果を増大



Forescoutによる開発



NEW コミュニティにて開発

エンタープライズ全体でのマクロ・セグメンテーション

Forescout 8.2では、eyeSightおよびeyeControlの最新のイノベーションによってeyeSegmentを補完することで、複数のネットワークドメインや散在する適用ポイントを網羅し、エンタープライズ全体でのセグメンテーションを支援します。このシームレスな体験により、ネットワークセグメンテーションを確実に設計・導入し、大規模環境におけるゼロトラストセキュリティを実現できます。

- 論理的分類にもとづくユーザー、デバイス、アプリケーション、サービス間のトラフィックフローのマッピングおよび可視化
- 論理的セグメンテーションポリシーの設計・シミュレーション・改善により、ポリシーの影響レベルを適用前に把握
- セグメンテーションの健全性(ハイジーン)をリアルタイムで監視し、ポリシー違反に対応
- ネットワークドメインや散在する適用ポイント全体を網羅するセグメンテーションコントロールを確実に適用

OT環境におけるセキュリティおよびリスク管理

SilentDefenseとForescout 8.2の統合により、OTおよびコンバージド環境のセキュリティおよびリスク管理の多種多様なユースケースに対応できます。

- SilentDefenseが提供するOTデバイスの分類および脆弱性情報をeyeSightと共有し、eyeSightの新ユーザーインターフェース経由でIT/OTネットワーク全体での可視化を統合
- IT/OT一体型センサー内蔵アプライアンスで、コンバージド環境におけるデバイスを検出・分類
- 同一のIPアドレスレンジを複数のサイトや製造ライン、工場で再利用する「ネットワークのクローン環境」において、デバイスを一意に識別し、ポリシーを適用
- SilentDefenseの最新機能(NERC CIP準拠レポートの拡充、業務に影響を与えない選択的アクティブインスペクションによる詳細な可視化、複数のリスク要因を影響スコアに集約したアセットリスクフレームワーク機能など)をOT環境に活用

Arista環境におけるネットワークアクセスコントロール

Forescout 8.2はAristaのインフラと直接連携が可能なため、Aristaおよび様々なデバイスが混在する環境におけるネットワークアクセスコントロールを当社経由で実施できます。これにより、802.1X認証に依存することなく、エージェントレス方式でITおよびIoTデバイスを検出・制御できます。

- ネットワークに接続するあらゆるITおよびIoTデバイスをリアルタイムで検出・評価
- eyeSightおよび3rdパーティからのコンテキスト（デバイスタイプ、所有者、ユーザーの役割、デバイスの準拠状況/セキュリティポスチャーなどの情報）をもとに適切なネットワークアクセスをプロビジョニング
- 様々なネットワークアクション（制限、セグメント化、検疫、デバイスブロック等）を状況に応じて自動化し、リスクを緩和

パブリッククラウドへの展開

これまで、当社のデバイス可視化やコントロールはオンプレミスの物理/仮想マシン上でのデプロイに限定されていたため、クラウドファーストのIT戦略を掲げる組織にとっては完全性に欠けるものでした。Forescout 8.2は、当社のセンサーアプライアンスやエンタープライズマネジメント機能を貴社のAmazon Web ServicesやMicrosoft Azureクラウド環境にデプロイ可能なため、オンプレミスのフットプリントを削減できます。さらに、パブリッククラウドへのデプロイを、VMware、Hyper-V、KVMのプライベート基盤の物理/仮想アプライアンスと柔軟に組み合わせることもできます。

物理　仮想　パブリック　ハイブリッド
いずれかまたはすべての組み合わせ

エンタープライズスケール

Forescout 8.2は、大規模エンタープライズに求められる厳格な要件を満たす、圧倒的なスケーラビリティを提供します。さらに、キャンパス、データセンター、クラウド、IoT/OT環境における接続デバイス数の爆発的な増加にあわせて拡張することができます。

- 業界最大のデバイスクラウドナレッジベースを活用し、1,100万以上のエンタープライズデバイスを分類可能なため、接続デバイス（IoT、OT、ITアセット）をより正確かつ迅速に検出できます
- 200万種類のデバイス（物理、仮想、クラウド、ハイブリッドなどの導入形態を問わず）を単一のデプロイで管理します

FORESCOUT

フォアスカウト・テクノロジーズ
株式会社

〒101-0051 東京都千代田区
神田神保町2－11－15

住友商事神保町ビル2階

詳細は Forescout.com をご覧ください