FORESCOUT

What's New
Forescout 8.1

デジタルトランスフォーメーションの勢いが衰えることなく継続する中、企業はますます多くのスマートデバイスを自社のネットワークに接続することで、業務を自動化し、効率性を高めています。IoT、IIoT、またはOTを問わずこれらのデバイスによって、かつてないほどの拡大と多様化が企業ネットワークにもたらされています。

このビジネストランスフォーメーションを推進するには、従来は分断されていたネットワーク間での接続性と情報共有を高めなければなりません。その結果、ITとOTの融合が進み、キャンパスに接続されたITデバイス、クラウドベースアプリケーション、オペレーショナルテクノロジーシステムの間で新たなデータフローが生まれます。このようなメリットがある一方、事業リスクも高まります。なぜならば、脅威アクターは新たに相互接続されたネットワーク上を水平方向に移動し、機密情報にアクセスしたり、業務を混乱させたりすることができるようになるからです。

> 「2021年までに、OTセキュリティの70%（現在35%）がCIO、CIS、またはCSO部門によって直接管理されるだろう」[1]
>
> – Gartner、2018年5月

ITとOTの統合により、現在このビジネスエコシステム全体を保護することを任されているCIOとCISOに新たな要求が課されています。ITチームは、ユーザーデバイス、アプリケーション、およびデータの管理に責任を持つだけではなく、セキュアかつ、効率化されたビジネスオペレーションに対しても責任を持つようになるのです。これらの課題に取り組むためには、完全なデバイスの可視性とコントロールが必要です。

Forescout 8.1: ITおよびOTのセキュリティの為の統合されたデバイス可視化とコントロール

Forescout 8.1は、融合されつつあるITネットワークとOTネットワークに対して、統合的にデバイスの可視化とコントロールを行う世界ではじめてのプラットフォームです。Forescout 8.1を利用することで、企業は相互接続された環境にあるすべてのデバイスの状況を把握することや、サイバーリスクとオペレーションリスクの両方を軽減するアクションをオーケストレーションすることができます。Forescout 8.1の新たな機能は以下の通りです。

- Cisco ACI、Microsoft Azure、Beldenの産業用スイッチング環境の可視化。これにより、データセンター、クラウド、OTのネットワークがカバーされ、ITドメインとOTドメイン全体に必要な見通し線を得ることができる。
- IoTデバイスとOTデバイスの自動分類の広範囲にわたる強化、産業用制御システム（ICS）の脆弱性アセスメント、不正デバイスの検出。これにより、ITネットワークとOTネットワークの両方のサイバーレジリエンスが高まる。
- FortinetファイアウォールとCisco DNA Centerによるセグメント化のオーケストレーションと、ServiceNowを利用したインシデント対応。これにより、コントロールを自動化し、セキュリティオペレーションの効率を高めることができる。
- 物理環境、仮想環境、クラウド環境、ハイブリッド環境に広がる200万台という比類ない数のデバイスを単一のデプロイメントで管理

エンタープライズスケール

物理環境、仮想環境、クラウド環境、ハイブリッド環境に広がる200万台のデバイスを単一のデプロイメント内で管理

デバイスの発見	自動分類	リスクアセスメント	コントロールの自動化
Microsoft Azure、Cisco ACI、Beldenの産業用スイッチング環境の可視化、およびより低レイヤーのOTネットワークスタックの可視化	100以上のITプロトコルとOTプロトコルを対象とした新しいディープパケットインスペクションより、医療用、産業用、建設用オートメーションデバイスと、IoTデバイスの自動分類を強化	OTやICSの新たな脆弱性評価、および偽装者を特定し抑止する不正デバイス検出によって、サイバーレジリエンスを向上	FortinetファイアウォールとCisco DNA Centerによるネットワークセグメント化のオーケストレーション、およびServiceNowのITSMとSecurity Operationsを利用したインシデント対応

強化されたデバイス可視化

セキュリティは、ネットワーク上にあるものを確実に把握することから始まります。つまり、全てのデバイスを、デバイスがネットワークに接続された瞬間に特定するということです。2019年には、9億台以上の物理デバイスと仮想デバイスが企業ネットワーク上に存在していると予測されています。この増加するデバイスの大部分は、IoTデバイスおよびOTデバイスと、パブリッククラウドおよびプライベートクラウドのインスタンスです。

> 2023年までに標準的なCIOが管理するエンドポイントの数は、2018年の3倍以上になる」[2]
>
> – Gartner、2018年9月

- Forescout 8.1はこれらの分野の可視化を引き続き強化。キャンパス、データセンター、クラウド、OTのネットワーク全体にあるデバイスすべてを一元表示
- マルチクラウドの可視化は、AWSとVMware向けの既存機能に加え、Microsoft Azureに対応
- Cisco ACIとの統合により、データセンターのSDN環境を可視化
- Beldenの産業用スイッチング製品群との統合により、OTネットワークの可視化範囲を拡大
- OTネットワークスタックの低レイヤーをパッシブに監視することで、監視デバイス、プロセス制御デバイス、計測デバイスを可視化

より優れた自動分類

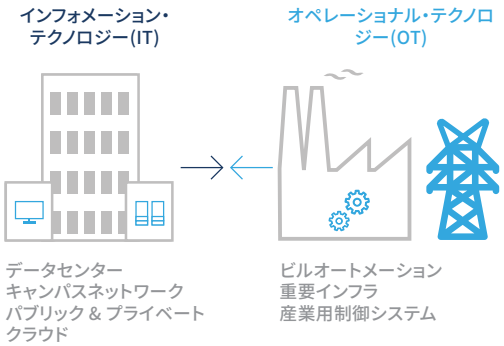
IoTデバイスやOTデバイスの多様化により、企業がこれらを正確に特定し整理することは困難になりつつあります。これらのデバイスを保護するために、ターゲットを絞ったポリシーを作成し実施するには、きめ細かな分類が不可欠です。Forescout 8.1は、広範な機能拡張が行われており、以下の機能を通じ、より多くのデバイスを自動分類し、そのコンテキストを活用してポリシーを実施することができます。

- カバレッジの強化により、500以上のOSバージョンと、5,000以上のデバイスベンダーとモデルを特定
- 350以上の医療テクノロジーベンダー（Global Top 20を含む）のヘルスケアデバイスを分類
- 100以上のITプロトコルとOTプロトコルを対象とした新しいディープパケットインスペクションにより、製造、エネルギー、石油およびガス、公共事業、鉱業、重要インフラの何千もの産業オートメーションデバイスを自動分類
- IT、IoT、OTをカバーする800万台以上のデバイスから成るForescout Device Cloudに実現された、分類の効率性、スピード、カバレッジを強化

クロスドメインでのリスクアセスメント

OTの脆弱性評価

ITネットワークとOTネットワーク間の接続が進む中、それぞれのドメインに存在するデバイスのリスクプロファイルを把握することが重要です。どちらかの側にある脆弱なデバイスが侵害を受けたことにより、脅威がドメインを横断して業務の中断や金銭的な損失を引き起こす場合があります。



- Forescout 8.1では、ネットワーク上の高リスクデバイスについて把握できる脆弱性評価機能に、従来のWindowsに加えて、OTとICSの脆弱性評価を追加
- Forescoutからの頻繁な更新により、ICSの最新の共通脆弱性識（CVE）に関する最新情報を利用できるため、脆弱なデバイスを特定し、修復アクションをオーケストレーションすることができる。
- 定期メンテナンス期間内にのみパッチを適用または修復できる脆弱な産業デバイスおよびオペレーションデバイスについては、Forescoutはそれらが修復可能になるまで、デバイスを「安全な」ネットワークゾーンにセグメント化するなどの緩和策を実施できます。

不正デバイスの検出

IoTとOTの急増がもたらすもう一つの問題は、デバイスのなりすましと、MACアドレスの偽装です。IoTデバイスとOTデバイスは、ネットワークアクセスを可能にするためにしばしば長いホワイトリストに含まれている為、ネットワークにアクセスしようとする脅威アクターは、より多くのMACアドレス群をターゲットにすることができます。こうしたデバイスのディスプレイ画面は安全対策が施されていない場合がしばしばあり、MACアドレスが盗み見られてしまう可能性があります。偽装者は容易に正規デバイスを偽装してネットワークにアクセスし、業務の中断を引き起こしたり、機密情報を入手したりすることができます。

Forescout 8.1は、特許出願中の新しい不正デバイス検出機能を備えており、MACアドレススプーフィングによるなりすましを特定し、阻止します。

- ネットワークの常時監視により、複数のなりすまし行為を有線ネットワークおよび無線ネットワークの全体で検出（同時接続、同一ロケーションでの交代、別ロケーションでの交代の試みを含む）
- Forescoutが、被害を受けたデバイス及びなりすましデバイスを特定。その後ポリシーに基づき、なりすましの企てをブロックし、悪意のあるアクセスを防止
- Forescoutを利用することで、MACスプーフィングに対する耐性を監査人に実証し、監査コンプライアンスを向上

コントロールのオーケストレーションと自動化

セキュリティツールから通知されるセキュリティ上およびコンプライアンス上の問題が増加しており、ITセキュリティチームはその対処に忙殺されています。こうしたセキュリティツールには、優先順位を決定するための十分なデバイスコンテキスト、またはコントロールを実施するための自動化機能が不足しています。そのため、高度な技能を持つセキュリティチームは、些末な問題に手動で対処することに時間を浪費しており、プロアクティブにリスクを軽減することや、脅威に対して迅速に対応することに集中できていません。Forescout 8.1により、デバイスコンテキストを提供すると共に、アクションのオーケストレーションとコントロールの自動化を可能にします。

「自社のSIEMまたは専用プラットフォームを通じたセキュリティ自動化機能、オーケストレーション機能、対応機能を備える企業組織の比率は、2018年の5%未満から2021年には70%まで上昇する」[3]
– Gartner、2018年12月

ネットワークのセグメント化

企業がIoTやOTの次世代セキュリティアーキテクチャを構築するに際し、セグメント化が主要な役割を担います。従来型デバイスとは異なり、IoTデバイスやOTデバイスはエージェント経由で定期的にパッチを当てたり、セキュアにしたりすることができません。したがって、これらのデバイスを論理セキュリティゾーンにセグメント化することが、リスク軽減戦略として不可欠になります。

ForeScout 8.1を利用することにより、複数のエンフォースメントテクノロジーを横断して、セグメント化をオーケストレーションすることができます。これには以下に挙げる新しい統合が含まれます。

- Fortinetファイアウォールを用いたセグメント化コントロールの自動化を、既存のPalo Alto NetworksおよびCheck Pointとのオーケストレーションに追加し、次世代ファイアウォールの多様なサポートを強化
- Cisco DNA Centerによるセグメント化コントロールのオーケストレーションをサポート。既存のVMware NSXやAWSに加えソフトウェアディファインド・ネットワーキングテクノロジーおよびクラウド・ネットワーキングテクノロジーとの連携を強化

クロスドメインでのネットワークのセグメント化

インシデント対応の自動化

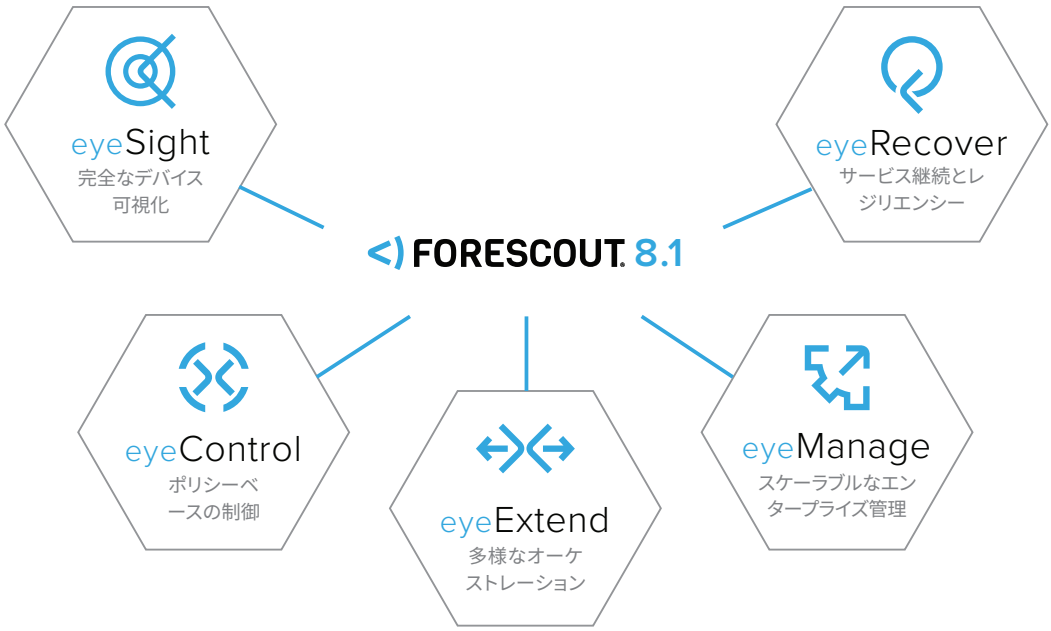
ますます多くのITチームやセキュリティチームが、低リスクの問題に対処する手段として、対応の自動化に注目しています。それによって、スキルのある人員が、リスク軽減や、その他のビジネスインパクトのある成果に集中することができるからです。Forescout 8.1は、ServiceNowのITSMやセキュリティオペレーション製品と連携することで、インシデント対応の自動化、迅速化可能になります。

- ServiceNowのITSMとの新たなオーケストレーションにより、サービスインシデントの作成と、設定コンプライアンスに対するポリシーベースの対応を自動化
- ServiceNowのセキュリティオペレーションとの新たなオーケストレーションにより、セキュリティインシデントの作成と、高リスクのデバイスや侵入を受けたデバイスへの対応を自動化
- インシデントの修復が完了した後、ServiceNow CMDBとの高度なオーケストレーションにより、Configuration Items（CI）を更新することで、閉ループサービスとセキュリティ管理ワークフローを円滑化

スケーラブルで柔軟なプラットフォーム

ForeScout 8.1は大規模エンタープライズ環境における厳しい要件を満たす、比類ないスケーラビリティと柔軟性を提供します。

- 単一のインストールで、キャンパス、データセンター、クラウドネットワーク、OTネットワークに広がる最大200万台の物理デバイス、及び仮想デバイスを管理可能
- モジュール式の製品群は、進化するビジネス要件に適応するための柔軟性を提供します。まずForescout eyeSightでデバイス可視化から始め、制御の自動化、セキュリティのオーケストレーション、運用の耐障害性、およびOTセキュリティのための強力な機能を追加していくことが可能
- 購買ニーズに柔軟に対応するため、Forescoutの全ソフトウェア製品で、無期限ライセンス、または期間ベースのサブスクリプションを提供



1『2018 Strategic Roadmap for Integrated IT Security』– Gartner、2018年5月
2『Gartner Top Strategic IoT Trends and Technologies Through 2023』、2018年9月
3 日Gartner、『Emerging Technology Analysis: SOAR Solutions』、2018年12月7日、Eric Ahlm

詳細については、Forescout.comをご覧ください

FORESCOUT

フォアスカウト・テクノロジーズ株式会社
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