FORESCOUT

ゼロトラストの基本は「100%可視化」

デバイス可視化プラットフォーム「Forescout Platform」によるゼロトラストセキュリティの実現

> 貴重な資産を保護するには可視性が不可欠です。見えないものは守れません。業務エコシステム全体のネットワークをさらに可視化することで、侵入の予兆を素早く検知し、食い止めることができます1。
>
> — 2019年7月 Forrester Research

すべてを疑う

情報セキュリティのゼロトラストモデルはその効果が認められ、各企業のセキュリティ戦略やセキュリティベンダーの開発ロードマップの一部として定着しました。社内ネットワークにおける境界ベースのセキュリティアーキテクチャ（信頼性が高いとデフォルトで考えられている）の失敗例は後を絶たず、コストも増大しているからです。

境界ベースのセキュリティが無意味になりつつある

エコシステム上のパートナー、モバイルワークフォースなどに大きく依存しています。さらに、デジタル変革により、ユーザーやアプリがアクセスするアカウント数やデータ、リソースが増えるため、さらなるアジリティが求められます。調査会社のガートナーは「デジタル変革の結果、ほとんどの企業では、社内よりも社外で展開するアプリやサービス、データのほうが多くなるだろう[2]」と予測しています。

同時に、ネットワークリソースに接続するデバイスの数や種類も、従来のエンドポイント管理をはるかに上回る規模となっています。こうしたデバイス（ビジター用デバイス、BYODシステム、IoTデバイスやオペレーショナルテクノロジーを含む）の多くは社内管理エージェントを実行しない/できないため、セキュリティ部門ではネットワーク上の当該デバイスを把握しきれず、ユーザーの特定、セキュリティ状態の評価、アクティビティ管理などの作業に支障が出る恐れがあります。

境界ベースのセキュリティのシステム的な欠陥から、それに代わるゼロトラストモデルが、Forrester Research社のアナリストにより2010年に開発されました。ゼロトラストとは、企業のセキュリティ部門向けの概念・アーキテクチャモデルです。このモデルでは、セキュアなマイクロ境界の実現、難読化によるデータセキュリティ強化、過度なユーザー権限やアクセス付与に伴うリスクを制限し、分析や自動化を活用してセキュリティ課題の検出率や即応性を飛躍的に向上するためには、現行ネットワークをどのように再設計すべきかを解説しています。

ゼロトラスト：概念モデルから包括的フレームワークまで

ゼロトラストモデルの初期段階では、既存のセキュリティコントロールを生かした実務運用に関する方向性は固まっておらず、あくまでも保護目的でのセグメンテーションや最小権限によるアクセスコントロールの概念が中心でした。その後、基本モデルが進化・成熟し、Forrester社が名付けた「ゼロトラスト・エクステンデッド(ZTX)」エコシステムが確立しました。ZTXは、必要なセキュリティテクノロジーを、ゼロトラストの原則が当てはまる標準的エンタープライズ環境における7つの主要領域（ネットワーク、データ、人材、ワークロード、デバイス、可視化/分析、自動化/オーケストレーション）に落とし込んだ包括的フレームワークです。

ZTXフレームワークは、セキュリティ部門が以下を実現するセキュリティテクノロジーについて理解するうえで有効です。

- ネットワーク分離、セグメンテーション、セキュリティに関する原則
- データの分類、分離、暗号化、コントロール
- ネットワーク上のインフラリソースとユーザーを保護すると同時に、ユーザーからも当該リソースを保護
- パブリック/プライベートクラウド上のワークロードアプリケーションスタックの保護
- 異機種環境全体でのゼロトラストの統制/プロセスの自動化およびオーケストレーション
- 拡張エンタープライズ環境のあらゆる場所をくまなく保護・可視化・分析

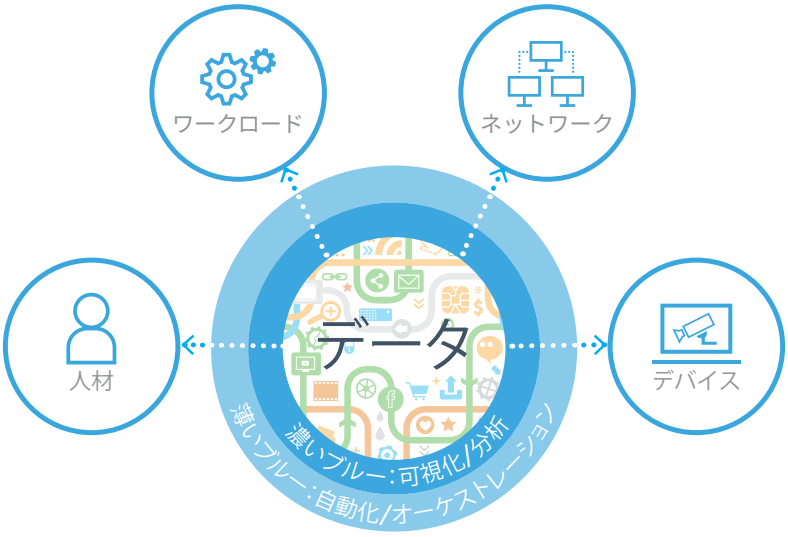

図1：Forrester Researchの提唱するZTEエコシステムフレームワークの7領域

可視化戦略に最適な Forescout Platform

ゼロトラスト戦略の重要な側面は、エンドポイントエージェントが搭載/実行されているか否かを問わずネットワークに接続するすべてのデバイスを検出/分類すること、およびデバイスやユーザーID/認証レベル、ソフトウェアスタック、設定準拠やセキュリティの状態を詳細分析したうえで最小権限のアクセスポリシーを厳格に適用することです。アクセス制限ポリシーを適用するには、ネットワーク上のあらゆるモノを可視化したうえで、アセスメントやコントロールを実施する必要があります。

Forrester Research社はゼロトラストにおける「可視性」を重視しています。同社のアナリストであるChase Cunningham氏は「貴重な資産を保護するには可視性が不可欠です。見えないものは守れません。業務エコシステム全体のネットワークをさらに可視化することで、侵入の予兆を素早く検知し、食い止めることができます1」と述べています。

こうした戦略を実現するには、デバイスの包括的な可視化および、従来のエンドポイント管理システムでは対応できないホスト（ビジター用/BYODデバイス、エージェントが無効化された社内エンドポイント、不正デバイス、IoTデバイス、ネットワークスイッチ/ルーター、製造現場その他のOTシステム、パブリッククラウド上の仮想マシン等）の可視化・コントロールに対応可能なソリューションが求められます。

可視化プラットフォーム「Forescout Platform」:可視化によるリスクコントロール

当社は、進化する先端ネットワーク技術を、自社のゼロトラスト対応プラットフォームに随時反映させています。当社のForescout Platformは、皆様の異機種/拡張エンタープライズネットワークにエンドポイントが接続した瞬間にそれらを動的に特定・評価するエージェントレス方式のセキュリティソリューションです。ユーザー、所有者、OSを迅速に認識すると同時にデバイス設定、ソフトウェア、サービス、パッチ状況、セキュリティエージェントの有無なども判断します。その後、対象デバイスの修復、コントロール、常時監視を行います。

当社はこうした機能を、企業が管理するマネージドデバイス、管理対象外のビジター用デバイス、物理/仮想サーバー、ネットワークインフラ、産業用オペレーション/制御システム、IoTデバイスに適用します。ソフトウェアエージェントやデバイスの予備知識は必要ありません。現行環境に簡単に実装でき、ほとんどの場合インフラ改修やアップグレード、エンドポイントの再設定は不要です。物理/仮想環境、ハイブリッドクラウド環境で「シームレスに動作可能」であることが当社の大きな強みです。

調査会社のForrester Researchは「ゼロトラスト構成要素の5つのカテゴリの機能において、Forescout Platformはマーケットリーダーである」として、ForescoutをZTXベンダーエコシステムのゼロトラストプラットフォーム提供ベンダーに指定しました1。また、2019年第4四半期のZero Trust Waveレポート3でもForescoutを「IoT/OT領域におけるゼロトラストセキュリティベンダー」として挙げました。

ゼロトラストによるデバイスの可視化、分析およびコントロール

Forescout Platformは、IP接続されたあらゆるデバイスを100%検出し、分類します。さらに、接続デバイスの状況をリアルタイムで把握できるよう、リスクおよびデバイスポスチャー評価を継続的に実行します。そこで得られたインテリジェンスを駆使し、ポリシーベースの自動統制やデバイス毎のアクションのオーケストレーションを行うことで、効果的なゼロトラストセキュリティ基盤が実現します。

エージェントレス方式でのデバイス検出 – Forescout Platformは、エージェントレス方式のアクティブ・パッシブメソッドを併用し、キャンパスからデータセンター、クラウド、OTネットワークにいたるまで、異機種/拡張エンタープライズネットワーク上のあらゆるデバイス(PCやラップトップ、物理/仮想サーバー、モバイル/IoTデバイス、クラウドインスタンスやOTシステム)を検出・分類します。対象デバイスの802.1X認証有無にかかわらず、ベンダー固有のネットワーク機器、既存インフラのアップグレード、スイッチの再設定やポートの変換などは不要です。

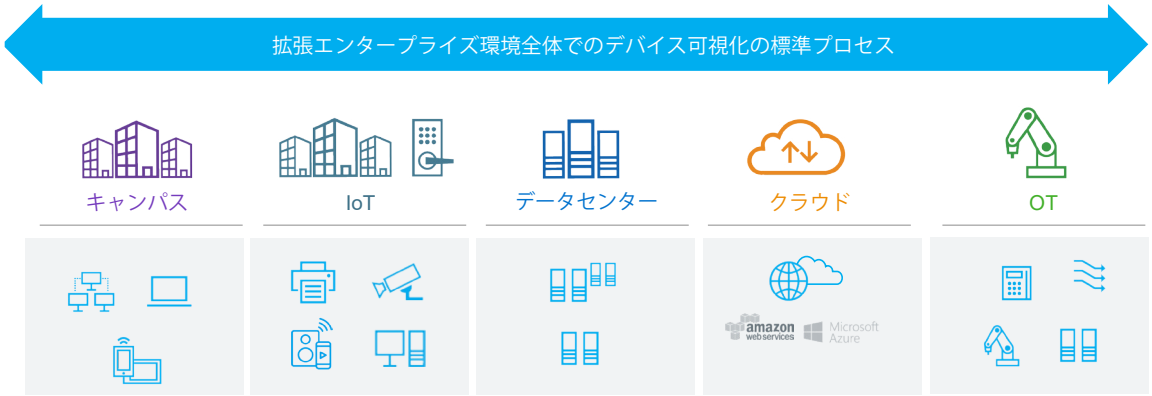

図2:拡張エンタープライズ環境のデバイス可視化およびコントロールを実現するForescout Platform

デバイス検出からアセットインテリジェンスまで - 当社は様々な検出・プロファイリング手法を活用し、デバイスID、状態、挙動に関する膨大な情報を迅速に生成し、常時更新します。得られたデータをもとに皆様の環境全体での詳細なアセット一覧を生成します。この資産情報を、様々な意思決定やアクションの判断材料およびリスク回避策のベースとしてご活用いただけます。さらに、セグメンテーションマッピング、プランニング、ポリシー作成時に重要となる「デバイスとデータソース間の通信およびシステムの依存性」についても、Forescout Platformで可視化・監視できます。

図3：あらゆるIP接続デバイスの詳細データを抽出可能な当社の分類プロセス

常時可視化およびポリシーベースのデバイスコントロール - Forescout Platformのポリシーエンジンは、このアセットインテリジェンスを活用し、デバイスの挙動がポリシーに準拠しているか否かを常に評価します。デバイスのネットワークアドミッションや認証その他任意の属性をもとに、リアルタイムでポリシーを起動します。たとえば、アウトバウンドでインターネットにアクセスする新規IoTデバイスを当社プラットフォームで検出し、制限付きネットワークセグメントに自動アサインする、などの対応も可能です。デバイスのセキュリティの状態変更（アンチウィルスエージェントまたは暗号化ソフトウェアが無効化された、または機能不全となった、等）についても検出可能です。当社プラットフォームは、デバイスがネットワークに接続される、または接続遮断される都度、各デバイスを再評価します。これらのコンテキスト情報を、関連する外部システムとリアルタイムで共有し、ポスチャー評価に必要なアクション（脆弱性や侵害痕跡に対処するためのデバイス再スキャン）を発動します。

当社プラットフォームでは、各種コントロールに必要なアクションをデバイス上で直接、またはネットワークインフラ経由（後述）で実行できます。ホストベースのコントロール項目には、アプリケーションの起動/停止、ウィルス対策セキュリティエージェントの更新、周辺デバイスの無効化、エンドユーザーの確認要求などがあります。必要に応じ、Forescout Platform側で、デバイスのパッチ適用や脆弱性アセスメント、エンドポイント保護、暗号化その他のセキュリティソフトの再インストールなどの自動修復措置を、外部ツールと連携のうえ実行します（後述）。

ゼロトラストの対象となるデバイス

企業にとって、ネットワークを出入りする膨大な数の「非管理デバイス㈠」を検出し、セキュリティを確保することは深刻な課題です。IoTデバイスの急増により、Forrester社いわく「潜在的な侵害領域が巨大化」1したため、ITやセキュリティ部門は、対応に追われています。IT-OTの融合が進むにつれ、散在するテクノロジーや責任の所在に関する線引きがあいまいになってきています。また「非管理」の問題だけでなく、OTデバイスなどはもはやエアギャップ状態にないため、セキュリティの観点でも懸念があります。企業のCIOは、こうした構造的変化の矢面に立たされていますが、脆弱性にあふれたコンバージド環境を制圧するためには、洗練された手法が不可欠です。当社のエージェントレス方式によるデバイス可視化・コントロールおよびパッシブ型の検出手法はこうした問題の解決に最適なアプローチです。システムを停止することなくIT、OT両方のデバイスを検出・管理できる理想的な機能の数々により、ForescoutはIoTセキュリティ市場の代名詞となりました。

当社はSecurityMattersの買収により、ネットワークベースの状況認識技術を拡充し、IT環境だけでなくOTや産業制御システム(ICS)まで網羅可能となりました。今般の統合により、100以上のIT/OTプロトコルのディープパケットキャプチャ/インスペクション、ネットワークマッピング、フロー分析、ポリシー/挙動監視、ネットワークフォレンジック、脅威のアセスメント、リスクスコアリングなどの対応力が増強されました。

当社のIoTおよびOTセキュリティのノウハウは、調査会社であるForresterからも高く評価されています。実際Forrester社は、「IoT/OTデバイスのセキュリティは、企業が解決すべき最難関のひとつであり、この領域に特化したセキュリティについては、Forescoutが最適なベンダーだ。これこそ同社の中核能力であり、IoT/OTセキュリティを実現するForescout Platformやその各種機能は競合他社を凌駕している。最大限の可視性により運用コントロールを最大化する同社のゼロトラストへのアプローチこそが、究極のセキュリティを実現する鍵となる3」と述べています

「IoT/OTデバイスのセキュリティは、企業が解決すべき最難関のひとつであり、この領域に特化したセキュリティについては、Forescoutが最適なベンダーだ。これこそが同社の中核能力であり、IoT/OTセキュリティを実現するForescout Platformやその各種機能は競合他社を凌駕している」—2019年10月 Forrester Research

ゼロトラストにおけるネットワーク機能

動的なネットワークセグメンテーション –ゼロトラストフレームワークの中心となる概念は「マイクロセグメンテーション」です。ただ、分散環境全体にわたり有効なセグメンテーションポリシーの設計、適用、維持は骨の折れる作業でした。従来のセグメンテーションソリューションは労働集約型であり、トラフィックの依存性を把握するためには手作業でのフロー分析やログ取得が必要でした。このため、人的ミスや一貫性に欠けるセグメンテーションポリシー、さらには業務に支障をきたすなどのリスクが増えます。ほとんどのセグメンテーションは、複雑なマルチベンダー/マルチドメイン構成のエンタープライズ環境で実行されるため、大規模な工数が必要となります。

当社は「すべてのネットワークセグメンテーションを網羅できる単一の解決策はない」と考えています。各種ツールは一長一短であり、得意とするユースケースやネットワーク領域もまちまちです。当社の考えるポリシーベースのゼロトラストセグメンテーション戦略は、アプリケーション中心型かつ、デバイス/役割中心型およびバウンダリー中心型のアプローチであり、エンタープライズネットワーク環境のすべての領域（キャンパス、データセンター、IT/OT、クラウド）をカバーします。

セグメンテーションの適用を簡素化・スピードアップするために、当社はコンテキスト中心の多層型アーキテクチャを開発しました。これにより、各種アプリケーション、ユーザー、デバイス、サービスで構成される、今日の幅広いユースケースに対応します。当社プラットフォームと多層型のネットワークセグメンテーション手法を組み合わせることで、拡張エンタープライズ環境における全体像を完全に把握していただけます。さらにオーケストレーション機能により、環境全体でのサイバーリスクや運用リスクを低減することができます。

図4：エンタープライズ全体でのネットワークセグメンテーションのベストプラクティスとして当社が推奨する3層型アーキテクチャ。最上位のポリシーレイヤーには当社のForescout eyeSegmentを実装。

- ポリシーレイヤー：当社は2019年、拡張エンタープライズ環境全体での動的ネットワークセグメンテーションの設計、プランニング、デプロイの迅速化を支援する製品「Forescout eyeSegment」を発表しました。eyeSegmentは、包括的なデバイス可視化および、当社の別製品「eyeSight」が提供するリアルタイムの詳細コンテキストをベースとした製品です。eyeSightはエージェントを必要とせず、管理/非管理デバイス、IoT/OTデバイスのみならず、仮想インスタンスやクラウドベースのワークロードの検出・プロファイリングについても優れた機能を発揮できるため、IP接続システムすべてに対するゼロトラスト原則を適用していただけます。eyeSegmentではまず、トラフィックフローおよび、ユーザー/アプリ/サービス/デバイス間の依存性を可視化します。その後、ポリシーの設計、シミュ―レーション、監視を行い、貴社環境全体における影響を把握します。

- **コントロール・オーケストレーションレイヤー：**2番目のレイヤーは、ポリシー適用の基盤テクノロジーやネットワークドメイン全体を、ベンダーに依存することなく連携するポリシーのオーケストレーション支援レイヤーです。ネットワークアクセスコントロールの代表的ソリューションであるForescout eyeControlは、キャンパスやデータセンター、クラウド環境上の汎用的スイッチ、ルーター、ポリシー適用ポイントと連携のうえ、ポリシーベースのセグメンテーションを設定します。Forescout eyeExtend製品群により、オーケストレーションレイヤー上の統合プロセスの合理化を支援します。
- **ポリシー適用レイヤー：**3番目のレイヤーは、ベンダー別の適用ポイントを連携し、物理/仮想ネットワーク全体にわたるセグメンテーションコントロールを実行するレイヤーです。さらに、既存のポリシー適用システムも活用できるため、これまでの投資も無駄になりません。

ゼロトラストベースのアクセスブローカー： Forescout Platformは、ネットワークインフラ経由でデバイスコントロールアクションを発動します。ユーザーID/役割/認証/デバイスステートの統合ビューをもとに、ネットワークアクセスプロビジョニングに関する一元的ブローカーサービスおよび意思決定ポイントを提供し、30種類以上のスイッチやワイヤレスベンダー製品とネイティブで統合可能です。さらに、Linux OS実行ルーターとの直接統合も可能です。また、ネットワークスイッチに関するVLANアサインの変更、ACLの追加、スイッチポートの無効化の対応も可能です。ワイヤレスコントローラーについては、MACアドレスのブラックリスト化、ユーザーの役割変更に対応するほか、リモートVPNユーザーを制限することも可能です。

当社のエージェントレスプラットフォーム「Forescout Platform」は、IP接続するレガシーデバイスをすべて検出・評価し、アクセスのプロビジョニングを実行できるため、ゼロトラストの実務展開にあたり大きな強みとなります。IP接続デバイスをすべて可視化・コントロールし、あらゆるIT/OTネットワークインフラと一律に統合します。

当社のエージェントレスプラットフォーム「Forescout Platform」は、IP接続するレガシーデバイスをすべて検出・評価し、アクセスのプロビジョニングを実行できるため、ゼロトラストの実務展開にあたり大きな強みとなります。今後、多くのWindows OSがサポート期限を迎えるため、この点は極めて重要です。

ゼロトラストによる自動化およびオーケストレーション機能

Forescout Platformは、インフラ全体のセキュリティ管理と連携し、これまでバラバラだったセキュリティ製品が一体化します。ネットワーク、セキュリティおよび管理の相互運用を実現する独自のテクノロジーをForescout eyeExtend製品群経由のAPIで増強・拡張することで、セキュリティやIT管理に関する70種類以上のサードパーティ製品との統合が実現しました*。システムが一体化することで、対応のスピードアップ、業務効率の大幅改善、卓越したセキュリティを実現できます。

当社は以下の3つの方法で、セキュリティ自動化およびオーケストレーションを実現します。

- **コンテキストにもとづく洞察（インサイト）のリアルタイム共有** - 当社はエンドポイントデバイスのIDや設定、セキュリティの詳細を常時監視し、貴社が所有/利用する外部のセキュリティ/管理システムと動的に共有します。双方向型のデータ交換により、外部ツールのルールエンジンに適用するプロパティの全体像が拡充でき、ポリシーやアクションを精緻化できます。
- **ワークフローの自動化** - 従来は手作業で分析し、システム全体に展開していたポリシーベースの意思決定を、システム間で共有できます。ワークフローやプロセスの自動化により、連携のとれた即応態勢を実現できます。
- **対応アクションの自動化** - IT担当者は、高度な脅威検知システム、SIEMソフト、脆弱性アセスメントツールなど、様々なセキュリティ製品を利用してセキュリティの問題を把握できます。当社は、これらのセキュリティ製品から得られたインサイトを即時に適用し、対応アクションを自動実行できるほか、広範囲なポリシーベースのコントロール（デバイスの隔離、脅威を排除するためのエンドポイント修復など）も適用可能です。

ゼロトラストにおけるワークロード機能

Forescout Platformは、各種インフラコンポーネントやワークロード自体を利用してハイブリッドデータセンターやクラウド環境全体の物理/仮想サーバーの検出、分類、プロファイリングを実行します。さらに、ワークロードがこれらの環境をスピンアップ・ダウンする都度、追跡・監視し、可視性のギャップを防止します。当社プラットフォームは、下位レベルのハイパーバイザーやクラウドプロパティから、ワークロードにインストール済/実行中のアプリに至るまでの情報を収集します。その後、収集したコンテキストを活用し、権限を付与されたユーザーやデバイスのみに個別ワークロードへのアクセスを許可することで、ゼロトラストポリシーへの準拠を徹底します。

ゼロトラストにおけるユーザー機能

Forescout Platformは、汎用的なディレクトリやID管理システムと統合可能なため、利用可能なユーザー情報（役割やリソースアクセス権限など）を取得できます。この情報を、検出したデバイス設定情報やセキュリティステート、コンプライアンスデータと照合することで、デバイスおよびユーザーインサイトにもとづくリソースアクセスの判断が可能となります。また、ユーザー挙動の常時監視、特権アクセス管理システムとの統合により、権限違反のユーザーアカウントを検出できます。

ゼロトラストによるデータ機能

当社は、暗号化、難読化、およびポリシーで必要なその他の情報セキュリティソフトウェアの存在と動作状態を可視化することにより、すべてのIP接続デバイスにわたるデータセキュリティを支援します。必要なアプリが欠如、または無効となっている場合、当社プラットフォーム側でポリシーベースのアクション（ユーザーへのアラート、管理者への通知、修復されるまでデバイスを隔離する等）を起動できます。

ゼロトラストを成功に導くデバイスの完全可視化

Forescout Platformの価値を詳しくご理解いただくために、様々な方法をご提供します。

- 試乗会のご体験：プラットフォーム導入前・導入後の違いについて、5つの効果的ユースケースをもとにハンズオンでお試しいただけます。
- デモのご依頼：当社のデモページからパーソナルデモをご用命ください。情報満載のオンデマンド・デモおよび動画オプションもお申込みいただけます。
- 事業価値のROI（投資効果）判定ツールのご利用：Forescout Platformが実現する定量的な事業価値をわずか10分で試算していただけます（IDCの事業価値モデルによる計算）。
- 当社コンサルティングサービスにお問い合わせください：現行環境をゼロトラストモデルに再編中の皆様は、当社コンサルタント にお申しつけください。当社では製品導入やプロセス開発、システムインテグレーションに加え、ネットワークアクセスやエンドポイントコンプライアンスのベストプラクティスについて、徹底したトレーニングを実施しており、経験豊富なコンサルタントがご案内いたします。

*2019年9月30日現在

***出典**

1 2019年7月11日付Forrester Research「The Zero Trust eXtended Ecosystem Road Map: The Zero Trust Security Playbook」

2 2019年4月付「Gartner Market Guide for Zero Trust Network Access」

3 2019年第4四半期版「The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers」

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