FORESCOUT

エージェントレスなデバイスの可視性とコントロール

効果的なサイバーセキュリティの基盤となる機能

> “価値あるアセットを保護する上で可視化はキーとなります。ビジネスエコシステム全体のネットワークアクセスが可視化されればされるほど、違反となり得る進行中の兆候を迅速に検出し、阻止できる確率が高くなります。”[1] ”
>
> **– Chase Cunningham博士**
> **Forrester Research主席アナリスト**

デバイスの可視化とコントロールが必要な理由

ネットワークに接続するすべてのデバイスを検出、分類、評価、およびコントロールする機能は、システムとビジネスの安全を確保するために不可欠な前提条件です。すべてのセグメントにおけるすべての物理/仮想エンドポイントのリアルタイムの把握、設定とセキュリティ状態の詳細な洞察、および自動化されたポリシーベースのアクセスコントロールによってのみ、システムとデータのセキュリティを確実に確保し、インシデントに迅速かつ正確に対応し、コンプライアンスを達成し、ビジネスとインフラストラクチャのリスクを管理し、セキュリティ効率を最適化できます。攻撃者は、管理されておらずセキュアでないデバイスを常に探しているため、盲点が見つかると悪用します。可視化とコントロールは、セキュリティとコンプライアンスの要なのです。

デバイスの可視化とコントロールが困難な理由

従来、ネットワークエンドポイントの管理は、各デバイスにインストールされたソフトウェアエージェントによって行われてきました。これはほとんどのエンドポイントが静的で企業所有のPCまたはサーバーであったため効果的でしたが、モビリティ、多様なデバイスタイプ、そして仮想化の台頭により、コンテキストの可視化とコントロールがかなり複雑になりました。今日のエンタープライズ環境において、クラウドとデータセンターのセグメントは、仮想マシン上で稼働し仮想化ネットワークによって接続された、動的にプロビジョニングされたワークロードで一杯です。キャンパスセグメントはセキュリティエージェントの入っていないユーザー所有のBYODノートパソコン、タブレット、スマートフォン、およびセキュリティエージェントをサポートしないIoTデバイスであふれています。また、オペレーショナルテクノロジー（OT）セグメントによって、エージェントをサポートせず、独自プロトコルで通信し、ミッションクリティカルなプロセスを管理し、内部への介入を受け付けない膨大な数のデバイスが追加されています。IT組織では、これらの多様な環境すべてにおよぶ、包括的な可視性およびコントロールを提供するエージェントレスソリューションを緊急に必要としています。

フォアスカウトのソリューション: エージェントレスなデバイスの可視化とコントロール

フォアスカウト・テクノロジーズは、今日の動的で多様な環境におけるデバイスの可視化とコントロールという課題に対応する、ネットワークセキュリティへのエージェントレスアプローチを開発しました。フォアスカウトのデバイスの可視化とコントロールのプラットフォームは、キャンパス、データセンター、クラウド、およびOTネットワークのすべてのデバイスにおよぶ継続的で統合されたビューを提供します。

フォアスカウトのプラットフォームは以下を検出します。

- キャンパスネットワークのデバイス: ノートパソコン、タブレット、スマートフォン、BYOD/ゲストシステム、IoTの各デバイス
- データセンターのインフラストラクチャ: 仮想マシン、ハイパーバイザ、物理サーバー、仮想/物理ネットワーク
- パブリック/プライベートクラウドのインフラストラクチャ: AWS®、Microsoft® Azure® 、およびVMware® の仮想マシン
- OTおよび産業制御システム (ICS) : 医療、産業、およびビルの自動化用の各デバイス
- 物理的およびソフトウェア定義のネットワークインフラストラクチャ: スイッチ、ルーター、ファイアウォール、VPN、ワイヤレスなアクセスポイントとコントローラ

拡張されたエンタープライズ全体でデバイスを可視化

図1: フォアスカウトのデバイスの可視化で拡張されたエンタープライズ全体を把握します。

> “リスクと信頼の評価と可視化、およびコンテキストの交換は、デジタルビジネスにとっての免疫システムとなります。”[2]
>
> **— Neil MacDonald 氏、ガートナー社副社長兼アナリスト**

当社が提供すること

フォアスカウトはIT組織に次のことを提供します。

- すべてのネットワーク上のすべてのIP接続デバイスの検出: キャンパス、データセンター、クラウド、産業環境全体の物理/仮想デバイス
- 多様なIT、IoT、OT/ICSデバイス、さらに仮想マシン (VM) とクラウドインスタンスを、デバイスのタイプと機能、ベンダー、モデル、オペレーティングシステム、バージョンの識別に基づいてリアルタイムに分類
- ポリシーコンプライアンスに対するデバイスのセキュリティ状態を評価し継続的にモニタリング
- ポリシー、業界指令、ネットワークセグメンテーションなどのベストプラクティスへの準拠
- 非準拠またはセキュリティが侵害されたデバイスを制限、ブロックまたは隔離
- エンドポイント、ネットワーク、およびサードパーティのコントロールアクションの自動化

すべてのセグメントのすべてのIP接続デバイスとOTシステムの検出方法

フォアスカウトのプラットフォームは、20を超える設定可能な情報収集技術を提供します。その技術は、主要なITおよびOTネットワークのスイッチ、ルーター、ワイヤレスアクセスポイント、ファイアウォール、VPNコンセントレータ、およびデータセンターとクラウドのソリューションプロバイダーとの高度な統合を利用するものです。ネットワークトラフィックを受動的にモニタリングし、多数の異なるプロトコルストリームを解析し、ネットワークインフラストラクチャとエンドポイントの両方と直接やりとりすることができます。フォアスカウトの可視性技術には次のものが含まれます。

- **ネットワークとエンドデバイスの両方に対して受動的な方法:** この例として、スイッチおよびワイヤレスコントローラからの**SNMP**トラップの受信、**SPAN**ポートのモニタリングとトラフィック内のプロトコルストリームの解析（フォアスカウトでは、100を超えるITおよびOTプロトコルに高度なパケット検査を提供）、フローデータの収集と分析、または**DHCP**リクエストおよび**HTTP**ユーザーエージェントのトラフィックの評価が含まれます。**802.1X**が実装されている場合、フォアスカウトはビルトインまたは外部の**RADIUS**サーバーをモニタリングできます。
- **ネットワークインフラストラクチャに対してアクティブな手法:** この例には、接続されているデバイスおよびVMのポーリングスイッチ、**VPN**コンセントレータ、ワイヤレスコントローラ、およびプライベート/パブリッククラウドのコントローラが含まれます。ユーザーおよびデバイスのデータについて、フォアスカウトのプラットフォームはディレクトリサービス、Webアプリケーション、または外部データベースにクエリを行います。
- **エンドデバイスに対してアクティブな手法:** この例として、**NMAP**を使用した接続デバイスのためのネットワークセグメントのスキャン、**WMI**または**Mac**を使用した**Windows**デバイスのリモート検査、SSHを使用した**Linux**デバイスのリモート検査、**SNMP**クエリを使用したエンドポイントプロファイリングが含まれます。

デバイスの可視化手法

パッシブテクニック
SNMP traps
SPANポート監視
DHCP リクエスト
HTTP user-agent
TCP フィンガープリント
DICOMプロトコル解析 (メディカルイメージデバイス)
ICS-OTプロトコル解析 (60+ プロトコル)
フロー解析
Netflow
Flexible Netflow
IPFIX
sFlow
DHCPリクエスト(ip-helper経由)
HTTP user-agent (URLリダイレクト経由)
RADIUSリクエスト
MACアドレスOUI

インフラに対するアクティブテクニック
物理ネットワークインフラへのポーリング
コントローラベースのネットワークインフラストラクチャー連携
Meraki
Cisco ACI
プライベートクラウド(仮想環境) 連携
Vmware
パブリッククラウド連携
AWS
Azure
ディレクトリサービスへのクエリ (LDAP)
Webアプリケーションへのクエリ (REST)
外部DBへのクエリ (SQL)
オーケストレーション(ITSM, UEM, EPP, EDR, VA)

エンドポイントに対するアクティブテクニック
エージェントレスでのWindows検査 (WMI, RPC, SMB)
エージェントレスでのMacOS, Linux 検査(SSH)
NMAP
SNMP
エージェントベース検査 (SecureConnector)

図2: フォアスカウトのデバイス可視化方法.

複数のデバイス可視化手法があることの優位性

フォアスカウトのプラットフォームは、セットアップ時に容易に設定でき、設定後の変更も簡単な、多数の異なる検出方法を提供します。そのため比類なく高い柔軟性、効率性、効果性を発揮します。

OTネットワークに対してパッシブな手法のみで検出、分類、評価: OTネットワークは多くの場合、工程管理システムや業務を妨げる可能性があるアクティブなプロービングやスキャン技術に適切な環境ではありません。いったんデバイスを理解すれば、能動的な方法は選択的に適用することができます。フォアスカウトのプラットフォームは、SPANトラフィックモニタリング、および約100ものOT特有のプロトコルに対するディープパケットインスペクションという完全にパッシブな組み合わせによって、OTネットワーク全体のデバイスの可視性を提供します。フォアスカウトは、BACnet、CIP、DNP3、Ethernet/IP、ICCP、IEC 69-0870-5- 104、IEC 60850、IEEE C37.118、Modbus/TCP、OPC、PROFINET、およびSiemens S7といった産業標準プロトコルをサポートします。さらに、ABB、Emerson、GE、Honeywell、Rockwell/Allen-Bradley、Schneider Electric、およびYokogawaなどの主要メーカーの独自プロトコルもサポートします。

大規模環境におけるコスト効率性の高いデプロイメント: リモート可視化技術によって、小規模サイトをローカルアプライアンスなしにモニタリングできるため、全体の導入費用を削減できます。

検出後のさらなる洞察: 分類および評価: パッシブおよびアクティブなプロファイリング技術をレイヤー化することで、フォアスカウトのプラットフォームはMACおよびIPアドレスによって単に接続デバイスを特定するだけでなく、それ以上のことができます。分類は、多数のレイヤーのコンテキストを取得し関連付け、各デバイスの詳細なプロファイルを作成するプロセスです。評価は、検出されたデバイス状態のプロパティを、アクセスコントロールと修正策の基準であるセキュリティポリシーと比較するプロセスです。どちらのプロセスにも詳細な調査が必要です。

インテリジェントな自動分類

詳細なポリシーを作成するには、各デバイスの完全なコンテキストがキーとなります。セキュアに管理する最善の方法の決定には、運用上のコンテキストまたは各デバイスの目的を知る必要があります。デバイスの増加と多様性により、これらのコンテキストを手動で収集するのはほぼ不可能で、適切なコンテキストなくポリシーを作成すると運用におけるリスクとなります。フォアスカウトでは、従来型、IoT、およびOTの各デバイスを、多次元の分類法によってデバイスの機能とタイプ、オペレーティングシステムとバージョン、ベンダーとモデルを自動的に分類します。

フォアスカウトのプラットフォームは下記を自動分類します。

- 500を超える各オペレーティングシステムのバージョン
- 5,000を超える各デバイスベンダーの製品とモデル
- 350を超える医療テクノロジーベンダーのヘルスケアデバイス
- 製造、エネルギー、オイル、ガス、ユーティリティ、鉱業、その他の重要な経済基盤産業で使用される何千もの産業制御デバイスおよび自動化デバイス

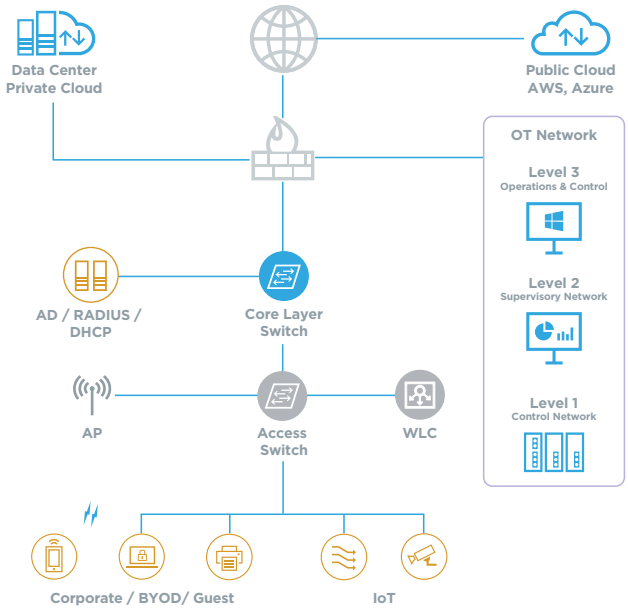
フォアスカウトのDevice Cloudによってプラットフォームの自動分類が強化され、この豊富なコンテキストの情報源がデバイスの成長と多様性に確実に対応し続けます。フォアスカウトの調査チームは、現在ある800万超のデバイス*からのインテリジェンスを当社のDevice Cloudで利用し、新しいプロファイルを頻繁にパブリッシュして、デバイス全体における分類の有効性、範囲、速度を向上します。

デバイスポスチャの評価

デバイスの分類によって、デバイスの用途という観点での運用上のコンテキストがわかります。つまり、そのデバイスが何であるかがわかります。しかし完全なコンテキストという観点では、各デバイスの正常性とセキュリティ状態をはかる手段が必要です。フォアスカウトではネットワークを継続的にモニタリングし、接続デバイスの設定、状態、およびセキュリティポスチャを評価します。そしてリスク特性を決定し、セキュリティおよび規制のコンプライアンスポリシーに準じているかどうかを決定します。たとえば、次のような重要な質問に回答します。

- デバイスが、最新のOSパッチを含む承認済みオペレーティングシステムで作動しているか
- セキュリティソフトウェアがインストール済みで機能しており、最新パッチでアップデートされているか
- 承認されていないアプリケーションが稼働しているデバイス、標準設定に違反しているデバイスはないか
- デバイスがデフォルトまたは簡単に破られるパスワード（IoTデバイスにとっての特定のリスク）を使用していないか
- スプーフィング技術により正当なデバイスになりすましたデバイスを含む、不正デバイスが検出されたか
- 接続デバイスのうち、どれが最新の脅威に最も攻撃を受けやすいか

デバイスの分類と評価



誰が？
- ユーザー
- 名前
- Eメール
- 役職
- グループ
- サブスクリプション/アカウント
- IAMオーナー/ロール

何が？
- 機能
- OS
- ベンダー/モデル
- IPアドレス
- ブラウザエージェント
- ポート
- 仮想/物理
- MACアドレス

ポスチャ
- アプリ
- サービス
- プロセス
- バージョン
- レジストリ
- パッチ
- 暗号化
- アンチウィルス

どこで？
- スイッチ
- コントローラ
- スイッチポート/SSID/VLAN
- AWS/Azure
- リージョン
- VNet/VPC
- Purdueレベル

図3: フォアスカウトのプラットフォームは、各デバイスをタイプ別に迅速に分類し、コーポレートマネージド、アンマネージド、IoT/OT、物理または仮想かどうかを明確にして、デバイスのコンプライアンスステータスを評価するのに役立ちます。

可視化を利用してコントロールを可能に

フォアスカウトのプラットフォームには、カスタマイズ可能な一連のポリシーに照らしてデバイスを継続的にチェックするポリシーエンジンを備えており、ネットワーク上のデバイス動作を決定づけて実行し、継続的でリアルタイムのモニタリングを最大200万のデバイスに提供します。ポリシーは、特定のデバイス上またはネットワーク内で発生するイベントによってリアルタイムにトリガされます。これらのイベントは、スイッチポートへのプラグインまたはIPアドレス変更などの、ネットワークアドミッションイベントであることがあります。さらに、RADIUSサーバーから受信するイベントのような認証イベントであることもあります。ポリシーはまた、デバイス属性の変更によって呼び出されることもあります。図4は、ポリシーがトリガされた際にフォアスカウトのプラットフォームで利用できるコントロールアクションの範囲について説明しています。

フォアスカウトのコントロールアクション

控えめ → 通知する → 準拠させる → 制限する → 厳格

	通知する	準拠させる	制限する
ネットワークコントロール	**ネットワーク/管理者**	**ネットワーク**	**ネットワーク**
	管理者へEメールを送信	ゲストネットワークへ移動	デバイス隔離（VLAN、仮想FW）
	Syslog/CEFメッセージを送信	ワイヤレスユーザのロール変更	スイッチポートをオフ
	ヘルプデスクチケットをオープン	自己修復VLANへの割り当て	ワイヤレスまたはVPNアクセスをブロック
	他のITシステムとコンテキスト共有	不正デバイス/インフラを制限	ACLでアクセス制限
ホスト コントロール	**ホスト/エンドユーザー**	**ホスト**	**ホスト**
	エンドユーザーへEメールを送信	必須アプリ/プロセスを開始	未承認アプリの終了
	オンスクリーン通知を送信	アンチウィルス/セキュリティエージェントをアップデート	NIC/デュアルホームの無効化
	Webページへリダイレクト	OSアップデート/パッチ適用	周辺機器デバイスの無効化
	エンドユーザーの確認をリクエスト	外部ドライブのコンプライアンス	修正アクション/システムをトリガ

図4: カスタマイズ可能なコントロールアクションによって、設定されているセキュリティポリシーに基づいて、適度から厳格までの適切なレベルのコントロールを実行することが可能になります。

ポリシーエンジンは2つの範囲のコントロール機能を利用します。1つ目はフォアスカウトのネイティブ機能で、2つ目は主要セキュリティ製品およびIT管理製品との統合によるデータ交換およびコントロールオーケストレーションを利用するものです。

ネイティブのコントロール機能

フォアスカウトのネイティブ機能には、ネットワークベースおよびホストベースのコントロールが含まれます。ネットワーク内のコントロールは、ポリシーベースのセグメンテーションを提供して、ユーザーID、ロール、デバイス状態に基づいてアクセス権を付与または制限します。ホストベースのコントロールは、アプリケーションの開始/中止、アンチウィルスおよび他のホストベースセキュリティエージェントのアップデート、または周辺機器デバイスの無効化を実施することでデバイスのセキュリティ状態を強化します。ポリシーエンジンはこれらのポリシーを、デバイスの企業ネットワーク全体における場所や移動、またはデータセンターやクラウドへの移動に関係なく自動的に適用します。

拡張されたコントロール機能

フォアスカウトのプラットフォームは、多数の異なるタイプのセキュリティおよびIT管理製品全体におよぶリアルタイムのデバイスコンテキストの共有およびワークフローのオーケストレーションによって、ポリシー実施の自動化、システム全体におよぶ応答の加速化、およびリスク低減を実現します。フォアスカウトは以下のカテゴリーにおいて主要ベンダーとの統合を提供しています。

- 高度な脅威検出
- クライアント管理ツール
- エンタープライズモビリティ管理
- エンドポイント保護、検出、応答
- ITサービスマネジメント
- 次世代ファイアウォール
- 特権アクセスの管理
- セキュリティ情報とイベントの管理
- 脆弱性評価

これらの統合により、フォアスカウトはインフラストラクチャ全体規模のセキュリティをオーケストレーションし、ユーザー、デバイス、アプリケーション、およびトラフィックの分類に基づくポリシー重視のコントロールを提供します。リソースに対して正確でフレキシブルなコントロールときめ細かいアクセスポリシーが施行されるため、IT組織は動的なネットワークセグメンテーションを導入し、リアルタイムの状況認識に基づくコンテキスト対応のセキュリティポリシーを作成することが可能となります。

フォアスカウトのコントロールアクション

ネットワークアクセスコントロールに基盤を置くフォアスカウトのプラットフォームは、ネイティブおよび拡張されたコントロール機能の双方の組み合わせによる、極めて幅広いデバイスコントロール機能を実現します。そのためIT組織に強力なネットワークセキュリティツールを提供することができます。

フォアスカウトのプラットフォームは、以下を行うことで、ユーザープロファイル（ゲスト、従業員、コントラクター）、デバイス分類、およびセキュリティポスチャに基づいてエンタープライズリソースへの**ネットワークアクセスを強化します。**

- ゲストおよびBYODデバイスに識別されたアクセスを付与
- 802.1X認証の有無にかかわらずネットワークアクセスポリシーを実施
- ネットワーク上の疑わしい、不正、またはシャドーITデバイスへの対応措置
- セキュリティが侵害されたデバイスまたは悪意あるデバイスのネットワークアクセスを制限またはブロック
- 非準拠のデバイスは、コンプライアンス違反が対処されるまで隔離または孤立

フォアスカウトのプラットフォームは、コンプライアンス評価を自動化し、内部セキュリティポリシー、外部標準、および業界規制に継続的に遵守するための修復コントロールを実施することで、**デバイスコンプライアンスを向上します。**その主な機能には以下が含まれます。

- エンドポイントが適切に設定されていることを確実にし、破られやすいパスワードまたはデフォルトパスワードを含む重大な設定違反に対する修正を開始する
- 必要なアプリケーションおよびセキュリティエージェントがインストールされ、稼働し、最新状態にアップデートされていることを確実にする
- リスクを持ち込む、またはネットワーク帯域またはリソースの生産性に不必要な負荷を与える可能性のある権限のないアプリケーションを無効化またはブロックする
- ハイリスクな脆弱点および重要なパッチの不足を識別し、修復アクションを開始する
- 必要なセキュリティソフトウェアのインストール、エージェントのアップデート、セキュリティパッチの適用などの修復アクションをプロアクティブに実施
- AWS、Azure、およびVMwareを含むクラウドデプロイメントにおける設定コンプライアンスのポリシーを導入し、コントロールを自動化

フォアスカウトのプラットフォームは、共通のポリシーフレームワークによって、拡張エンタープライズ内の異なるエンフォースメントテクノロジー全体にセグメンテーションポリシーを適用することで、**動的なネットワークセグメンテーションを導入します。**フォアスカウトのプラットフォームは次のことができます。

- デバイスのプロパティ、分類、およびセキュリティポスチャに基づいてセグメンテーショングループへデバイスを動的に割り当て
- キャンパスおよびOTネットワーク内のVLAN、ACL、WLANのコントロールおよびタギングを介してセグメンテーションエンフォースメントを適用
- AWS and VMware NSX®などのパブリックおよびプライベートのクラウド環境でセキュリティグループ/タグを介してセグメンテーションコントロールを適用
- 非準拠で脆弱な（特に、スケジュールされたメンテナンス枠でしかパッチまたは修復することができないような）デバイスを分離ゾーンにセグメント化し、ビジネス継続性を確保すると共に、攻撃のリスクを低減する。
- HIPAA、GDPR、PCI、およびSWIFT CSPなどの規制による要求に従い、セグメンテーションポリシーを実施して、特定デバイスおよび重大なデータフローを他のネットワークから分離

フォアスカウトのプラットフォームは、素早く効果的に脅威を阻止し、セキュリティインシデントに応答することで**インシデントレスポンスを加速化し、**業務の中断およびビジネスへのダメージを最小限にします。このデバイスの可視化とコントロールソリューションによって、次のことが可能になります。

- 制御されていないまたは修復されていないハイリスクデバイスの特定
- ATDソリューションとともに、デバイスの接続時に痕跡の情報（IOC）を特定して、対応までの平均時間（MTTR）を短縮
- セキュリティが侵害されたデバイスまたは悪意あるデバイスを迅速に隔離してマルウェアの内部拡散を阻止
- インシデントレスポンスを自動化し、セキュリティが侵害されたデバイスの修復ワークフローを開始
- 有益なデバイスコンテキスト（デバイス接続、場所、分離、およびセキュリティポスチャ）を、クロスファンクショナルなインシデントレスポンスチームおよび独立したテクノロジーに提供することでMTTRを短縮

セキュリティは可視化から始まる

軍の指揮官が常に高い場所を探して確保するには理由があります。高い場所なら近づく敵を遠くから見つけることができ、攻撃が始まる前に防御に備えることができるためです。フォアスカウトのプラットフォームは、IT組織が守るべきネットワークの全体的なビューを提供します。各デバイスを、その接続場所にかかわらず継続的に検出、分類、評価、およびコントロールすることで、フォアスカウトはITセキュリティの戦いの場所を、可視性のある明瞭で管理しやすい場所にします。

フォアスカウトのプラットフォームをお試しください

フォアスカウトのエージェントレスのデバイス可視化とコントロール機能をより深く理解するには、直接見ていただくことが最良です。フォアスカウトでは、フォアスカウトのプラットフォームについて、詳細な洞察を入手していただける以下のような多くの方法を用意しています。

テストドライブの受講: 効果的な6件の使用例を体験できるハンスオンテストドライブによって、フォアスカウトのプラットフォームの使用前と使用後の違いがわかります。

フォアスカウトの完全な可視性とリスクレポートの入手: 詳細なデバイスの可視性およびリスク評価を入手できます。詳細はお近くのフォアスカウト代理店にお問い合わせください。

デモをリクエスト: フォアスカウトのデモページからパーソナルデモをリクエストすると、オンデマンドデモおよびビデオオプションにアクセスできます。

フォアスカウトビジネスバリューROIツールのご利用: フォアスカウトのプラットフォームが貴組織に提供できるビジネスバリューを（IDCのビジネスバリューモデルによる計算によって）わずか10分で数値化します。

*** 2019年3月31日時点**

[1] The Zero Trust eXtended (ZTX) Ecosystem、Forrester Research、2018年1月

[2] Zero Trust Is an Initial Step on the Roadmap to CARTA, ガートナー社、2018年12月

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

米国内フリーダイヤル 1-866-377-8771
国際電話番号 +1-408-213-3191
サポート +1-708-237-6591

詳細はForescout.comをご覧ください