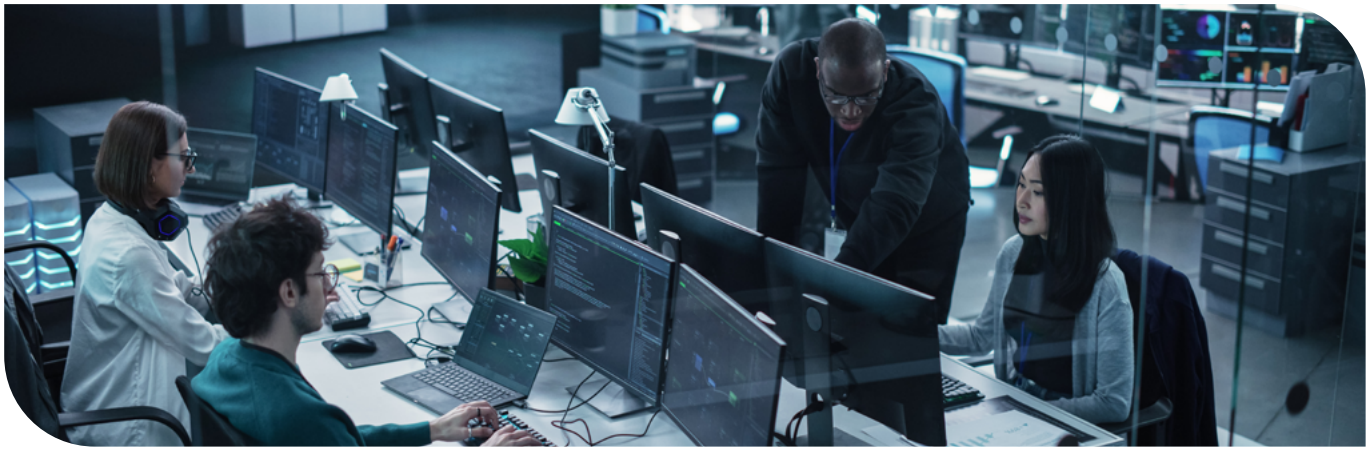
REM（リスクとエクスポージャーの管理）

リスクおよびコンプライアンス状況の特定・定量化・優先順位付け



「国家が関与する高度な攻撃や複雑な攻撃手法に起因するセキュリティ侵害は滅多にない。侵害の大半は、脆弱性リスク管理などの基本対策を適用すれば防げる一連の単純な手順が原因だ」

Forrester Research社が2023年3月に公表したThe State of Vulnerability Risk Managementより抜粋

シャドーITやハイブリッド勤務環境の拡大およびクラウドの普及に伴い、攻撃対象領域が急拡大し、自組織や重要デジタル資産の保護を担うネットワーク・セキュリティチームの対応が追い付いていません。陳腐化した技術、パッチ未適用の脆弱性、「価値の低い」IT資産などは普段見過ごされがちですが、攻撃者にとって格好の標的となります。悪意をもつ第三者はこうした弱点を突いて標的ネットワークを侵害して組織内を横移動し、より価値の高い資産に到達します。脅威や侵害の発生後にアラートを配信する事後対処型セキュリティツールに依存しすぎると、事前対処型のセキュリティ対策であれば防げたはずのダウンタイムを招くことがあります。

各組織においては、自社の攻撃対象領域をより効果的に把握し、業務オペレーションを中断したりユーザーに不便をかけたりすることのないセキュリティプロセスを設計することが求められます。資産やリスク管理の優先順位を機動的に判定し、インシデント発生時の対応や修復に必要なコンテキスト情報を提供してくれるツールも必要です。

リスクポスチャーを徐々に低減します

- サイバーセキュリティ資産管理の合理化
- 資産リスクに関する包括的インテリジェンス
- 各資産のエクスポージャーを明確かつ簡潔に評価
- インシデント対応のスピードアップ
- 予防的セキュリティポリシーの設計
- セキュリティフレームワークに含まれるIoTや医療機器のセキュリティを強化

リスクベースの優先順位判定により、ネットワークセキュリティポスチャーを強化

拡大する攻撃対象領域に圧倒され、縦割り型セキュリティツールが配信するデータのコンテキスト把握に苦戦しているサイバーセキュリティチームの皆様にとって、資産に関する包括的インテリジェンスを提供するForescoutのソリューション「REM（リスクとエクスポージャーの管理）」は、自社の攻撃対象領域におけるセキュリティポスチャーを把握するための基盤となります。リスクベースのアプローチで脆弱性を自動修復し、対象となるセキュリティエコシステム全体にわたる対応アクションの有効性を追跡管理し、リスクポスチャーおよびエクスポージャーレベルを低減します。

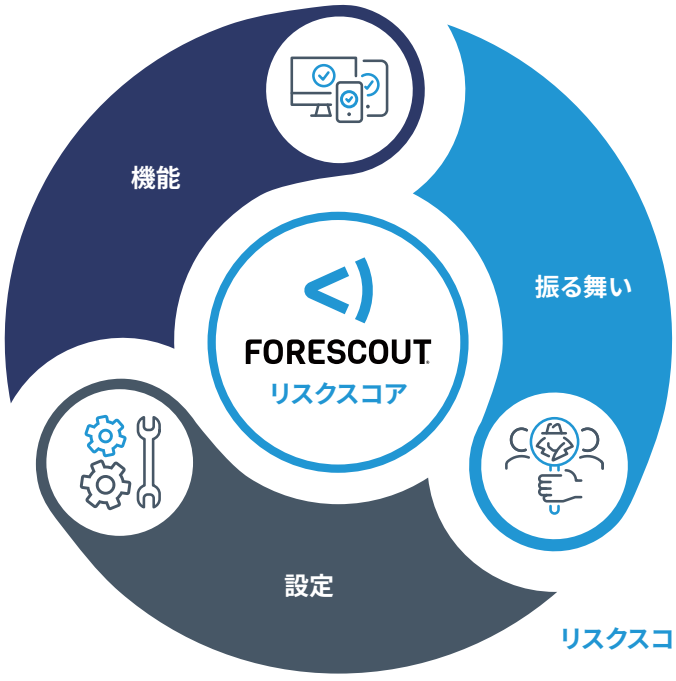
本ソリューションをご利用いただくことで以下を実現し、単なる可視化にとどまらない考察を得られます。

- サイバーセキュリティ資産管理における運用負荷の低減
- 攻撃対象領域のエクスポージャーを見極め、サイバーセキュリティハイジーンをさらに強化
- ネットワーク接続資産すべての設定と状態を把握し、個別リスクの深刻度と攻撃される可能性を正確に評価・分類・定量化
- すでに投資済の既存セキュリティ対策を有効活用し、それらの有効性の追跡管理を通じて徐々にリスクを低減
- インシデント調査および、再発防止に向けた予防的対応ポリシーの設計に要する時間の短縮

● 設定：
- 脆弱性（CVE）
- 悪用可能性（EPSS）
- 外部に露出するサービス

● 機能：
- デバイスの重要度

● 振る舞い：
- インターネットへの露出



リスクスコア = f（検出されたリスク指標、デバイスの重要度）

サイバーセキュリティリスクの優先順位が反映された IT資産インテリジェンスを常時提供

Forescoutの REM（リスクとエクスポージャーの管理）ソリューションは、脆弱性や設定不備に起因するエクスポージャーをもとにリスクを特定し、定量化して優先順位を判定します。複数の要素で構成される独自のリスクスコアを用いて各資産の設定、機能、振る舞い全般にわたるリスク因子を相関付けします。

特定

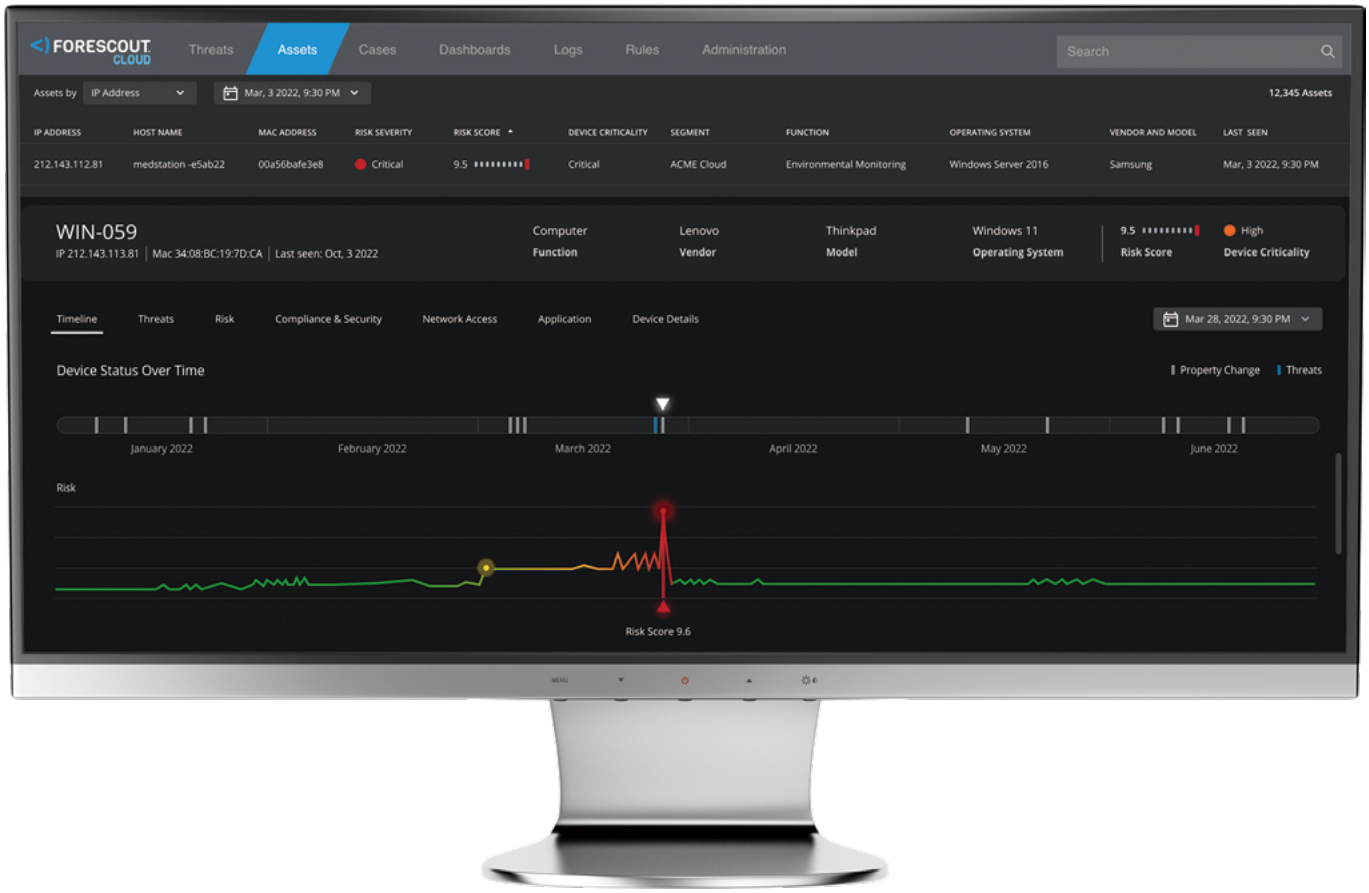
ネットワーク接続資産すべてに明確かつ簡潔なインテリジェンスを適用し、サイバーセキュリティ資産管理を合理化

クラウドを活用した分類手法で、管理デバイスおよび非管理デバイス（IT、IoT、IoMT、OT/ICS）の状態や設定変更の履歴が反映された正確な資産インベントリを常時作成します。

攻撃対象領域における資産インベントリ – クラウドを活用した忠実度の高い手法を用いて管理・非管理デバイスを分類

資産のコンテキスト情報を常時提供 – 検索できるようデータを90日間保管し、資産に関する補完的コンテキストデータ（資産の状態や変更履歴など）を追跡管理

エクスポージャープロファイルのフィルタリング – 侵害された資産と同じエクスポージャー属性をもつ資産の所在地を高度なフィルター機能で特定・追跡することで機動的な修復を支援



Forescoutが選ばれる理由

1. あらゆるデバイスタイプの資産インベントリを常時表示するモダンビュー
2. 設定、機能、振る舞いをもとに複数の要素でリスクを判定する独自のリスクスコア
3. クラウドを活用した忠実度の高い分類手法
4. 特許取得済のディープパケットインスペクション(DPI)テクノロジー
5. 脆弱性の悪用可能性と資産のエクスポージャーとの相関付け
6. 主なセキュリティ製品との連携および対策有効性の追跡管理
7. リスクとエクスポージャーに関する実用的なインサイトによるインシデント対応支援
8. リスクと脅威インテリジェンスの情報を格納するクラウドデータレイク

リスクとエクスポージャー管理に関する当社のアプローチ詳細およびデモのご依頼は、Forescout.jpをご覧ください。

定量化

サイバーセキュリティリスクに関する包括的インテリジェンス

ネットワークの予防的保護と合わせて、設定内容や機能、振る舞いをもとに複数の要素で構成されるリスクスコアを算出し、接続デバイスすべてのサイバーセキュリティリスクポスチャーを常時追跡管理します。

設定内容 – 各資産独自の設定要件を把握し、エクスポージャーレベルや脆弱性が悪用される可能性(以下の指標を含む)を見極めます

- 米国CISAが公開する既知の悪用済脆弱性(KEV)カタログに照らした共通脆弱性識別子(CVE)
- 悪用可能性の予測に関するスコアリングシステム(EPSS)
- 外部に露出するサービスやオープンポートおよび潜在的エクスポージャー(セキュリティ対策、アクセス)

機能 – 各デバイスの機能や用途をもとに、重要度を把握して分類します

振る舞い – 各資産の設定内容や振る舞いの変化を追跡管理し、インターネットへの露出を含む侵害リスクの増大につながる異常値を検知します

優先順位付け

インシデント調査および予防的修復ポリシーの作成にかかる時間を短縮

リアルタイムで常時提供する資産データをITおよびセキュリティチーム全体に配信し、先手を打ったリスク緩和対策やインシデント発生後の調査を支援します。

場所を問わずにアクセス可能な資産インテリジェンス – コンテキスト情報が充実した資産インテリジェンスをIT/セキュリティチーム全体で簡単に共有していただけるよう、Forescout Cloudポータル経由で配信します

リスクベースの優先順位判定 – インシデント調査および修復ワークフローの設計に役立てられるよう、各資産のコンプライアンス状況や設定状態に関するインテリジェンスをリスクとエクスポージャーの属性に反映します

資産コンテキスト情報の経時的変化 – リスク分析やインシデント対応のスピードアップにより、攻撃による影響範囲を極小化し、解決までの平均所要時間(MTTR)を短縮します

FORESCOUT

フォアスカウト・テクノロジーズ株式会社

〒105-0003 東京都港区西新橋1丁目1−1
日比谷フォートタワー 10階

詳しくはForescout.jpへ