RAPID7

ソリューション概要

攻撃可能領域を内外から可視化

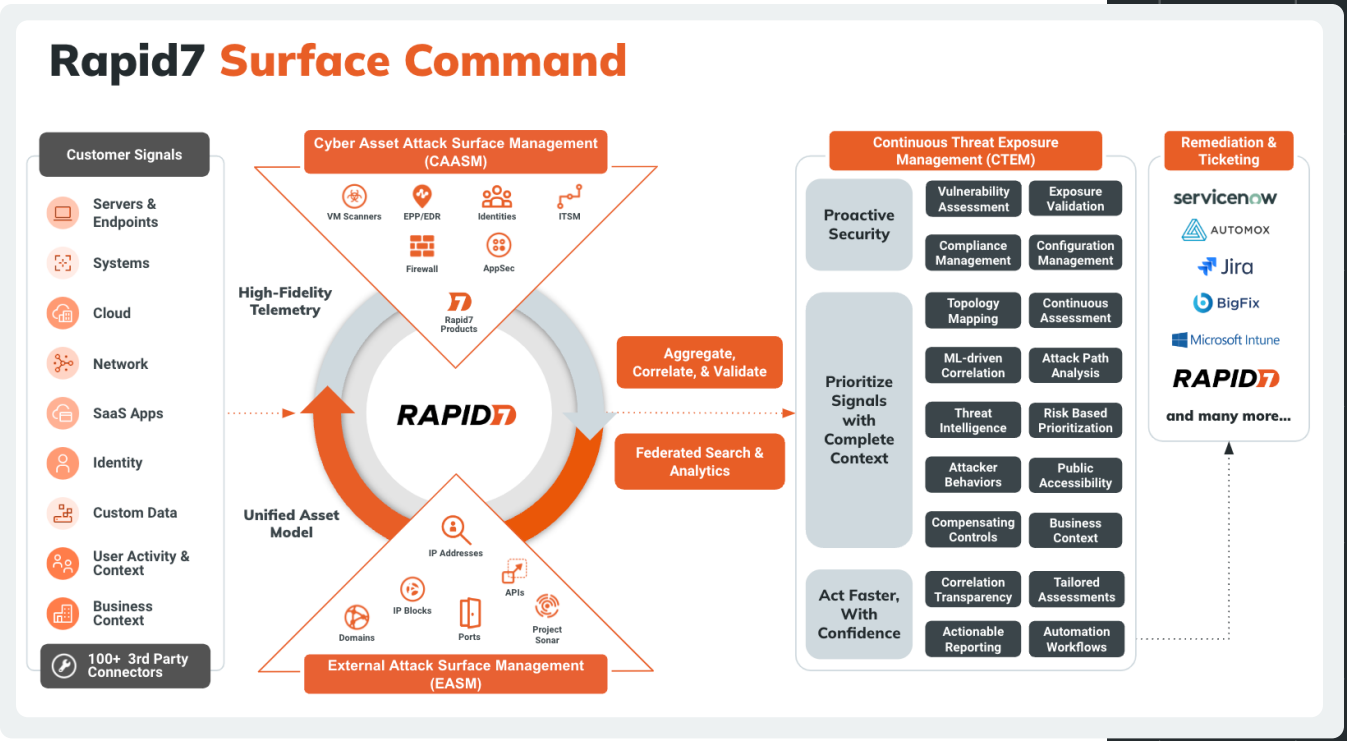
RAPID7 SURFACE COMMAND を活用

> 「資産の大部分（95%以上）を明確に識別し、インベントリを作成できる組織はわずか 17%に過ぎません。」
>
> 2024 Gartner® Innovation Insight: Attack Surface Management レポート

エンドポイントからクラウドまでの継続的外部スキャンと内部資産のコンテキストを組み合わせた Surface Command

組織が環境を管理し、セキュリティを確保するためのツールに支出する費用は増加傾向にあります。しかし、こうしたツールにまたがる可視性のレベルは低下しています。依然として、内部環境、外部環境、ハイブリッド環境には、広大な攻撃可能領域が断片的に残されています。この状況は、攻撃者にとって間違いなく付け入る隙となります。今日、このような状況を実際に管理しているチームは数少ないながらも存在します。このようなチームは、手作業で面倒なデータ入力を行い、資産とセキュリティのデータをスプレッドシートで横断的に関連付け、セキュリティ管理に欠け、パッチがまだ適用されていない、コンプライアンス違反のシステムを特定しています。攻撃者は、こうしたデータの急増を悪用します。大量のデータを隠れ蓑とし、組織がアタックサーフェスを関連付けて視覚化できず、重要な脅威を特定できない状況を濫用するのです。

Rapid7 Surface Command は、攻撃可能領域を総合的に一元管理するため、ハイブリッド環境全体でアタックサーフェスの全体像を把握することで、データのサイロ化を解消します。外部スキャンでは、アタックサーフェスを攻撃者の観点から把握でき、攻撃者が最も狙いやすい領域を明確化しながら、エクスポージャーを検知、検証します。Surface Command は、スキャンに使用するセキュリティツールや IT ツールに関係なく、これらの外部スキャンと内部資産の詳細なインベントリを組み合わせます。このプロセスにより、死角、保護されていない資産や不正なアクセスに対するリスクなしで攻撃可能領域を完全に可視化できます。資産の構成状態を把握することで、誤設定、シャドー IT、コンプライアンスの問題をすばやく特定して対処できます。こうした統合的なアプローチにより、デジタル環境の全体像を把握し、プロアクティブなリスク緩和、脅威の防止、迅速な対応が可能になります。



デジタル資産の信頼できる唯一の情報源を確立・維持

社内のすべてのツールで資産インベントリと ID を統一し、関連付け。調査結果を通常の外部スキャンと相互参照して組織の真のアタックサーフェスを把握し、すべてのチームで信頼できる唯一の情報源を確立します。

適切なセキュリティ対策が欠如している資産を発見

エンドポイントセキュリティエージェントや脆弱性スキャンなどの対策がされていない資産や、どの ID に管理者権限があるか、MFA がないかなど、セキュリティカバレッジのギャップを継続的に特定します。

チーム内の責任範囲を明確化

資産の所有権を理解し、コンプライアンス基準が満たされていない場合に責任範囲を明確化します。セキュリティチームと GRC チームで修正プロジェクトが必要な場合に、どの利害関係者を関与させるべきかが明確になります。

インシデント対応者に完全なコンテキストを提供

セキュリティ分析担当者は、資産、脆弱性、セキュリティ管理のコンテキストを一元化して意思決定を行い、既知の資産情報と TTP に基づいて組織全体で脅威ハンティングを行えるようになり、進行中の脅威をより効果的に優先順位付けできます。

調査結果を通常の外部スキャンと相互参照して組織の真のアタックサーフェスを把握します。

シャドー IT と統制されていない IT リソースの利用を検知

ネットワークに接続している未知のユーザーと資産を特定し、相対的なリスクと必要な改善策を理解するために必要なコンテキストを把握します。

CMDB ツールを強化して資産ライフサイクル管理を支援

組織全体におけるテクノロジーの導入状況を追跡し、強力なネイティブクエリ機能を活用することで、どの資産が現在もアクティブであるか、最後に更新または修正されたのはいつかなど、深い洞察を得ることができます。

Rapid7 について

Rapid7 は、デジタルトランスフォーメーションの加速に直面する組織のセキュリティプログラム強化の支援を通じ、あらゆる人にとってより安全なデジタルの未来を創造しています。最高レベルの Rapid7 のソリューションポートフォリオは、セキュリティ担当者がリスクを管理し、アプリからクラウド、従来のインフラストラクチャ、ダークウェブに至るまで、脅威のランドスケープ全体にわたって脅威を排除するための支援を提供します。Rapid7 は、オープンソースコミュニティと最先端の研究を促進し、得られる洞察を製品の最適化に活用し、最新の攻撃方法に対応する力を世界のセキュリティコミュニティに届けます。世界中の 11,000 社以上のお客様組織に信頼され、業界をリードするソリューションとサービスで、企業が攻撃者の一歩先を行き、競争に先んじ、常に将来に備えるためのお手伝いをします。

RAPID7

製品

クラウドセキュリティ
XDRとSIEM
脅威インテリジェンス
脆弱性リスク管理
アプリケーションセキュリティ
オーケストレーションと自動化
MDR サービス

お問い合わせ

www.rapid7.com/ja/about/local-contact/