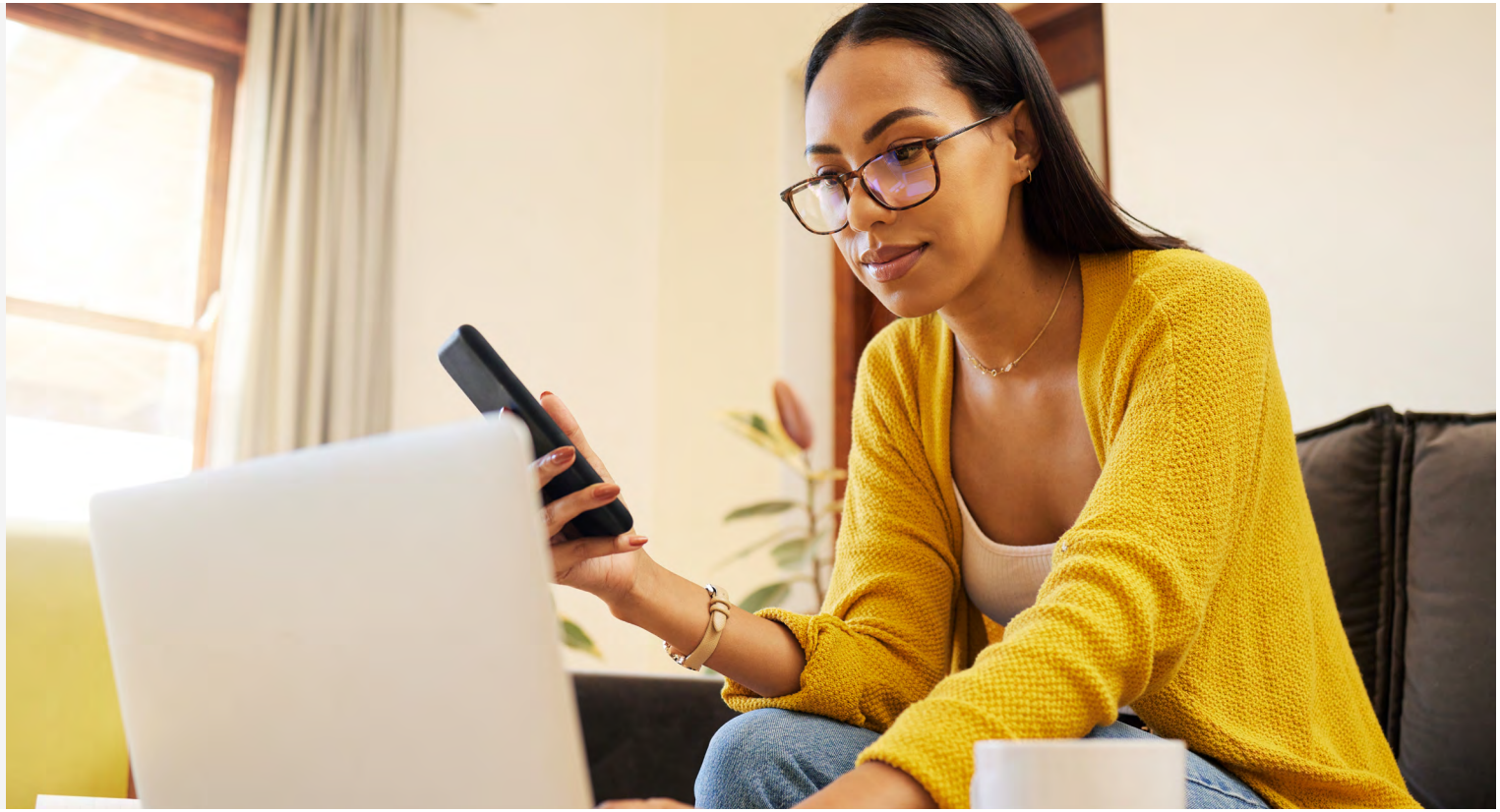
ivanti

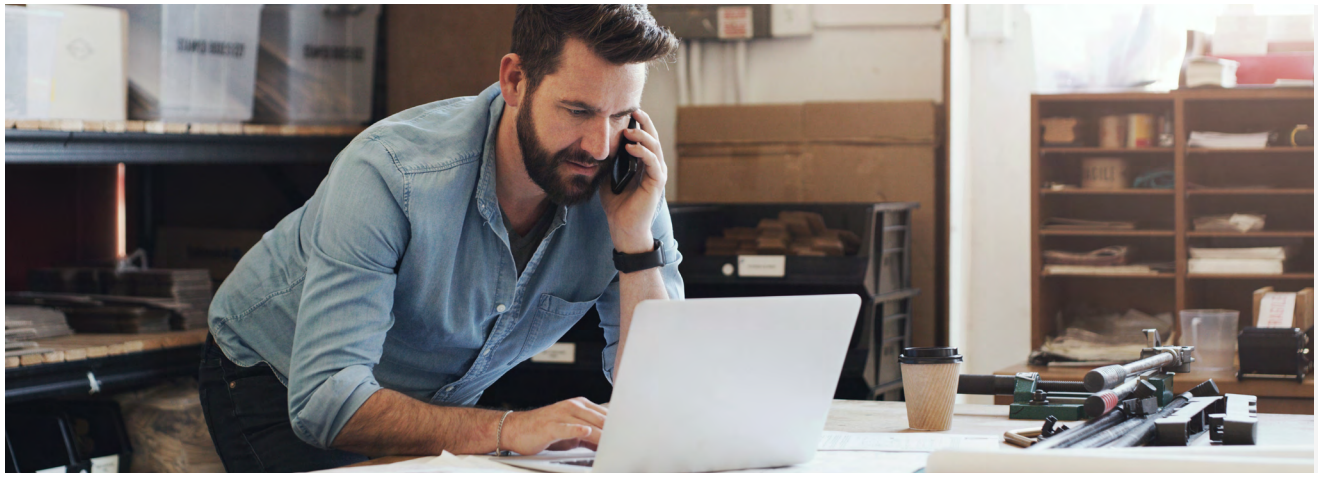
DATASHEET

Ivantiエクスポージャー管理

脆弱性管理の実施を拡大し、侵害を未然に防ぐ

従来の脆弱性管理は、今日見られるような大量かつ多様な資産やエクスポージャーを扱うようには設計されていませんでした。その結果、組織には多くのサイバー脅威に対する認識が不足しています。Ivantiのエクスポージャー管理ソリューションは、この問題を解決し、資産とエクスポージャーの完全な可視化に加え、リスクベースの優先順位付けを行うことで、改善への戦略的アプローチを導きます。





攻撃対象は常に拡大し、複雑化している状況です。伝統的な脆弱性管理のやり方はそれに対応して調整されることがほとんどないため、現代のIT環境を保護するには不十分となっています。

- 従来の境界（サーバーやエンドポイント）だけに目を向け、環境にリスクをもたらすモバイルデバイスやウェブサイト、アプリケーション、その他の資産に注視していません。
- 一般的な脆弱性とエクスポージャ（CVE）に厳密に焦点を当てる一方で、設定ミスなど、組織をリスクにさらす他のタイプのエクスポージャはチェックされていません。
- 共通脆弱性評価システム（CVSS）は、脆弱性の深刻度を測定しますが、リスクは測定しません。言い換えれば、脆弱性が悪用される可能性がどれだけあるかは測定するが、悪用されたかは測定しないということです。

その結果、従来の脆弱性管理方法を使用している組織は、最善の努力を尽くしても侵害のリスクが高まり、ダウンタイムや評判へのダメージ、その他の侵害がもたらす害を経験する可能性が高くなります。また、何千もの高深刻度の脆弱性を修正しようとする際に、実際のリスクをもたらすほんの一部の脆弱性に焦点を当てるのではなく、場当たり的な対応に陥りやすいです。

エクスポージャー管理は、脆弱性管理の欠点を解決します。これは、従来の方法を近代化する脆弱性管理の進化を表すものであり、資産とエクスポージャーの完全な可視化と適切な優先順位付けを確実にするものです。また、ガートナー社によると、2026年までに、継続的脅威エクスポージャー管理（CTEM）プログラムに基づいてセキュリティ投資を優先する組織は、侵害を3分の2削減できるとされています[1]。

CTEMとは？

ガートナー社が紹介した継続的脅威エクスポージャー管理（CTEM）は、企業が企業のデジタル資産と物理資産へのアクセス可能性、エクスポージャーおよび悪用の可能性を継続的かつ一貫して評価するための一連のプロセスと機能で構成されています。CTEMの実践は、Ivantiのエクスポージャー管理ソリューションのような、クラウド経由で提供される機能を使って実行されることが多くなっています。

Ivanti エクスポージャー管理について

包括的な攻撃表面の可視化とリスクベースの優先順位付けにより、Ivantiのエクスポージャー管理ソリューションは、従来の脆弱性管理では見過ごされがちなものも含め、組織がすべての資産とエクスポージャー、およびそれらがもたらす真のリスクを確実に認識できるようにします。

これにより、いわゆる「重大な」脆弱性を修正しようとする時代は終わりです。代わりに、組織のリスク許容度に応じてサイバーセキュリティリスクを戦略的に管理することができます。この最新のアプローチにより、事業継続性とブランドの評判を守るために、侵害に対して積極的に防御することが可能になります。

主な機能

完全に可視化する

既知のサーバーやエンドポイントを超える資産を含めるようにアパーチャーを広げることで、防御すべき攻撃面の全体像を把握できます。サイバー攻撃者が組織に侵入するには、たった一つの盲点があれば十分です。Ivantiのエクスポージャー管理は、ネットワークに接続する全てのデバイス、包括的に新規または未知のデバイスを検出し、アクティブ/パッシブスキャンとサードパーティコネクタを使用してインストールされたソフトウェアを把握します。

エージェントレスモニタリングにより、通常セキュリティチームの監視を逃れている外部に面した資産が明らかになります。これは、QAおよび開発環境や忘れられたマーケティングウェブサイトなどを含みます。Ivantiのソリューションは、CVEに留まらず、以下のベクトル内で外部に面した資産エクスポージャーを検出します。

- アプリケーションセキュリティ
- データ漏洩
- DNSヘルス
- Eメールセキュリティ
- ネットワークセキュリティ
- ソーシャルエンジニアリング

リスクを把握する

CVSSとそれがもたらす忙しさに別れを告げましょう。Ivantiは、エクスポージャーの修正努力を最も効果的な場所に集中させるための2つの独自のリスク評価方法を提供し、悪用やそれに続く影響を防ぐことができます。

脆弱性リスク評価（VRR）は、その内在的属性と現実世界の脅威のコンテキストに基づいてエクスポージャーを評価します。これは単に深刻度だけではなく、正確な評価を提供することで、どのエクスポージャーが即時の注意を要し、どれがリスクをもたらさないかを示します。

VRRは資産の重要度、脅威インテリジェンス、外部アクセスと組み合わされ、Ivanti RS3スコアを計算します。これらのスコアは、どの資産が最もリスクをもたらしているかを示します。また、リスクプロファイルの定量的な視点を提供し、時間を通じてエクスポージャー管理への取り組みの成果を示します。

解決するために行動する

分析に基づいて何もできないのであれば、エクスポージャーの評価に何の意味があるでしょうか？ Ivantiを使用すれば、悪用される前に重要なエクスポージャーを修正することで、リスクを軽減する具体的な手段を講じることができます。

API統合により、優先順位付けされたエクスポージャーのリストをエクスポージャー管理ソリューションからパッチ管理モジュールに直接配信し、修復を行うことができます。Windows、macOS、Linux、サードパーティ製アプリのサポートにより、ほとんどの最新環境で見られるエクスポージャーを高い割合で修正することができます。

Ivantiは、エンドポイントやエッジデバイス上の問題をプロアクティブに検出、診断、修復する自動化ボットを通じて、お客様に代わってアクションを実行することもできます。

Ivanti について

Ivantiは、ITとセキュリティ部門間の障壁を取り除きEverywhere Work（場所にとらわれない働き方）を実現します。IvantiのCIOとCISO向けに特化したプラットフォームは、ITとセキュリティ部門へ組織のニーズに合わせて拡張できる包括的なソフトウェアソリューションを提供し、セキュアに従業員体験を向上させます。Ivantiプラットフォームは、クラウドスケールのインテリジェントなハイパーオートメーションレイヤーであるIvanti Neuronsを搭載しており、組織全体でプロアクティブな修復とユーザーフレンドリーなセキュリティを実現し、ユーザーが満足するような従業員体験を実現します。Ivantiのエンドツーエンドのソリューションは、Fortune 100社のうち85社を含む40,000社以上の顧客によって採用されています。Ivantiは、すべての視点が聞き入られ、尊重され、評価される環境づくりに尽力し、顧客、パートナー、従業員そしてよりサステイナブルな未来を実現するために取り組んでいます。詳細については、www.ivanti.com/jaや@GoIvantiをフォローしてください。

ivanti neurons

詳細については、Ivanti までお問い合わせください。
www.ivanti.com/ja にアクセスしてください。

1. ガートナー社、「2024年のサイバーセキュリティのトップトレンド」、2024年1月2日