



脆弱性管理の 新たなアプローチ

脆弱性管理が依然として困難な理由

20 年以上にわたって改善改良が加えられてきた脆弱性管理 (VM) ですが、効果的な VM プログラムを提供しているベンダーはほとんどありません。ギャップは依然として組織をリスクにさらし、セキュリティと修復を担当する各部門間の摩擦は解消されないまま、既知の脆弱性を悪用した侵害は増加し続けています。最も高度とされるツールであっても、次のような重大な欠点を抱えています。



強化が限定的

CVE は引き続き焦点となっていますが、脅威インテリジェンスを活用するための強化は最小限にとどまっています。リスク軽減策やリスクレベルをより適切に判断するためのコンテキストを含めるような強化は実現には至っていません。



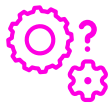
リスク計算が不明瞭

優先順位付けに悪用可能性などの追加のスコアリング要素を活用する限り、全体的なリスク計算は不明瞭なままです。



スケーラビリティが低い

大量のデータを処理できず、重要なスキャン結果へのアクセスに遅延が生じます。



カスタマイズ機能が不十分

多くのツールが、リスク計算のカスタマイズや修復ワークフローのような特有のビジネス要件を満たす機能を備えていません。

解決策に結びつけられない大量のデータ

一見シンプルなこれらの質問ですが、既存のツールを使用して答えようとするとは非常に難しい場合があります。

- 最も重要なアプリの脆弱性はどの程度か？
- エンドポイント エージェントは必要な場所にインストールされているか？
- 実際に所有している資産の数はいくつか？
- ツールが報告している脆弱性のうち、どれが重複しているか？
- すべての資産に所有者が割り当てられているか？
- 前回の取締役会以降、リスク態勢はどのように変化したか？

その他

また、テクノロジー スタックの進化に伴い、脆弱性の定義が拡大していることも問題をさらに複雑化させています。脆弱性は今や CVE だけの話にとどまるのではなく、設定ミス、コードの欠陥、業務プロセスのギャップなど、あらゆる所に存在します。しかし、脆弱性、資産、ユーザー、振る舞い、その他の業務システムなどを把握するために必要なデータは、数十の異なるツールに分散しているため、完全な可視性を得るには Excel を使って相関付けを行うしかないのが現状です。

統合型の脆弱性管理を実現する Zscaler UVM

Zscaler UVM は、新しい視点と革新的なソリューションで長年の課題を解決します。効果的なリスク管理には、包括的でデータ中心の戦略が不可欠という信念に基づき、Zscaler は CVE の管理方法だけでなく、セキュリティ データ全般の処理方法にも焦点を当てています。これは、これまでの統合型 VM ソリューションとは大きく異なる点です。

Zscaler のイノベーションは Data Fabric for Security にあり、セキュリティ データを使用してさまざまな課題に対処します。Data Fabric for Security は次のような幅広い機能を提供し、はるかに少ない時間と労力で VM プログラムを向上させます。

包括的なデータ統合

さまざまなソースからのデータを集約して関連付け、組織のセキュリティ状況を完全に可視化します。

コンテキスト化された豊富なインサイト

複数のセキュリティ ツールや業務システムにわたるセキュリティ データを強化してコンテキスト化し、組織の特定のリスク要因に基づいたセキュリティ ギャップに関する実用的なインサイトを提供します。

動的なリスク評価

業界のベスト プラクティスに従ったリスク軽減策とすぐに利用可能な多要素リスク スコアにより、そのリスク計算を確認してカスタマイズできます。また、自社の環境と固有のリスク要因に基づいた優先順位リストも入手できます。

自動化されたワークフロー

組織の構造やシステムに合わせて構築された自動でのチケットの割り当てと追跡により、被害につながる可能性が最も高いリスクに迅速に対応し、そのリスクが悪用される前に対処できます。

カスタマイズ可能なダッシュボードとレポート

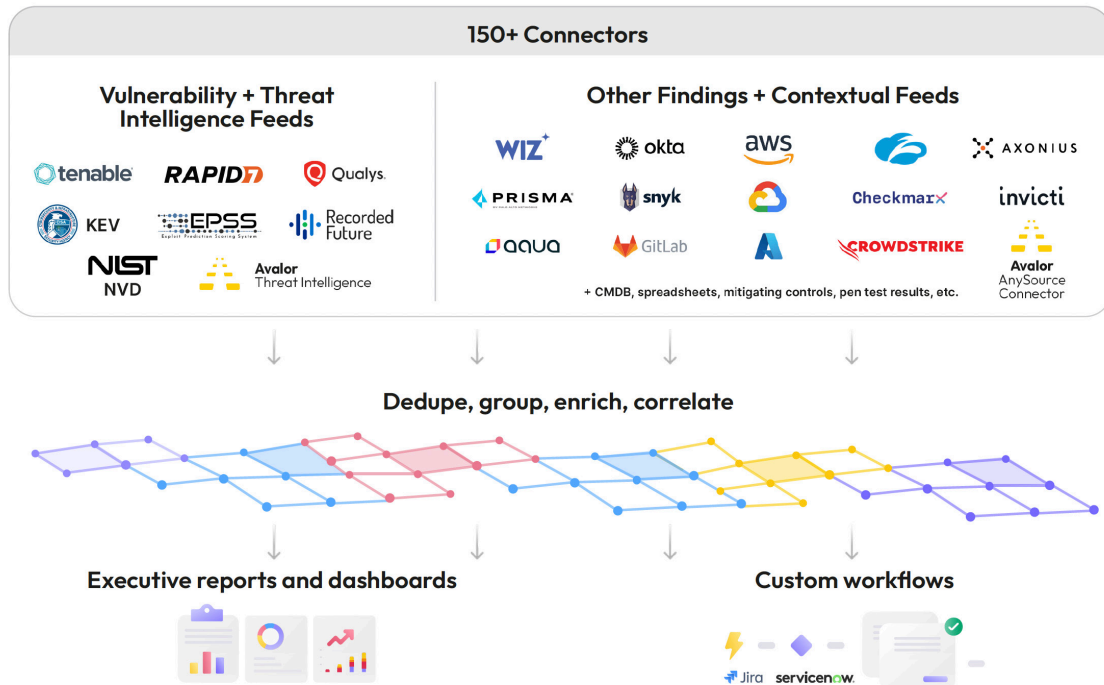
動的なダッシュボードとレポート作成機能を備えたプラットフォーム（単一の集約された動的データ セットから取得）により、組織の KPI や SLA、その他の重要な指標をカバーするビューやレポートを作成できます。また、セキュリティ態勢や各部門のパフォーマンスに関するリアルタイムのインサイトも提供されます。

Data Fabric for Security の活用

多くのセキュリティ上の課題と同様に、脆弱性管理はデータの問題であり、脆弱性やパッチ適用の問題ではありません。Zscaler のデータ専門家チームは、業界初の Data Fabric for Security を構築し、そのデータ ファブリック上にさまざまなアプリケーションを確保することで、最も困難なセキュリティの問題に対処します。

Data Fabric for Security は、形式や規模を問わず、数百のソースからデータを収集して関連付けます。Zscaler の Unified Vulnerability Management (UVM) モジュールはそのデータを使用して、リスク要因、軽減策、ビジネスコンテキストを集約するため、組織はリスクを包括的に把握できるようになります。

Data Fabric for Security



UVM が実現するメリット

UVM モジュールには幅広い機能が備わっていますが、導入は非常に簡単で、わずか数日で稼働できます。そして、数週間以内には次のような価値を実感できます。

- より効果的な「やること」リスト：UVM では、最初に対処すべきリスクが優先されるため、リスク エクスポージャーを効率的に削減できます。
- 合理的なオペレーション：データの関連付け、修復タスクの割り当て、優先順位の調整、チケットの管理がすべて自動化されるため、Excel での作業が不要になります。
- 迅速な修復：UVM は特定の組織のリスクを正確に把握し、適切な情報を適切な部門に届けるため、重要な作業が迅速に完了します。

このようなプロセスの改善と効率化によって、多くのお客様が次のような優れたメリットを実現しています。

1000:1

平均的な
チケット統合

80%

重大度が「重大」から
「中」に下がった問題

10 倍

コンテキストで向上
したトリアージ能力

6

回避されたカスタムの
統合作業の月数

3

価値実現
までの月数

スプレッドシートでのリスク管理を廃止

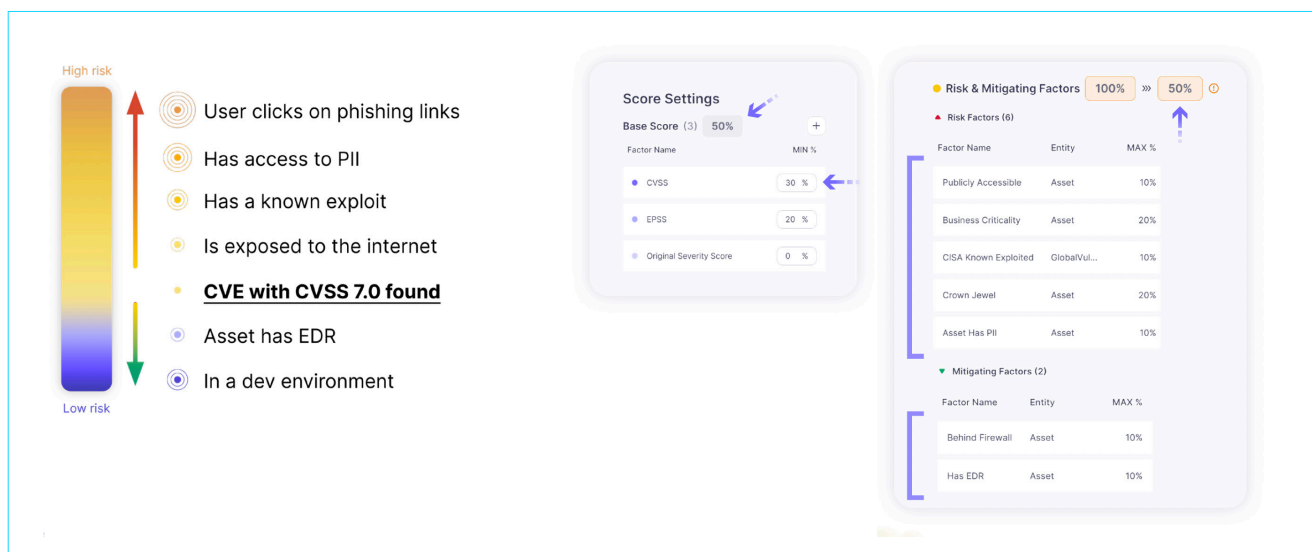
データをただ収集するのではなく、分析することこそが重要です。

UVM は、従来の VM ソリューションの制限を克服し、セキュリティの有効性を新たなレベルに引き上げられるようセキュリティリーダーをサポートします。また、データを関連付けて強化し、リスク態勢を迅速かつ効果的に改善するために必要なインサイトも提供します。

UVM はセキュリティ部門と、調査結果の修正に必要な IT や開発部門との間の摩擦を減らすのにも役立ちます。データをより最新の状態に保ち、リスク要因を組織固有の優先事項に基づいて設定し、部門構造に一致するワークフローを持つことで、本当に重要な問題に取り組めるようになります。

UVM プラットフォームはリスク要因と軽減策を考慮し、自動調整されたリスク スコアを提供するため、この実用性の具体的な例の一つといえます。

次の例では、修正がすぐに必要なもの (CVE A、リスク バーの高い方) とそうでないもの (CVE B、リスク バーの低い方) が、その理由と共に示されています。このように理由が詳細に示されることで、時には対立することがある部門間の理解が深まり、有益な会話を進められるようになります。



 | Experience your world, secured.™

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータセンターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、[zscaler.jp](https://www.zscaler.jp) をご覧いただくか、Twitter で [@zscaler](https://twitter.com/zscaler) をフォローしてください。

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™, [zscaler.com/jp/legal/trademarks](https://www.zscaler.com/jp/legal/trademarks) に記載されたその他の商標は、米国および/または各国の Zscaler, Inc. における (i) 登録商標またはサービスマーク、(ii) 商標またはサービスマークです。その他の商標はすべて、それぞれの所有者に帰属します。