ARMIS®

ホワイトペーパー

カオスからコントロールへ: サイバーセキュリティ資産管理を簡素化する

はじめに

組織がデジタル技術を採用し、依存し続ける中で、効果的なサイバーセキュリティ資産管理の必要性はますます重要になっています。しかし、デバイス、アプリケーション、クラウドベースのサービスの急増に伴い、サイバーセキュリティ資産の管理はかつてないほど複雑になっています。複雑化、分断化、制御不能の問題は、セキュリティチームにとって大きな課題となっています。

企業はサイバーセキュリティ・ソリューションに多額の投資を行う一方で、自社資産のセキュリティを見落としていることが多く、企業セキュリティの盲点となっています。攻撃者はこの盲点を利用して、組織のシステムやデータに不正にアクセスし、データ漏洩、財務上の損失、風評被害などの深刻な結果を招く可能性があります。

このような課題に対処するために、組織は効果的なサイバーセキュリティ資産管理のための包括的なフレームワークを必要としています。本ホワイトペーパーでは、サイバーセキュリティ資産管理における3つの主な課題（複雑性、断片化、管理の喪失）を探り、組織がこれらの課題を克服するのに役立つ効果的なサイバーセキュリティ管理のフレームワークを紹介します。

以下のセクションでは、これらの課題をそれぞれ詳しく検討し、それらがサイバーセキュリティ資産管理にどのような影響を与えるかについて議論します。また、企業セキュリティの盲点とそれが組織に与える影響についても検討します。最後に、組織がサイバーセキュリティ資産管理に対するプロアクティブで包括的なアプローチを行うための、効果的なサイバーセキュリティ管理のフレームワークを紹介します。

目次

06 **複雑からシンプルさへ**
07 断片化とコントロールの喪失
08 デバイスの増加、複雑化
09 **企業セキュリティの盲点に光を当てる**
09 ネットワーク資産のマッピング
09 全体像を見る
10 セキュリティギャップを埋める
11 断片化を解消し実用的な情報を得る
12 **サイバーセキュリティ資産管理をシンプルに：実践的なフレームワーク**
12 包括的で完全な資産ディスカバリー
13 実行可能なインテリジェンス：資産の特定からギャップ分析まで
14 動的なセキュリティポリシーによる素早い脅威対応
15 エージェントレス・アプローチによる迅速なセキュリティ管理
16 **結論**

複雑からシンプルさへ

サイバーセキュリティ資産管理では、組織全体におけるデジタル資産の急増が、セキュリティチームにとって大きな課題となっています。デバイス、アプリケーション、クラウドベースのサービスの数が増え続ける中、リスク態勢と脅威の状況を適切に管理するために、これらの資産をよりよく可視化する必要性がますます高まっています。

残念なことに、レガシー・ツールの「断片化」によって、これらの資産の管理はより困難になっています。資産の管理は多くの場合、複数のITおよびセキュリティ・ソリューションにまたがっており、その結果、完全な可視性も、信頼できる統合された情報源もない断片的な状況になっています。これは、ITチームとセキュリティチームが、どのような資産を本当に保有しているのかを理解し、ポリシーが適切に実施され、リスクが管理され、資産が保護されていることを確認するのに苦慮していることを意味します。

適切なサイバーセキュリティ資産管理が行われないと、組織はさまざまなサイバー脅威から資産を保護する際に大きな課題に直面する可能性があります。攻撃者は、資産に対する可視性と制御の欠如を悪用してシステムやデータに不正アクセスし、データ侵害、財務上の損失、風評被害などの深刻な結果を招く可能性があります。

このような課題に対処するためには、サイバーセキュリティ資産管理に対する包括的なアプローチが必要です。このアプローチには、組織にとっての重要性に基づいて資産を特定、分類、優先順位付けすることが含まれます。このアプローチはまた、資産情報の信頼できる統合された情報源を提供し、ITチームとセキュリティチームが資産の全体像を把握し、リスク管理と資産保護について十分な情報に基づいた意思決定を行えるようにする必要があります。

サイバーセキュリティ資産管理にプロアクティブかつ包括的なアプローチを採用することで、組織は資産を効果的に管理し、アタックサーフェス領域を縮小し、サイバー脅威のリスクを軽減することができます。絶えず進化するサイバーセキュリティの状況において、組織が資産を適切に保護するためには、サイバーセキュリティ資産管理を優先することが不可欠です。

あなたの環境にあるすべての資産を把握していますか？

- 資産の数、CMDBの精度は？
- 管理されている資産と管理されていない資産の数は？
- 事業所や部署ごとの資産の配分は？
- エンドポイントセキュリティが導入されていないラップトップはあるか？
- もしそうなら それらはどこにあり、誰が利用しているのか？
- アセットタイプ別にユーザー数はどれくらいいるのか、そして彼らの場所はどこなのか？
- 環境内に未許可のアプリケーションがいくつあるのか？
- 紛失されたデバイスがネットワーク内にないか？
- CVEの重大性、事業部門、所在地ごとに、いくつの脆弱な資産あるか？
- パッチが適用されていないオペレーティングシステムまたはアプリケーションが稼働しているデバイスが何台あるか？

断片化とコントロールの喪失

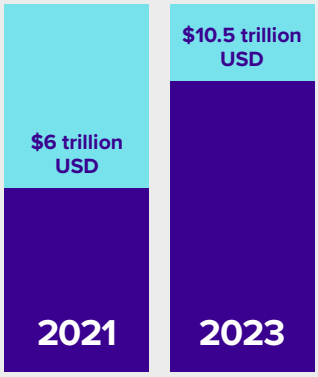
最近の研究では、ネットワークデバイスの数が以前の予測を上回っていることが示されています。Statistaのレポートによると、世界のモノのインターネット（IoT）デバイスの数は、2019年の266億6,000万台から、2025年には754億4,000万台に達すると予想されています。さらに、パンデミックの年は、組織が事業継続の取り組みをサポートするためにデジタルトランスフォーメーションのペースを急速に上げなければならなかったため、ネットワークデバイスの採用を加速させました。

今日、ほとんどすべての組織が、ビジネスのあらゆる側面を遂行するために、接続された資産やデバイスに大きく依存しています。これは、ラップトップ、デスクトップ、サーバーなどの管理対象デバイス、スマートフォン、BYOD（Bring Your Own Device）、仮想資産、クラウドサービス、IoTデバイス（「管理外デバイスの最たるもの」）などを通じて行われています。その結果、何十億ものデバイスが重要なデータやインフラに接続され、毎日さらに多くのデバイスがオンライン化されています。

しかし、デバイスの数が増え、可視性と制御性が欠如しているため、ITチームやセキュリティチームが資産を効果的に管理し、保護することは困難になっています。また、COVID-19の流行は、リモートワークや分散運用モデルをサポートするために、より多くの、そして様々なタイプの資産が使用されるようになったため、複雑性の問題を増加させる一因となりました。マッキンゼーの調査によると、COVID-19はネットワークデバイスの採用を加速させるのに実際に役立ったといいます。一般的にイノベーションを制限する標準的な組織の障壁が取り除かれ、生産性向上の取り組みが促進されたからです。

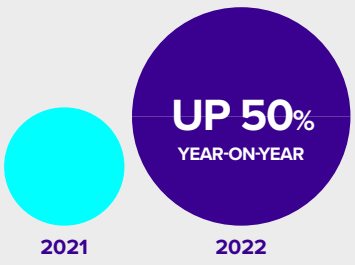
資産を効果的に管理し保護するために、組織は異種のツール間で可視化と制御を行う必要があります。これは、組織にとっての重要性に基づいて資産を特定、分類、優先順位付けし、資産情報の真実の情報源を一元化することを意味します。サイバーセキュリティ資産管理にプロアクティブかつ包括的なアプローチを採用することで、組織は資産を効果的に管理し、アタックサーフェス領域を縮小し、サイバー脅威のリスクを軽減することができます。

Global Cost of Cybercrime



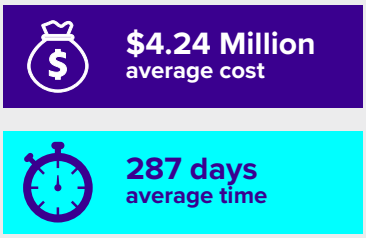
年までに、サイバー犯罪の世界的コストは、2021年の6兆米ドルから10.5兆米ドルに達すると予測されている。

Average Cost of a Cyber Attack



年、企業へのサイバー攻撃1件の平均コストは270万米ドルで、前年から50%増加した。

Average Time to Identify and Contain a Data Breach



データ漏えいを特定し、封じ込めるまでの平均時間は287日で、1件あたりの平均コストは424万米ドルである。

SOURCE: ARMIS CYBERWARFARE REPORT, JANUARY 2023

デバイスの増加、複雑化

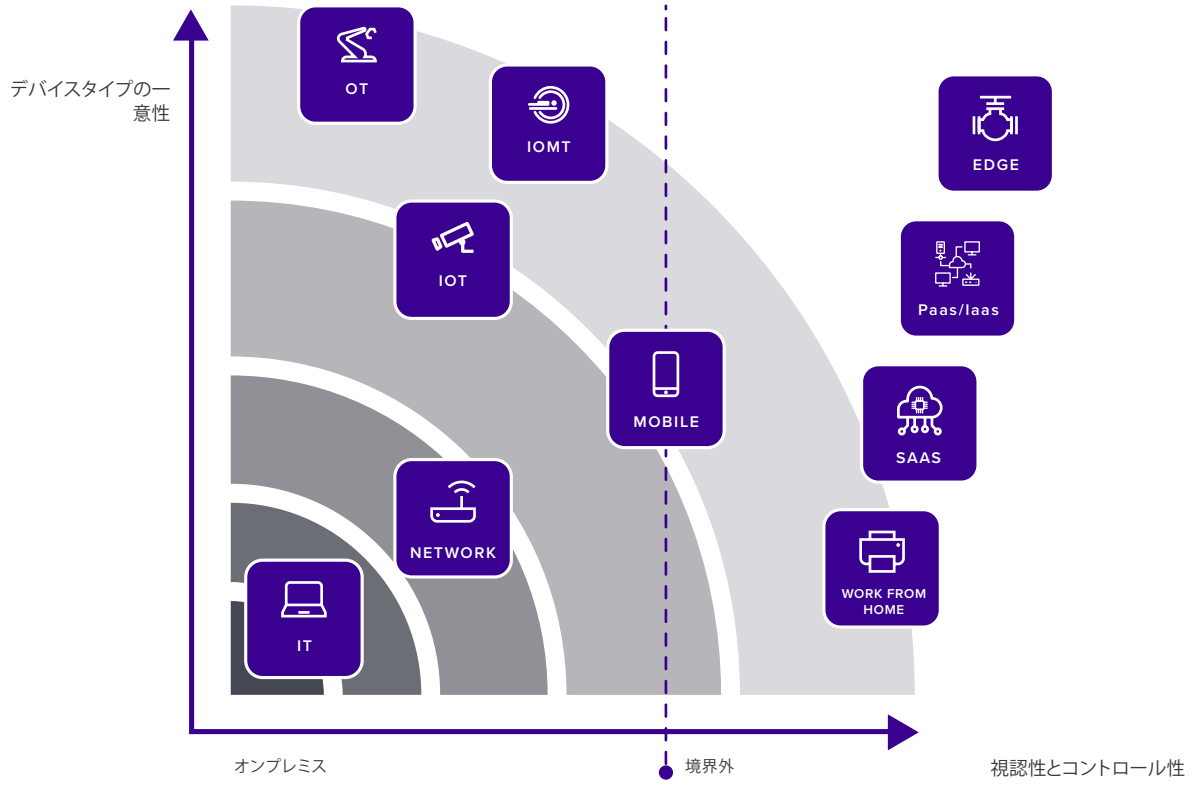
組織で使用されるデバイスやツールの数が増え続ける中、資産の管理とセキュリティ確保はかつてないほど複雑になっています。このような資産とデバイスの急増は、ITチームとセキュリティ・チームがナビゲートしなければならない非常に複雑な状況を生み出すため、サイバーセキュリティ資産管理には不可欠です。

ネットワークに接続する各デバイスには、ITチームが考慮しなければならない新たな考慮事項が発生します。これには、オペレーティングシステム、アプリケーション、ユーザー・アクセス、ネットワーク接続、パッチ、アップデートなどが含まれます。 これらは基本的なことに過ぎず、新しいデバイスがネットワークに追加されればされるほど、複雑さは増すばかりです。

その結果、非常に複雑でダイナミックな環境に死角が生まれ、ITチームやセキュリティチームが資産を包括的に把握することが難しくなっています。この複雑さが、組織が重要なデータを効果的に管理し、保護することを妨げています。

さらに悪いことに、絶えず進化する脅威の状況は、サイバーセキュリティ資産管理に新たな複雑さを加えています。サイバー犯罪者は、デバイスやシステムの脆弱性を悪用する新しい方法を常に見つけているため、ITチームとセキュリティチームが資産を完全に可視化することがさらに重要になっています。

この複雑さを克服するために、組織にはサイバーセキュリティ資産管理へのプロアクティブなアプローチが必要です。これには、IT チームが組織にとっての重要性に基づいて資産を特定、分類、優先順位付けできるフレームワークを導入することが必要です。資産情報の真実の情報源を一元管理することで、IT チームは資産を効果的に管理し、アタックサーフェス領域を縮小してサイバー脅威のリスクを軽減することができます。さらに、資産管理タスクを自動化し、人工知能（AI）と機械学習（ML）を活用することで、ITチームは複雑化する環境を管理することができます。



企業セキュリティの盲点に光を当てる

ネットワーク資産のマッピング

組織がネットワーク上で平均的に確認できるデバイスの割合は、組織の規模、デバイスの種類、ネットワーク可視化ツールやセキュリティ対策のレベルなどの要因によって異なります。

新しいデバイスや技術の急速な成長と普及は、セキュリティ対策が追いつく能力を上回り、その結果、企業のセキュリティに脆弱性を生み出す盲点が急増しました。 企業が簡単な接続や仮想マシンの即時デプロイといった利便性を受け入れるにつれ、これらのデバイスや資産は、保護されていない接続を悪用しようとする攻撃者の標的となります。

リスクが増大しているにもかかわらず、多くの組織はセキュリティ体制のこうしたギャップを検出できず、サイバー犯罪者に攻撃を成功させる機会を与えています。このような死角の出現により、企業ネットワーク上のすべてのデバイスと資産に対する可視性と制御の強化、およびより洗練された脅威の検出と対応機能が急務となっています。

適切な保護がなければ、サイバー攻撃者はこれらの盲点を突いて機密データにアクセスし、企業システムを侵害することができます。これらの盲点に対処し、進化する脅威の状況を先取りするためには、包括的なセキュリティ対策を実施することが不可欠です。ネットワークを保護するための積極的な対策を講じることで、企業はサイバー攻撃のリスクを低減し、重要な資産と情報を保護することができます。

全体像を見る

資産をリアルタイムで包括的に把握できないことは、多くのITチームやセキュリティチームが直面する共通の問題です。 スプレッドシートや手作業による集計など、さまざまな方法を駆使しているものの、組織が保有する資産の数や種類を正確に把握するのに苦慮することが多くあります。この問題は、単一目的で断片化されたそれぞれのツールの管理範囲が限られており、すべての資産の完全で統一されたリアルタイムのリストを提供できないために、さらに深刻になっています。その結果、ITリーダーやセキュリティ・リーダーがWindowsホストの数などの具体的な詳細について問い合わせても、異なるチームやツールから相反する回答が返ってくる可能性があります。

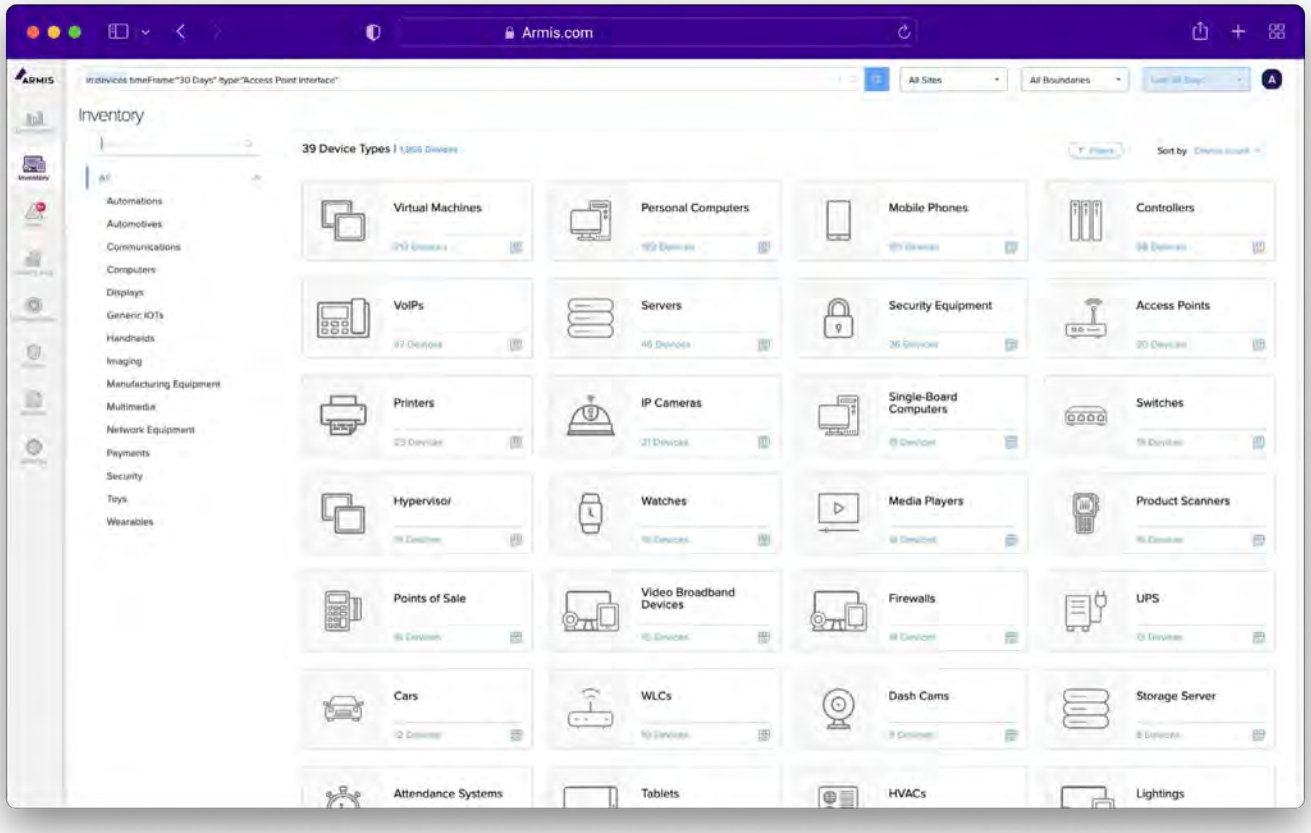
サイバーセキュリティ資産を効果的に管理するために、組織は可視性の問題に取り組むことから始めなければなりません。セキュリティチームが資産を適切に管理するには、数、種類、アプリケーションを含むすべての資産を把握していなければなりません。ビジネス・チームはスピードとイノベーションを優先しますが、こうした要素はセキュリティ組織にとってリスクを生む可能性があります。テクノロジーは常に進化しているため、常に多くの資産と新しいバージョンが存在し、バリエーションと断片化が生じます。そのため、ITチームとセキュリティチームは、すべてのデバイスと資産に関するコンプライアンスとセキュリティの全体像を完全に可視化できる一元管理された情報を必要としています。

Armisプラットフォームは、企業のITおよびセキュリティチームに、管理対象および非管理対象のすべての資産に対する必要な可視性を提供し、永続的でますます攻撃的になる脅威をもたらす資産セキュリティの盲点をなくします。企業ネットワーク外のデバイスを含むすべてのデバイスを識別し、その姿勢に関する継続的な情報を提供することで、Armisプラットフォームのユーザーは、脅威を隔離し、セキュリティ上の問題を迅速かつ効果的に修正することができます。

資産のライブマップ としてのArmis

ギャップを埋める

ITとセキュリティ・スタックの既存のセキュリティツールは、脅威の状況を断片的かつ不完全にしか把握できず、組織はサイバー攻撃に対して脆弱なままになっています。これらのツールは、個々のサービスやデバイスを保護するために使用されますが、脅威が存在する場所を包括的に把握することはできません。各資産と対応するサービスのセキュリティおよびコンプライアンス・ポリシーと設定を管理するには、刻々と変化する内外の脅威の状況に目を配りながら、それらの資産上で稼働しているオペレーティングシステムとアプリケーションを特定する必要があります。



しかし、このアプローチでは、資産の数とそのセキュリティ態勢について孤立した見解が生まれ、その結果、可視性と実施にギャップが生じます。このような盲点は、セキュリティ・インフラストラクチャの弱点を狙うサイバー攻撃者にとって格好の標的となります。この問題に対処するために、IT チームとセキュリティ・チームは、すべてのシステムからすべての資産と関連情報を網羅する、デバイス・セキュリティの適用範囲に関する信頼できる一元管理された情報源を必要としています。

皮肉なことに、独自の目的のために「より多くの」セキュリティツールを導入すると、セキュリティ対策がかえって複雑になり、その結果、死角が生じて組織がリスクにさらされる可能性があります。すべての資産の状態、構成、およびポリシーの実施に関する統一されたビューがなければ、ITチームとセキュリティチームは、組織の完全なセキュリティ態勢を理解することができず、潜在的に大きなリスクを生み出すことになります。そのため、すべての資産に対して完全な可視性と保護を提供し、絶えず進化する脅威の状況を先取りできるようにする、デバイス・セキュリティへの包括的なアプローチが急務となっています。

断片化を打破して実用的な情報を得る

今日の複雑なセキュリティ環境で有意義かつ効果的な情報を得るためには、組織が従来リスクを区分し、一般的なアプローチによってセキュリティを妨げてきた断片化を取り払う必要があります。

従来のセキュリティツールは、特定のリスクを軽減するのに有効であった一方で、可視化と制御を妨げる断片化を生み出し、その結果、実用的な情報が得られなくなっていました。現代のセキュリティ環境では、デバイスや資産が運用される環境の絶え間ない変化に対応できる、よりダイナミックで資産に特化したアプローチが求められています。資産に特化したアプローチがなければ、適切なポリシー制御や実施なしに、デバイスや資産が簡単にオンライ

ン化され、セキュリティとガバナンスの問題が急激に増加することになります。この課題を克服するために、組織は、断片化を解消し、より優れた可視性と制御を可能にする、よりプロアクティブで全体的なセキュリティ・アプローチを採用しなければならなりません。このアプローチは、各デバイスと資産のユニークな特性に適応するように設計された資産固有のポリシーを中心としたものでなければならず、セキュリティとガバナンスが今日のペースの速いデジタル環境において最優先事項であるものでなければなりません。

サイバーセキュリティ資産管理をシンプルに：実践的なフレームワーク

今日の相互接続されたデジタル世界では、効果的なサイバーセキュリティ資産管理は、サイバー脅威から組織を保護するために不可欠です。その重要な側面は、資産の完全かつ統一されたビューを持つことであり、これにより組織は、その環境の真のリスク状況を理解し、管理することができます。

ネットワーク・アクセス・コントロール（NAC）製品は資産管理の出発点と見なされることが多いですが、それだけでは十分ではありません。多くのデバイスは、セキュリティ責任者が検出できないままになっています。この課題に対処するには、ネットワーク境界、クラウド環境、特定のデバイスやアプリケーションなど、複数の場所で問題を特定できるITおよびセキュリティ管理ツールを活用する必要があります。

さらに、企業は、ある時点での評価にとどまらず、継続的な監視を採用する必要があります。このアプローチは、環境のセキュリティ状態をより包括的に把握し、脅威をリアルタイムで検出して対応することを可能にします。

残念ながら、既存のツールの多くは特定の問題に対処するように設計されているため、可視性のギャップや誤った精度を生み出す狭いビューを持つ孤立したコンソールになります。このような限界を克服するために、組織は、さまざまなセキュリティおよびIT管理ツールを一元化されたプラットフォームに統合する全体的なアプローチを採用すべきです。 このプラットフォームは、資産とそれに関連するリスクに関する統一されたビューを提供し、チームが十分な情報に基づいた意思決定を行い、脅威を軽減するためのプロアクティブな措置を講じることを可能にする必要があります。

効果的なサイバーセキュリティ資産管理には、資産とそれに関連するリスクを一元的に把握できる包括的、継続的、かつ全体的なアプローチが必要です。このようなアプローチを採用することで、組織はサイバー脅威からよりよく身を守り、デジタルインフラの回復力を確保することができます。

包括的かつ完全な資産ディスカバリー

進化し続ける今日のテクノロジー状況において、従来の境界という概念はもはや時代遅れとなっています。 資産やデバイスは、もはや単一の場所に限定されるものではなく、ワイヤレスでもネットワーク接続でも動作します。したがって、包括的で完全な資産発見ソリューションは、場所、ネットワークに接続されているかどうか、オンプレミスか仮想かにかかわらず、あらゆるタイプの資産を識別できなければなりません。

組織のセキュリティ状況を完全に把握するためには、資産管理ツールは、オンプレミス、クラウドを問わず、すべてのデバイス、アプリケーション、オペレーティングシステム、その他のシステムやサービスを包括している必要があります。そのためには、既存のインフラ、API、ネットワーク接続、その他のプロトコルを活用して、すべてのデータソースに接続できることが必要です。

包括的で完全な資産ディスカバリーを実現するためには、場所や接続状態に関係なくあらゆる種類の資産を識別でき、既存のインフラ、API、ネットワーク接続、その他のプロトコルを介してあらゆるデータソースに接続できる資産管理ソリューションが不可欠です。

効果的なサイバーセキュリティ資産管理に対するArmisのアプローチは、環境に存在するすべての資産とデバイスの一元化された最新のインベントリを確立することから始まります。このインベントリには、すべての仮想インスタンス、クラウドサービス、現在環境に接続されている急速に拡大する管理対象外の資産やIoTデバイスが含まれます。

Armisプラットフォームは、新しいデバイスやアセットがネットワークに接続されると常に検出·識別し、アセット全体を包括的かつ継続的にカバーします。すべての資産に関する完全かつ正確なビューを提供することで、Armisプラットフォームは、各デバイスに関連する潜在的なリスクを把握し、セキュリティ対策に優先順位を付け、ネットワーク全体の脅威をプロアクティブに管理することを可能にします

実用的なインテリジェンス資産の特定からギャップ分析まで

環境内のすべての資産を包括的に理解することで、ITチームとセキュリティチームは、デバイスにインストールされているアプリケーションなど、リスクをプロアクティブに管理するための資産の詳細の特定と評価を開始することができます。 コンプライアンス·ギャップや潜在的なリスクを特定するためには、ポリシーが実施されているかどうかを知ることだけでなく、ユーザー、設定、態勢など、各資産に関連する完全なコンテキストを理解することも同様に重要です。このレベルの情報を得るには、各資産のコンテキスト·データを取り込み、分析する必要があります。

多くのセキュリティツールは、この種の分析のための基本的な機能を備えていますが、多くの場合、デバイスや資産の広範なコンテキストを考慮することなく、境界アクセスやクラウド·ストレージなど、セキュリティの単一の領域に焦点を当てています。 その結果、これらのツールは、特定のデバイスや資産に固有の問題を総合的に特定できないことが多いのです。

リスクを特定する能力を備えていること。また、データを集約して分析し、特定のデバイスや資産に固有の問題を特定することで、ITチームとセキュリティチームに、組織のセキュリティ状況を完全かつ文脈的に理解させることができなければなりません。

Armisプラットフォームは、すべてのデバイス、アプリ、オペレーティングシステムを識別し、CVEを評価し、各資産にリスクスコアを割り当てることで、サイバーセキュリティリスク低減します。Armisプラットフォームは、30億台以上のデバイスを追跡する世界最大のデバイスナレッジベースであるArmis Collective Asset Intelligence Engineを活用しています。Armisプラットフォームのユニークなコンポーネントであるarmis Collective Asset Intelligence Engineは、デバイスの動作を継続的に分析し、潜在的なセキュリティ脅威を特定することで、資産の動作の包括的なビューを提供し、潜在的なセキュリティ侵害を示す可能性のある異常や不審な動作を特定します。

動的なセキュリティポリシーによる素早い脅威対応

自動化されたセキュリティ対策は、セキュリティ・ギャップに対処するプロセスを合理化し、対応時間を短縮し、人的ミスのリスクを最小限に抑えることができます。これらの対策には、影響を受けるデバイスの自動隔離、ポリシーベースのソフトウェア更新、リアルタイムの脆弱性スキャンなどがあります。自動化によってこれらのアクションを編成することで、組織は迅速かつ効果的にセキュリティ・リスクを軽減し、IT環境の安全性を確保することができます。

このレベルの自動化とリアルタイムの対応を実現するには、既存のセキュリティ・ソリューションと統合し、オンプレミスとクラウドの両方で組織全体のすべてのデバイスを管理できる包括的な資産管理ツールが必要です。自動化とリアルタイムのセキュリティ対策を活用することで、企業はよりプロアクティブで効果的なセキュリティ管理のアプローチを実現することができます。

脆弱性、リスク、セキュリティ・ギャップを迅速に特定し、解決することは、安全なIT環境を維持するために不可欠である。しかし、これらの問題に手作業で一貫して対処することは、シンプルなITセットアップを持つ小規模な組織にとってさえも困難なことです。この課題を克服するために、組織には、デバイスの隔離、ソフトウェア・アップデートの開始、アラートのトリガー、デバイスが触れる可能性のあるすべての資産にわたる脆弱性のスキャンなど、必要なアクションを編成できるリアルタイムのポリシー実施と自動化されたセキュリ

重要なセキュリティギャップ分析

- エンドポイントエージェントの導入ギャップの特定
- エージェントのバージョン遅れに対処する
- モジュールが適切に設置されていることを確認する（例. Protectionのアンインストール、リモート・レスポンス）
- 直接ツールを使用せずに、ギャップの評価とレポートを簡素化

コンプライアンス環境の確保と確認

- 未スキャンの資産とネットワークセグメントを特定する
- 資産のレポート 過去7日以内に未スキャンのデバイス（または他 の間隔で）
- スキャンデータを他のセキュリティツールからの情報と関連付ける
- スキャンされたデバイスのコンテキストを得る（例：コンピューターとIoTの区別をつける）

エージェントレスアプローチによる迅速なキュリティ管理

多くのセキュリティ·ツールは、活動傾向を収集·分析するためにエージェントをIT環境に導入することに依存しています。しかし、ITとセキュリティの専門家は、すでに混雑している資産リストに新たなエージェントを追加することをためらっています。エージェントレス·アプローチは、一過性の資産も含め、リアルタイムで包括的なデバイス·インベントリを構築するための受動的だが効果的なソリューションを提供します。

デバイスと資産の使用状況にコンテキストを提供するには、設定、アクティビティ、その他の異常の分析が必要です。それは、以下に焦点を当てるべきです：

完全な可視性：Armisを使用することで、強力なディスカバリと統合された資産インベントリを実現し、組織のデバイスとネットワークに対する包括的な可視性を提供します。この堅牢なソリューションは、3倍以上の資産を検出し、インフラストラクチャ全体を効果的に管理および保護します。

コンテクスチュアル·インテリジェンス：多角的なビューと包括的な分析により、コンテキスト·インテリジェンスを強化します。Armisの高度なアプローチにより、SOCの調査時間を50%短縮し、セキュリティ·インシデントに対処する効率と効果を向上させます。

リスクと脅威の把握: Armisの支援により、セキュリティ管理における脆弱性管理と優先順位付けのギャップを特定します。エージェントのカバー率を15%向上させることで、企業はリスクと脅威をよりよく理解して対処できるようになり、全体的なセキュリティ態勢が強化されます。

世界中のお客様がアルミスを選ぶ理由

完全な可視性
パワフルな検知能力
統一されたインベントリ

3倍以上の資産を発見

コンテクスチュアル·インテリジェンス
多次元ビュー
包括的な分析とインテリジェンス

SOCで50%以上の調査時間を削減

リスクと脅威を理解する
脆弱性の管理と優先順位付け
セキュリティ管理のギャップを特定

エージェントの導入を15%改善

価値実現までの時間の短縮
最新のクラウドアーキテクチャ
業界のリーダー、信頼できるパートナー

レスポンスまでの時間を10%改善

Armisは、資産管理への完全なエージェントレスアプローチを提供することで、他のセキュリティツールとは一線を画しています。この独自のアプローチにより、デバイスの運用を中断することなく、単一のオフィスから広大なグローバルネットワークまで、さまざまな環境への導入を簡素化し、迅速化します。

リアルタイムの監視により、継続的な資産の発見と自動化された実施が可能になり、すべてのデバイスが適切にインベントリ化されていることを確認できます。Armisプラットフォームは、デバイスデータを分析し、デバイス情報、製造元、評判、既知の脆弱性などの複数の要因に基づいてリスクスコアを計算します。さらに、アクティビティと動作を評価し、デバイスの既知の良好なプロファイルと比較して、問題や脅威を特定します。

Armisプラットフォームのエージェントレスかつパッシブな性質は、企業がデバイスの運用を中断することなく、迅速かつ容易に資産の完全な可視性を得ることができることを意味します。これは、接続されたデバイスとリモートワークの数が増加し続け、分散した従業員全体のセキュリティリスクを管理することがより困難になっているため、特に重要です。

結論

技術革新とITの変化が重要な効率性をもたらし続ける一方で、組織資産の保護に複雑さをもたらしています。資産の数が増え続ける中、組織の重要なデータに触れているものを可視化することはますます難しくなっています。

このような可視性の課題を克服するために、ITチームとセキュリティチームは、サイロ化された断片化を克服しながら資産とデバイスを特定できるソリューションを提供するArmisプラットフォームに頼ることができます。Armisプラットフォームは、資産の発見から始まり、ITおよびセキュリティチームが重要なセキュリティギャップを特定し、セキュリティポリシーの自動実施を適用してリスクに即座に対処できるようにします。

Armisプラットフォームにより、最新の組織はITの変化と革新に対応するための十分な設備を備えています。Armisプラットフォームは、ネットワーク上のすべての資産とデバイスを可視化し、サイバーセキュリティ資産管理の基本フレームワークを構築します。

Armisについて

アセット・インテリジェンス・サイバーセキュリティ企業であるArmisは、攻撃面全体を保護し、組織のサイバーリスクをリアルタイムで管理します。急速に進化するボーダーレスな世界において、Armisは組織がすべての重要な資産を継続的に把握し、保護し、管理することを確実にします。Armisは、フォーチュン100、200、500の企業や、国、州、地方公共団体において導入されており、重要インフラ、経済、社会を24時間365日安全に保護することに尽力しています。Armisはカリフォルニア州に本社を置く非公開企業です。

armis.com

japan@armis.com

20231117-1