ivanti

セキュリティのシフトレフト

現在の IT ツールでレスポンシブなセキュリティ環境を構築する方法

目次:

01 セキュリティの岐路:
プロアクティブな修正とテクノロジーの統合

02 DevSecOpsの先にある「シフトレフト」の定義:
共通の定義がセキュリティと IT アプローチの架け橋となる

03 IT ツール + セキュリティ
ITSM / ITAM と UEM をセキュリティのユースケースで再利用する方法

04 すべての道は DEX に通じる:
テクノロジーを共有することで、従業員のデジタル体験がどのように向上するか

この文書は厳密に指針としてのみ提供されています。いかなる保証をも提供するものではありません。この文書には、Ivanti Inc.およびその関連会社（総称して「Ivanti」）の機密情報および専有財産が含まれており、Ivanti が事前に書面で同意していないかぎり、開示または複製が禁止されています。

Ivantiはこの文書または関連する製品の仕様ならびに説明について、いつでも予告なく変更を行う権利を有します。Ivantiは、この文書の使用に関する一切の保証を行ないません。また、この文書に瑕疵があったとしても一切の責任を負わず、この文書の情報を更新することも約束しないものとします。最新の製品情報については、ivanti.com/ja/をご覧ください。

ivanti

01

セキュリティの岐路

予防的なサイバーセキュリティのニーズと技術統合への圧力とのバランス

このセクションの内容:

1. レスポンシブなサイバーセキュリティエコシステムを構築…
2. …あるいは技術スタックを統合するか
3. セキュリティはいかにして両方を同時に実現できるのでしょうか。

ivanti

相反するセキュリティ義務の岐路に立つ

サイバーセキュリティチームは、現在のセキュリティの緊急事態を継続的に改善しながら、将来のサイバー攻撃リスクに対処するために先手を打つ必要があります。十分な資金があり、協力的な組織であっても難しい任務です。と同時に、技術スタックの作業量を削減し、各部門の予算が逼迫している状況に合わせて「より少ない作業量でやりくり」します。

一体どうやって両方を達成できるでしょうか。

そこで、より広範な組織の文脈の中で、この 2 つの責務について考えてみましょう。

結局のところ、この岐路では、ひとつの職務を選んで、もうひとつの職務を無視することはできません。

セキュリティチームは、少ないリソースで予防的な改善を行うために、両方の道を同時に歩む方法を見つけなければなりません。

このガイドではその方法を紹介します。

セキュリティの責務 1:

予防的な改善のための「レスポンシブサイバーエコシステム」の構築

たとえば、最近の Gartner のレポートでは、アナリストは、最新のセキュリティチームが「レスポンシブサイバーエコシステム」と呼ぶ仕組みを開発する必要性について述べています。

これらのレスポンシブエコシステム:

- 継続的に環境をスキャンする
- 現在および潜在的なリスクを特定する
- 問題が顕在化する前に対応を試みる

これらの目標は、継続的な脅威暴露管理、ユーザーとアクセスの検証、セキュリティギャップを検出し最小化する「デジタル免疫システム」の構築によって実現されます。

これらは、どのセキュリティチームにとっても非常に野心的な取り組みですが、次に説明するように、セキュリティツールの削減を奨励している今日の環境では特に困難です。

これらの傾向は、脅威管理とサイバーセキュリティの検証に**継続的なアプローチを適用することで、リスク解決への取り組みを前進させます。**検出と対応能力を向上させ、よりデジタルに免疫が高い ID エコシステムを構築するのに効果があります。

- Gartner
「2023 年の主要な戦略的サイバーセキュリティの動向」

Gartner

ivanti

セキュリティの責務 2:

セキュリティコストセンターの技術スタックを統合

一方、セキュリティツールの統合と再構築を求める 2 つ目のトレンドは、セキュリティ部門や IT 部門でさえ、予測不可能な経済による財務的圧力を完全に回避することができないことを物語っています。

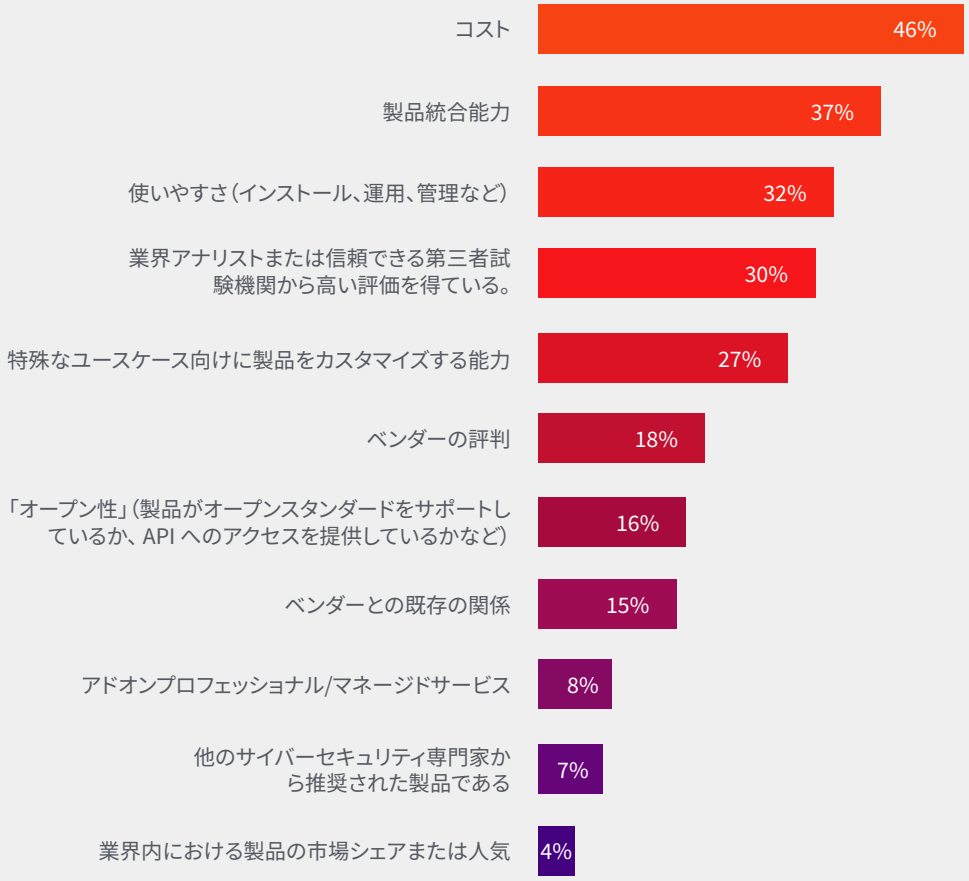
結局のところ、両チームはビジネスのセキュリティと機能にとって重要ではあるものの、直接的に収益を生み出すわけではありません。

ウォール・ストリート・ジャーナル紙の業界インタビューによると、セキュリティはコストセンターであるという認識から、CSO や CISO は、技術の統合や現在使用しているツールの統合を進めるなどして、部門の経費を削減するよう強く求められるようになったといいます。

また、ESG と ISSA の最近の調査によると、調査対象のサイバーセキュリティ専門家は、第三者機関によるテストや業界アナリストの推奨よりも、コスト、製品統合機能、使いやすさを重視する傾向があることがわかりました。

このような圧力は、ニッチなテクノロジーや「最高のテクノロジー」ではなく、多機能なプラットフォームを求め、技術スタックを統合するよう組織をさらに駆り立てています。

あなたの組織がサイバーセキュリティ技術を購入する際に、最も重要視する製品はどれですか。



（回答者の割合、N=280、3 回答可）出典: ESG, a division of TechTarget, Inc.

第三の道: 部門横断的なツールを活用した事前予防的セキュリティのユースケース

現在の火災を消火するだけでなく、将来の火災も未然に防ぐという、一見相反する 2 つの使命を背負わされ、しかも予算はますます限られているため、使い捨てのツールを使う余裕はありません。セキュリティチームは、不明確な岐路で不可能な決断を迫られています。

どの道を進むべきか？
どちらを優先するか？

しかし、もし新たな道を切り開く方法があるとしたらどうなるでしょうか。セキュリティチームが両方の義務を果たせるような、まだ名前の知られていない第 3 の道があるとしたら？

この第 3 の選択肢は、導入に迷ったり、チームを疲弊させたり、時間やリソースを浪費したりすることなく、予防的な改善と高価なポイントツールの削減という 2 つの成果をもたらすものでなければなりません。

この道は、セキュリティが他のチームのツールやソリューションをよりうまく再利用し、自分たちのユースケースに再利用できる場合にのみ可能となります。

最初の機会 IT チームの現在のツールとアーキテクチャ。

このようにして、セキュリティチームは、すでに予算化され使用されている IT プラットフォームを再利用することでコストを削減しながら、迅速なサイバーセキュリティ環境を構築することができます。

また、セキュリティチームがすでに導入済みの IT ツールを使用する利点は、目先のコスト削減だけではありません。ツールの簡素化によって業務が改善され、従業員がより効率的になることが多いというのがアナリストの意見です。

共有ツールプラットフォーム:

- 部門間の連携を強化する
- 各チームの管理負担を軽減する
- サイバーセキュリティ体制を総合的に改善する

ただし、セキュリティチームと IT チームの双方が、IT ヘルプデスクのチケット削減やセキュリティのDevSecOpsアプリケーションを超えた「シフトレフト」の重要性についての理解を共有し、アプローチを拡大する場合に限られます。

02

DevSecOpsの先にある「シフトレフト」の定義:

セキュリティと IT のアプローチの共通点を見つける

このセクションの内容:

1. セキュリティと IT における相反する「シフトレフト」の定義
2. シフトレフトに対する共通のアプローチ

ivanti

セキュリティと IT における相反する「シフトレフト」の定義

セキュリティ業界も IT 業界も「シフトレフト」という言葉を使いますが、それぞれのチームによって言葉の定義は異なります。
このような違いは、いくつかの共通点や目標の共有にもかかわらず、チーム間の摩擦を増大させることにつながります。

	DevSecOpsのためのセキュリティの「シフトレフト」	IT 部門のヘルプデスクチケットの「シフトレフト」
定義	セキュリティの専門家とツールは、最終的な導入の直前ではなく、開発中にセキュリティリスクを特定します。	エンドユーザーが気づき、ヘルプデスクのチケットを申請する前に、技術によって潜在的な IT 問題が自動的に特定されます。
重点	DevSecOps　リリースモデルの一部として、製品およびプロセス開発に集中します。	社内のエンドユーザーに対する IT ヘルプデスク業務のサービス管理に専念できます。
当面の成果	予防的かつ継続的な改善により、製品およびプロセス展開の遅延を削減します。	ヘルプデスクへのチケット申請を減らし、より高いレベルの IT スペシャリストへのエスカレーション率を下げます。
その他の利点	セキュリティを事後的な検討事項にするのではなく、「セキュリティ第一」の組織文化を推進します。 セキュリティが外部監督当局から不可欠なチームメンバーへと移行することで、サイロ化が解消されます。	専門性の低い IT 専門家が問題を修正できるようにします。 ヘルプチケットの申請が減り、全体的な人件費が削減されます。
タイムラインへの影響	セキュリティが納期直前の障害ではなく、予防的に考慮されるようになると、既知のセキュリティリスクが低減され、製品やプロセスの開発スケジュールが（場合によっては延長されるかもしれないが）ますます予測可能になります。	IT担当者は、専門的な能力開発と、より幅広い戦略的で能動的なタスクを増やすための時間とリソースを新たに見つけました。

結局のところ、シフトレフトの戦術的な表現がセキュリティチームと ITチームで異なるように、各部門のユースケースにはいくつかの基本的な特徴があります。

実際、どちらのモデルも、コストのかかる土壇場での緊急事態に対処するため、問題の初期段階で、時間をかけずに予防的に修復する必要性を、セキュリティと IT が共有していることを示しています。

セキュリティと IT のシフトレフトに対する共通のアプローチ

Ivantiでは、「シフトレフト」という言葉を、問題が真の問題や緊急事態になる前に、多くの場合、そもそも問題があったことに外部のステークホルダーが気づく前に、問題を軽減し、解決する戦略的プロセスを指す言葉として使用しています。

こうすることで、シフトレフトは、部門をまたがる自動的かつ予防的な改善の文化的アプローチとなり、以前はサイロ化されていたプロセスを、単一の統一された基礎的アプローチの下に統合することができます。

この定義は、IT 部門の中核的なユースケース、つまり、問題が発生する前に、また、問題が発生していることを誰もが知る前に、問題を解決するというユースケースを忠実に反映しているが、このシフトレフトアプローチは、DevSecOps特有の実装や考慮事項を超えて、予防的でレスポンシブなエコシステムを構築するというセキュリティ部門の使命と密接に連携しています。

人間がその存在に気づく前に問題を解決するというその性質上、自動化はあらゆる部門のシフトレフトを支援する上で重要な役割を果たしますが、次の章で各チームが気づくように、特に共有セキュリティと IT のユースケースにおいて重要です。

シフトレフトとは何か

このガイドでは、「シフトレフト」とは、**小さな問題が大きな緊急事態になる前に、多くの場合、**外部のステークホルダーが問題の存在に気づく前に、問題を特定し、軽減し、解決する戦略的プロセスと戦術的自動化のことを指します。

03

IT ツール + セキュリティ:

セキュリティチームが一般的な IT ツールを活用するための実践的なユースケース

このセクションの内容:

1. ITAM および ITSM + セキュリティ
2. UEM + セキュリティ

ivanti

セキュリティのために使用する一般的な IT ツール: ITAM、ITSM、UEM

セキュリティが使用する可能性のある IT ツールのうち、ここでは 2 つの一般的なソリューションプラットフォームに注目します。

これらの解決策は、さらに3つの異なる解決策に分けることができます

1. IT 資産管理 (ITAM)
2. IT サービス管理(ITSM)。
3. 統合エンドポイント管理（UEM）には、最新のデバイス管理（MDM）クライアントと機能も含まれます

IT 部門は従来、これらの共通技術に対する監督と予算配分を担ってきましたが、セキュリティ部門は IT パートナーと協力することができます。

このパートナーシップは、かつてのポイントソリューションやニッチな製品スタックが、統合による淘汰を乗り越えられる堅牢で部門横断的な多目的プラットフォームに変わります。

一般的な IT ソリューションとツール

サービス管理

ITAM (IT 資産管理)

- 自動的に更新される組織資産のリスト/データベース
- 資産、ユーザー、アクティビティに関する標準および既定の変数を追跡可能

ITSM (IT サービス管理)

- IT部門の中心的なユーザー向けジョブボードと準プロジェクトマネージャー
- Wiki、FAQ、内部フォーム機能を含むことが可能
- IT 関連のバックエンド自動化をホスト可能

デバイスとエンドポイントの管理

UEM (統合エンドポイント管理)

- エンドポイントデバイス管理とポリシー制御の基礎
- 各組織のデバイスとエンドポイントに存在する MDM クライアントを含むことが可能

ITAM および ITSM + セキュリティ

このセクションの内容:

- ITAM と ITSM の定義
- ITAM と ITSM のセキュリティに特化した使用事例
- ITAM と ITSM でセキュリティのシフトレフト

簡単な定義: ITAM と ITSM

IT 資産管理 (ITAM) ツール	IT サービス管理 (ITSM) ツール
ITAM は、ハードウェアやソフトウェア資産などの構成アイテム (CI) の管理を提供します。	ITSM は、IT 部門がエンドユーザーやその他の社内顧客からの技術的なリクエストを追跡し、対応し、サービスを提供する能力を向上させます。
このツールを使えば、企業は CI のライフサイクル全体 (購入から廃棄まで) を通して、CI の構成、最適化、追跡を行うことができます。	ITSM には、ヘルプデスクサポートのレベルをゼロにする「セルフヘルプ」の動きとして、ユーザーが簡単で一般的な技術的問題を解決するための補助的な機能が含まれていることもあります。

ITAM がパートナーの ITSM プラットフォームなしで存在することはめったにありませんが、ITSM 製品は ITAM パートナーの補完機能なしで実装することができます。

優れた ITAM と ITSM のソリューションプラットフォームは、いずれも次の項目を追跡します。

- 元の購入日と情報
- デバイスの所有者とユーザー
- 現在適用されているユーザーアクセスアプリケーションポリシー
- ソフトウェア OS、および現在のアプリケーションとソフトウェアのインストールと使用状況
- デバイスの位置情報
- デバイスの種類
- パフォーマンス、使用状況、コンプライアンス状況

ITAM と ITSM のセキュリティに特化した使用事例

適切なセットアップ、ポリシー、IT チームとの連携があれば、組織の現在の ITAM と ITSM プラットフォームは、セキュリティチームに以下のような重要な洞察を提供することができます。

1

動的な資産検出

2

構成管理データベース (CMDB) 機会

3

ガバナンス、リスク、コンプライアンスの強化 (GRC)

4

手作業が多いセキュリティ業務を支援する再構成可能な独自の IT 自動化機能

1 セキュリティと資産検出

資産の検出と管理は、あらゆるセキュリティプログラムの基礎となるものです。実際、すべての主要なサイバーセキュリティフレームワーク (CSF) やデータ保護規制は、資産検出を安全なシステム構築の基本と考えています。

その理由は？サイバー攻撃を成功させるための第一歩は偵察です。悪意ある行為者は、組織の CI 資産やシステムを可視化することで、何をどのように攻撃するかを知ろうとします。

一部の CSF における資産開示要件

CSF	関連セクション	資産検出の関連引用
NIST サイバーセキュリティフレームワーク	第一の中核機能: 特定する	「特定する: システム、人、資産、データ、能力に対するサイバーセキュリティ・リスクを管理するための組織的理解を深める」
Center for Internet Security (CIS) Critical Security Controls, V8	第一の統制: インベントリ	**「物理的、仮想的、遠隔地、およびクラウド環境内のインフラに接続されたすべての企業資産** (ポータブルおよびモバイルを含むエンドユーザーデバイス、ネットワークデバイス、非コンピューティング/モノのインターネット (IoT) デバイス、サーバー) を能動的に管理 (インベントリ、追跡、および修正) し、**企業内で監視および保護が必要な資産の全体像**を正確に把握する」 「また、削除または修復すべき未承認や管理されていない資産の特定をサポートします」
Australia Cyber Security Centre: Essential Eight	成熟度レベルの概要	「このシステムには、あらゆる成熟度レベルの攻撃を防ぐための重要なステップとして、**資産検出**が含まれています」
欧州法指令 2022/2555 (NIS2)	条項 44	「CSIRT (コンピューターセキュリティインシデント対応チーム) は、新たに特定されたサプライチェーンの侵害や重要な脆弱性に関して、事業体の全体的な組織リスクを特定、理解、管理するために、重要な事業体からの要請に応じて、事業体のインターネットに面した資産**を敷地内外で監視する能力**を持つべきです。

そのため、どのフレームワークも、サイバー攻撃から身を守るためには、セキュリティチームが何を守っているのかを正確に理解する必要があります。

もちろん実際には、ほとんどの組織でネットワーク資産の可視性に 20〜30% のギャップがある傾向があります。

実際、自社のネットワークにアクセスしようとするすべてのデバイスを完全に可視化できていると答えた IT 専門家は 47% に過ぎません。

しかし、ITSM や ITAM 製品など、さまざまな IT 技術プラットフォームに搭載されている資産自動検出機能を利用すれば、セキュリティチームが技術資産やユーザーに関連するリスクを能動的に分析できるようになります。

「環境に何があるのかを知らなければ、安全を確保することはできません。「脆弱性管理で最も懸念されることは、攻撃対象と目に見えるものを理解することです。」

- クリス・ゲットル
Ivanti エンドポイントセキュリティ製品管理担当部長

IT 部門にとって、自動化された資産検出は、予算化されたデバイスやソフトウェアの購入と、ネットワーク上のデバイスや使用統計との照合に役立ちます。

ITSM と同期すれば、これらの統計はユーザーのヘルプデスクリクエストと組み合わせることができ、IT チケットや障害の可能性を文脈化することができます。

セキュリティチームにとっては、IT 部門のソリューションにある同じ資産検出機能を再利用して、あらゆるセキュリティフレームワークの資産検出要件を満たすことができます。

また、自動資産検出のセキュリティのユースケースは、既定の設定から想像されるよりもさらに推進でき、セキュリティチームは次のことができるようになります。

検出

ベンダーのデバイスを使用し、サードパーティのアクセスポリシーに準拠するようにアクセスを制御する

スキャン

リモートでデバイスを操作し、組織のセキュリティポリシーやパッチ更新に準拠しているか確認する

セグメント化または修正

過渡デバイス

2 セキュリティと CMDB

自社の資産を知ることは、予防的なセキュリティ実装に向けた最初の、そして最も基本的なステップです。しかし、チームが組織全体のリスク環境を完全に理解するためには、各デバイス、アプリ、ユーザーが互いにどのように相互に作用しているかを知る必要があります。

IT の構成管理データベース (CMDB) は、このような関係に対する重要な洞察を提供します。

ITAM が資産のライフサイクルを追跡するのに対し、CMDB（多くの場合、ITSM プラットフォーム内に収容される）は、構成項目（CI）とその環境との関係を管理します。

ITAM と同様に、CMDB には、誰が特定のワークステーションを使用しているか、その場所はどこかといった基本的な資産やユーザー情報が含まれます。しかし、どのデバイスやソフトウェアがそのワークステーションと連携しているかといったコンテキスト情報も含まれます。

経験豊富なセキュリティの目には、このような関係から、CI がリスクにさらされていること、そしてそのリスクを軽減するためのヒントが見えてきます。

3 セキュリティと GRC

こうしたネットワーク上の関係やアクティビティをマッピングすることで、コンテキストに基づいたリアルタイムのガバナンス、リスク、コンプライアンス（GRC）の理解と実施も可能になります。

ITAM と ITSM がセキュリティの GRC をどのように支援するか

ガバナンス

共有データによるコンテキストの拡大
誰も従わないような指示、つまり自分のチームや組織に関係のない指示は出したくないものです。.

セキュリティチームと IT チームは、ITAM と ITSM の機能によって収集された正確なデータを使って、組織のリスク、ユーザー、資産環境の現状を理解し、適切で意味のあるポリシーを作成することができます。

バックエンド経由の既定のポリシー
IT 部門がすでに管理しているのと同じバックエンドシステムを使用することで、セキュリティチームは、セキュリティに焦点を当てたポリシー、管理、文書が整理され、簡単にアクセスできるようになります。

また、各部門にまたがる技術プロセスに情報を提供する広範な組織文書に、ポリシーが既定で含まれるようにします。

リスク

検出による攻撃対象領域のマッピング
ITSM および ITAM 製品を使用することで、セキュリティ・チームは組織の潜在的な攻撃対象領域をマッピングし、ネットワーク、デバイス、ユーザーの構成を分析できます。

ハッカーにさらされる真の攻撃対象領域をより深く理解することで、組織固有の脅威環境とネットワーク活動に最適なセキュリティ戦略と戦術を提供します。

CMDB による自動化トリガー
セキュリティチームは、現在の CI を利用し、ITAM の CMDB で追跡されるカスタムのセキュリティ固有の変数を、自動化された計算式のトリガーやコンポーネントとして作成できます。

コンプライアンス

データ収集によるベンダーの施行
ITAM リストや常に更新される ITSM プラットフォームを通じて収集されたデータを使用することで、セキュリティチームは、組織のポリシーへの実質的なコンプライアンスをサポート、施行するベンダー契約の作成を支援し、サプライチェーンのセキュリティリスクを低減することができます。

検出によるエンドポイント施行
資産検出機能により、IT 部門とセキュリティ部門の双方が、機密性の高い組織ネットワーク上の未承認デバイスを特定できます。

これらの機能は、デバイスの自動コンプライアンスアラート、ネットワークセグメンテーション、あるいは必要に応じてエンドポイントの完全な隔離もサポートします。

IT ポリシーによるセキュリティ施行
組織全体で一般的なコンピューターポリシーを実施するのと同じ IT 機能が、必要に応じてセキュリティプロトコルを報告し、施行することもできます。たとえば、ヘルプデスクの問題でユーザーを支援する IT 管理者に安全策を講じたり、ポリシー違反の可能性や内部脅威の指標に関するアラートを送信したりすることができます。

現実世界への影響

病院タブレットの思考実験

あなたが病院に勤めていると仮定してみてください。

IT およびセキュリティチームは、医療関係者のみがアクセスすべきタブレットを含め、インターネット機能を持つすべてのエンドポイントを追跡しています。

しかし、あるセキュリティ専門家は、病院内のデータベースやイントラネットしか見ないはずのタブレットが、奇妙な動きをしていることに気づきました。

実際、このエントリは外部インターネットブラウザーへのアクセスを記録しており、「情報漏洩」ゲームアプリのダウンロードを試みていました。.

その不審な行動は、ITSM / ITAMの自動化（CMDB のログと CI の変数を一部使用）によって警告されたので、セキュリティチームは調査し、その行動に関して最も最近ログに記録されたユーザーを調査します。.

結局、そのフロアの監督者は、患者が治療を受けている間、気軽にインターネットを閲覧するためにタブレットを使わせることを職員に非公式に許可したことを認めました。

(実際、このフロアでは小児患者しか診察していません!)

確かに、監督者は子どもたちを含むすべての人を守るために作られた社内の手順や方針に違反しました。– ハッカーから保護される。

しかし、セキュリティチームは、怠慢や態度の悪さではなく、善意を想定して、この誤ったエンドユーザーを罰しないことを選択するかもしれません。

その代わり、IT 部門と協力して、引退間近の古いタブレットを患者用に再配置することもあります。

これらのタブレットは、患者が治療中に（セキュリティ上承認された）ゲームをプレイできるようにする一方で、機密性の高い病院のイントラネットから隔離し、悪意のある行動を自動的に追跡します。

最初は関係者全員が少し苦労するかもしれませんが、この解決策は三拍子そろったものになるでしょう。

患者 は、以前と同じようにケアされ、十分に治療されていると感じています

セキュリティと IT はともに、ユーザーが積極的に回避しようとするポリシーを強制する「No 部門」になることを避けます。

エンドユーザーである職員 エンドユーザーである職員は、「本物の」タブレットを患者と共有する以外の選択肢があります。セキュリティがあれば安心だと感じ、将来的なセキュリティや IT の要求に進んで応じる可能性が高くなります。

4 ITAM と ITSM の自動化でセキュリティのワークロードをシフトレフトする

IT のツールをセキュリティのユースケース（特に ITAM や ITSM）に活用することを検討する際には、現在の IT に特化した自動化や実装を利用して、チームのシフトレフトを促進する方法を検討します。

ダッシュボード上の基本的なアラートやダイヤルを超えて、真に予防的なリスク修正を行うことで、より少ない労力でより多くのセキュリティ対策に取り組むことができることがわかります。

1 エンドユーザー向けセルフサービスオプションの改善

セキュリティに関するリクエストや質問で、シニアアナリストをフィッシングの特定から解放します。

2 セキュリティインシデント解決の一元化

ITのチケットソフトウェアや優先順位付けキュー（リクエストフォームから供給される）と連携することで、優先順位付け、追跡、コンテキストの可視化を改善します。

3 バックグラウンド IT 自動化の再利用

セキュリティ目的では、ユーザーがチケットを提出する前にデバイスを修正できるのと同じ自動化が、エンドポイント環境のセキュリティを向上させ、悪意のある活動を検知することもできるからです。

自動化 1:

「レベルゼロ」サポートのためのセキュリティセルフサービスを改善します。

IT ヘルプデスクの負担を軽減する同じシステムは、セキュリティに関する問題にも利用できます。!

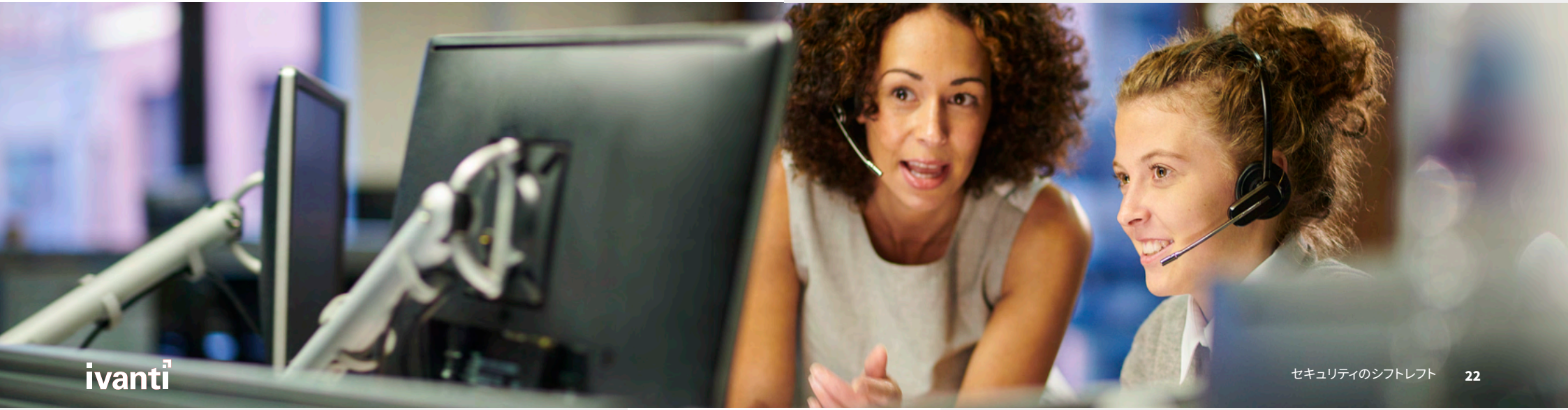
2 要素認証の有効化、フィッシング攻撃の疑いに関する報告、パスワードリセットのリクエスト方法など、セキュリティに関連する一般的な質問やリクエストを一元化することで、エンドユーザーはセキュリティチームに直接サポートを依頼するのではなく、自分たちで解決できるようになります。

セキュリティに最も頻繁に必要とされる回答、情報、リクエストを、IT部門と同じインフラを持つ1つの場所に統合することで、エンドユーザーはどこを探せばよいかを正確に知ることができます。結局のところ、それはIT情報を得るために利用するのと同じ方法なのです。そして、システムを回避する方法を探そうとはしないでしょう。

★★★★

セキュリティ Wiki では、次のような内容を検討してください。

- **現在のすべてのポリシー** 各ポリシーには、どのユーザーとデバイスがポリシーの対象となるのか、ポリシーによってどのような制限や許可が与えられるのか、例外要求のプロセスと場所、そして（最も重要なこととして）このポリシーがどのように組織を保護するのかが、スキャン可能なリストで前置きされている。
- **新しいパスワードまたはユーザー名をリクエストする方法。**
- **新規ベンダーやソフトウェアのセキュリティ承認申請方法** – また、セキュリティが単発のアプリを承認しなければならない理由や、それによって組織の安全がどのように保たれるのかについても説明する。
- **2FA** を組織の各対応デバイスとアプリケーションに実装する方法。
- **社内のステークホルダーとのコミュニケーション用に承認された、将来の導入計画に関するセキュリティポリシーロードマップ。**



自動化 2:

コンテキスト化されたデバイスとユーザーデータでセキュリティチケットキューを一元化

ヘルプデスクチケットと同じITSMプラットフォームで、セキュリティの質問や改善の優先順位付けのための特定のキューを形成することができます。

レベルゼロの「セルフサービス」ユーザーサポートのために、セキュリティ wiki 内にファイルアクセスやポリシー免除のリクエストフォームを実装することもできます。

これらのフォームにより、ユーザーのリクエストが一元化された公開キューに送信されます。このため、メールの受信トレイに散在し、専門家が「優先度の高い仕事」に先に取りかかることで、いつまでも無視されることがなくなります。

そうすれば、これらのリクエストは、下位のセキュリティ・レベルの従業員が簡単に割り当てて解決することができ、より優先順位の高い事項に戦略的なマンパワーを確保することができます。

さらに、セキュリティWikiを作成することで、セキュリティチームは、Wikiに書かれたポリシーにリンクして、役員レベルのステークホルダーに対してでさえ、リクエストされた許可を与えるか拒否するかを判断することができます。

自動化 3:

IT 自動化を、拡大された予防的セキュリティのユースケースに再利用します。

ITAMやITSMの特定の設定に基づいてトリガーされる同じ修正および予防的IT自動化は、さまざまなセキュリティ目的のために複製され、微調整することができます。

セキュリティユースケースのための IT 自動化

デプロビジョニング

離職する従業員またはベンダーの資格情報が、契約終了またはユーザーステータスの入力をトリガーとして廃止されることを確認します。

ベースライン評価

自動化により、組織の活動の「ベースライン」を収集・集計し、生産性に対する将来のセキュリティ上の影響や侵入の可能性を発見するのに役立ちます。

悪意ある活動の警告

正常でない CI をトリガーとして、潜在的な内部脅威や侵害されたアカウントに警告を発し、人間のセキュリティアナリストによる手作業でのデバイスやユーザーのレビューを促します。

ロールアウトの監視

パッチやポリシーのロールアウトの際には、あらかじめ決められたウォーターフォールスケジュールに基づき、現在のワークフローで管理されているユーザーやデバイスのプロファイルごとに優先順位をつけて、混乱を監視するように自動化を設定することができます。

UEM + セキュリティ

このセクションの内容:

- UEM と MDM の定義
- UEM のセキュリティに特化した使用事例
- UEM 自動化によるセキュリティのシフトレフト

簡単な定義: UEM と MDM

統合エンドポイント管理 (UEM)	モバイルデバイス管理 (MDM)
UEM は、システム管理者が複数のエンドポイント（デバイス、ハードウェア、その他の技術）を単一のプラットフォームまたはダッシュボードから管理するために使用する IT 技術プラットフォームです。 UEMは、さまざまなメーカーや開発者が提供する幅広いオペレーティングシステム（OS）とデバイスに対応しています。	現在では「最新」デバイス管理と改名されることも多いMDMは、かつてはITチームがMDMのAPIをサポートするスマートフォンやタブレット、その他のエンドポイント上のポリシー、設定、ソフトウェアを制御し、実施するのを支援するスタンドアローンのニッチ技術でした。 しかし、MDMは特定のオペレーティングシステムを実行しているデバイスに限定されることが多く、ITチームはすべてのデバイスを管理するために複数のMDMを同時に実行する必要がありました。 現在でもOSメーカーやニッチデバイスメーカーはエンドポイントを管理するためのポイントMDM製品をリリースしていますが、包括的なUEMソリューションには、そのプラットフォーム内にMDM機能が含まれています。

UEMプラットフォームは、ITチーム、そして今ではセキュリティチームをもサポートします！単一のプラットフォームとダッシュボードからハードウェアとソフトウェアの資産を管理することができます。次の点の影響は受けません。

- OS
- デバイスの種類
- デバイスまたはアクセス場所
- 固有のユーザー権限

UEM のセキュリティに特化した使用事例

ITチームのUEMとMDMクライアントは、次のようなセキュリティチームのニーズに合わせて再構成できます。

特定のデバイスとユーザープロファイルに対するセキュリティ優先のアクセス制御を念頭に置いた、新入社員向けの予防的なデバイス展開

堅牢なモノのインターネット（IoT）制御とネットワークセグメンテーションにより、ハッカーがコアネットワークに侵入する足がかりとなる、更新が難しく追跡が困難なデバイスをロックダウンします。

将来的な拡張やユースケース（ITとセキュリティの両方）に対応する、OSやデバイスに依存しない包括的な基盤です！ - 予算が増え、ニーズが高まるとき

セキュリティとデバイスのオンボーディング

現在のITプロセスにセキュリティが入り込みやすいのは、新入社員の入社時です。特に、現在ハイブリッドや完全リモートを導入している組織ではなおさらです。

結局のところ、IT部門は、オフィスに一歩も足を踏み入れることのないエンドユーザーに対して、適切なソフトウェアとアクセス許可を備えた新しいデバイスをプロビジョニングする責任があります。

このプロセスは、リモートユーザーやデバイスが組織のネットワークに接続する前に、最初から安全に設定されていることを確認する、セキュリティのためのまたとない機会を提供します。

UEMソリューションにより、IT管理者は、以前に確立された仮想マシン（VM）に基づいて、新しいノートPCやPCに事前設定されたユーザープロファイルやデバイスプロファイルを設定することもできます。

ITSM　と組み合わせることで、採用担当者は、実際の依頼やデバイス/プロファイル設定の前に、IT　部門の誰かを積極的に巻き込むことなく、依頼や許可の際にセルフサービスポータルを使用することができます。

おそらく、IT 部門はすでに新規ユーザーのオンボーディングのためのプロセスを導入しているはずです。次の点を確認してください。

- どのようなプロセスステップをすでに導入しているか
- 導入の際にUEMをどのように使用しているか
- セキュリティ担当者やポリシーが、標準的な業務手順の中に紛れ込んでしまう可能性があります。

現実世界への影響

初日からセキュリティポリシーを組み込む

Forrester Consulting が Ivanti に委託して実施した TEI 調査のインタビューでは、ある靴の小売業者の統合エンジニアが、以前はソフトウェアのインストールや構成に 1 台あたり 2〜3 日かけていたと語っています。

しかし、Ivanti Neurons for UEMを導入した後、インタビューの対象者は次のように述べました。

「現在では、イメージ化されたら、Ivantiをインストールし、そのデバイスをすべてのソフトウェアタスクにドラッグするだけです。5 〜 10 分程度で完了し、1 日の終わりにすべてのアプリケーションがインストールされていることを確認するだけです。ユーザーのオンボーディングプロセスにかかる時間が確実に短縮されました。」

「時間があるときに」と後回しにするのではなく、チームの構成要件をこの最初のオンボーディングに含めることができます。

必要なのは、各ユーザープロファイル、チーム、デバイスの種類ごとに、組織で必要とされる最小限のデフォルト権限、アプリケーション、アクセスについて、ITパートナーと入念に交渉することだけです。

FORRESTER®

セキュリティと IoT

IoT エンドポイントセキュリティポリシー（UEMおよびMDMクライアントを通じて提供され、実施される）は、セキュリティチームが現在のITの技術スタックを再利用しようとする際に、優れた付加価値を提供します。

結局、IoT 攻撃は、2021 年には世界の全マルウェア攻撃の 12% 以上を占めていました。これは、2019 年の全マルウェア攻撃の 1% 未満という数値から上昇しています。

しかし、調査対象となった IT 専門家の 47% は、自分の組織には IoT コンプライアンスポリシーがないと回答しています。

おそらく、これらの組織にはIoTポリシーが欠如していたのではなく、むしろIoTポリシーについて知らなかったようです。

しかし、チームやスペシャリストからのセキュリティ情報を追加すれば、UEM の比較的シンプルなネットワークセグメンテーションとアクティブスキャン機能によって、企業やリモートの職場にある脆弱なインターネット対応デバイスを修正できるようになります。

現実世界への影響

温度計の脅威

北米のあるカジノでは、ハッカーがカジノのロビーの水槽の温度計の脆弱性を利用し、管理されていない IoT が経営に大きな影響を与える可能性があることが判明しました。

この対応水槽はカジノのネットワークでのセグメント化が不適切であったため、ハッカーはカジノのクラウドインフラストラクチャに横移動して攻撃を続けることができました。

セキュリティと相互 OS 統合

この eBook では、現在の IT ツールやプラットフォームを再利用することをテーマにしていますが、いずれは組織のセキュリティ・リスクや要件が、現在のツールが提供するポリシーや施行オプションでは対応できなくなることを私たちは知っています。

しかし、UEM ソリューションは、将来のセキュリティツールの導入をあらゆるデバイスとユーザーアクセスプロファイルに統合するための、非常に有利な出発点となります。

結局のところ、UEM 自体は、所有、管理されているすべての組織デバイスに直接クライアントがインストールされています。

UEM クライアント経由で他のセキュリティツールを同じデバイスに接続し、エンドポイントセキュリティの防御を即座に強化しつつ、組織のエンドユーザーの生産性を損なわないようにするには、基本的には数クリックで行えます。IT パートナーにとって大きな勝利です。

UEM や MDM を介して展開する将来のセキュリティ統合オプション

パッチ管理 (PM) とリスクベースの脆弱性管理 (RBVM)

ITSM、ITAM、UEM プラットフォームによって推進される自動化と監視を一歩進め、UEM 自体をリスクベースのパッチおよび脆弱性管理ソリューションと組み合わせることで、攻撃を受けた脆弱性を修正するためのシームレスで予防的なリスク対応が可能になります。

PM と RBVM ソリューションをセキュリティ設定された IT プラットフォームと組み合わせることで、セキュリティチームと IT チームは同様に、現在の資産環境と ITAM/ITSM プラットフォームからの重要なワークフロー情報によって相互参照され、IT セキュリティ SLA に従ってUEMによって配布される、頻繁に悪用される脆弱性に対する最も緊急なパッチをコンテキスト化することができます。

モバイル脅威防御 (MTD)

UEM の構成や設定は、フィッシングリンクのクリックによる最初の被害を抑えるのに役立つかもしれません。特にパッチソリューションと組み合わせて使用することで、ハッカーが権限を昇格したりネットワーク内を移動したりする能力を大きく阻害することができます。しかし、モバイル脅威対策 (MTD) の専用ソリューションと組み合わせなければ、その効果はほとんど期待できません。

最高の MTD ソリューションは、登録されたデバイスの UEM クライアント（組織所有のものでも BYOD プログラムで使用されるものでも可）を通して実行することができ、悪意のある可能性のあるアクティビティやフィッシング攻撃を動的に検出、セグメント化、隔離、警告します。

UEM でセキュリティのワークロードをシフトレフトする

ITAM と ITSM が、セキュリティのシフトレフトを IT に集中させ、これまで手作業で行っていた作業をより能動的に行うための自動化の機会をもたらしたように、UEM もセキュリティの目標達成に役立つ自動化機能を備えています。

UEM には、セキュリティチーム独自の自動化や実装があります。

離職する従業員やサードパーティベンダーの「ゾンビ資格情報」の 100% 廃止ポリシー遵守を保証します。

組織のネットワークへのアクセスを許可された、実際に管理されているデバイスまたは BYOD デバイスに対して、セキュリティポリシーを適用します。

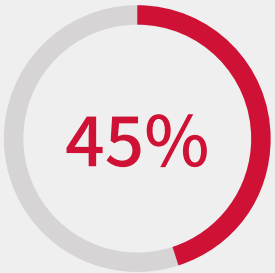
インシデント対応時やアラートの文脈を明確にするために、セキュリティに焦点を当てたデバイスの記録を編集してふるいにかけることができます。

1 「ゾンビ資格情報」の廃止 コンプライアンスの保証

Ivanti が 900 人以上のセキュリティ専門家を対象に実施したグローバル調査では、回答者の 68% しか、解雇または退職した従業員、サードパーティの請負業者、その他のベンダーに対する資格情報のデプロビジョニングガイダンスに従っていると回答していません。

実際、同じセキュリティ専門家の45%が、元従業員や請負業者が、廃止されなかった古いログイン情報を使って、会社のシステムやファイルにまだ不正にアクセスしている疑いがあると回答しています。これが「ゾンビ資格情報」です。

UEM プラットフォームとデバイスがホストする MDM クライアント内の自動化機能により、ユーザーの内部プロファイルが有効な用途に使用されなくなった場合、ゾンビ認証情報を即座に破棄することができます。



セキュリティ専門家は、元従業員や元契約社員が、まだ有効なユーザー名、パスワード、ログイン情報の形でシステムやファイルにアクセスできる疑いがあるか、確実にアクセスできると回答しています。

2 オフィス内でもリモートでも、すべての管理対象エンドポイントデバイスにセキュリティポリシーを適用します。

人的ミスは常にセキュリティ戦略の弱点であり続けますが、ITチームのUEMプラットフォームによって実施されるセキュリティソリューションとポリシーは、特にリモートやハイブリッドの職場にいる場合、あまり関心を持たないエンド・ユーザーによって引き起こされるリスクの一部を軽減するのに役立ちます。

たとえば、現代の脅威行為者が使用する初期の偵察や侵入の手法の多くは、適切な資産の検出、ネットワークのセグメンテーション、デバイスの監視によって改善することができます。

これらの改善はすべて、以下の方法で実行できます。UEMソリューション - 適切なセキュリティに重点を置いた構成とサポート機能。

セキュリティ重視のポリシーと設定を備えた UEM ソリューションを導入することで、企業はエンドユーザーが必要な更新やセキュリティアプリケーションをインストールすることに頼る必要がなくなります。

UEM で管理されたデバイスは、特定の更新スケジュールやアプリケーションインストールに自動的に登録されるため、ユーザーの操作は必要ありません。

3 インシデント対応時に UEM がホストするデバイスの記録をレビューします。

UEM プラットフォームが記録するデバイスやユーザーのログは、通常、エンドユーザーのデバイスをより効果的に修復するために IT 担当者が管理・確認するものですが、セキュリティ目的でも使用することができます。

たとえば、従業員が内部脅威となる可能性があると考えられる場合、セキュリティチームは、PowerShell などのシステム管理者ツールがユーザーのデバイスに不正にインストールされ、使用された形跡がないかどうか、デバイスのレコードを確認できます。

あるいは、ある組織のシステムが、普通の「ユーザー」の活動に対してアラートを発し、そのユーザーが組織の管理対象デバイスで突然高度なネットワーキング技術を実行したことを示すかもしれません。

このような活動は、実は正規のユーザーではなく、そのユーザーの (漏洩した) 認証資格情報の背後に隠れて、企業ネットワーク内で特権を昇格しようとしているハッカーであることを示す兆候かもしれません。

適切な構成、アラート、セキュリティツールがあれば、ハッカーが組織のネットワーク内を移動したり、管理者レベルの権限を取得するよりもはるかに前に、エンドポイントやモバイルデバイスでこのような活動を検出することができます。

また、サイバー保険料の高騰により、すでに疲弊している組織の財政に新たな圧力がかかる中、IT とセキュリティの両チームは、より厳格なポリシーとユーザーアクティビティに関するアラートを実施し、能動的なリスク修正と保険料の低減を図るという財務的な責任を負っていることに気付くかもしれません。

04

すべての道は DEX に通じる:

このセクションの内容:

1. セキュリティチームとITチームの両方がDEXを気にすべき理由

2. 共有技術スタックからのバックエンド DEX が技術管理者にどのように役立つか

DEX: IT とシフトレフトする際のセキュリティの隠れた優位性

このガイドを通じて、セキュリティチームは、IT チームがすでにサポートしている ITSM、ITAM、UEM の機能を利用するだけで、技術的な負担を軽減すると同時に、緊急時の消極的な対応から、より能動的で即応性の高いサイバーエコシステムへと成長できることを示しました。

しかし、IT とセキュリティツールを組み合わせて統合することで、組織にはさらなる利点がもたらされます。

これらのDEXの利点は、エンドユーザーだけでなく、組織全体を対象とすることができます。以下のようなユースケースも含まれます。

セキュリティの
ニーズ

IT のニーズ

一般的な技術
管理ニーズ

71%

クラス最高のセキュリティ組織は、エンドユーザーの DEX は組織のセキュリティ戦略にとって優先度が高いか、まさにミッションクリティカルであると回答しています。

(これは、成熟度の低い組織よりも20ポイントも高い数値です。)

エンドユーザー DEX は、セキュリティと IT の両方に利点がある

セキュリティ部門と IT 部門は、それぞれ異なる理由で従業員の体験に関心を持っていますが、エンドユーザーの DEX を向上させることは、すべての関係者にとって利益となります。

セキュリティにおける DEX の利点

DEX の利点	セキュリティチームが関心を持つ理由
優れたユーザー体験はシャドー IT を抑制します。	従業員は、組織のバージョンが面倒であったり、不満があったりすると、承認されていないデバイスやアプリ、つまりシャドーITに目を向けます。 2022 年には、クラウドベースのサイバー攻撃の 12.8% にシャドー IT が関与していました。 エンドユーザーのDEXを優先させることで、企業は、シャドーITを減らすと同時に、エンドユーザーにとってセキュリティで承認されたアプリケーションやデバイスでの作業を容易にします。なぜサードパーティのアプリをわざわざインストールする必要があるのでしょうか？
ユーザーの暗黙のコンプライアンスを促す、セキュリティポリシーの「隠された」バックエンド実装。	組織は、エンドユーザーに対して、特定の行動を取るか避けるかによって安全性を維持することを要求する紙のポリシーを発行することができます（そして、実際に発行しています！）。 あるいは……セキュリティチームは、すべての管理対象デバイスとネットワークユーザープロファイルにポリシーを黙々と適用するバックエンドの自動化を実装するだけでもよいでしょう。ユーザーがこれらのポリシーを知るのは、不正なアクションを起こした場合だけです。そうでなければ、これらの制限の存在に気づくことはありません。 このようなDEXに適したセキュリティ実装は、組織がもはや平均的なエンドユーザーの好意や記憶に頼るのではなく、むしろユーザーに何も求めない堅実なバックエンド実装に頼ることを意味します。
ハイブリッド対応のセキュリティコントロールは、場所にとらわれないユーザーの利便性を提供します。	リモートワークやハイブリッドワークが増加する中、セキュリティチームは、ネットワークやエンドポイントセキュリティに対する基本的な「壁に囲まれた庭」のアプローチにもはや頼ることはできません。 したがって、UEMやITAMのようなバックエンドのITプラットフォームを活用することで、オンプレミスでもリモートでも、あらゆるOS上で動作するあらゆる種類のデバイスを追跡、管理、保護することができます。これにより、セキュリティチームは、ユーザーがオフィスに出社することなく、組織の安全を守ることができます。

ご存じでしたか？

あなたの組織のIT部門は、エンドユーザーの生産性を向上させるために、継続的にDEXの取り組みを行っているかもしれません。

セキュリティチームと連携することで、ITリーダーは、現在共有されている技術スタックを正当化するための影響力をさらに高めることができ、そうでなければCIOの利害関係者にとっては抽象的すぎてさらなる投資を正当化できないと考えられていたDEXプログラムを継続できるようになります。

ITにおけるDEXの利点

DEX の利点	IT チームが関心を持つ理由
ユーザーエクスペリエンスに関する問題が減るということは、サービスデスクのチケット数が減り、サービス提供が迅速になることを意味します。	再起動による中断や、RAM不足による処理速度の低下もなく、デバイスがユーザーの要求通りに動作するのであれば、ユーザーがヘルプデスクチケットを申請する理由はありません ある宗教団体がDEXに重点を置いたITSMを導入したところ、ITチームはチケット数が減少し、ヘルプデスクのサポートスタッフのサービス体験が90%改善されました。
ユーザーの自己修復により、IT人材費が削減されます。	トラブルシューティングやリクエストフォームがエンドユーザーが見つけて使える場所にあれば、人件費が高いIT担当者ではなく、ユーザーが自分で問題を解決することができます。 ある大学では、ITSMベースのセルフサービスポータルをバックエンドの補完技術とともに導入した後、その新しいIT技術が学生や職員に全面的に受け入れられ、ネットワークに接続されたデバイスに新しいセルフヘルプ機能が広く採用されるようになりました。
DEXに重点に置いた技術は、表面的な修正にとどまらず、根本的な問題を解決します。	DEXに特化した技術スタックにより、ITチームは、障害が発生したデバイスが世界のどこにあっても、デバイスとそのユーザーアクティビティを迅速に評価し、表示することができます。 これらの洞察は、ありふれた問題を「修復」する高度な自動化と相まって、IT専門家が問題をより迅速に診断し、修正することを可能にします。 エンドユーザーに同じ問題で何度も問い合わせをさせることはなく、最初のチケットでデバイスを修正することができます。

管理者DEXは共有技術スタックの利点を享受

優れたデジタル従業員体験は、エンドユーザーだけではありません。このような技術を使う管理者も優れたDEXを享受できるはずです。

セキュリティおよびIT管理者にとってのDEXの利点

DEX の利点	管理者が関心を持つ理由
作業ツールやデバイスは、ユーザーが報酬を得て行う仕事を支援します。	調査対象となったセキュリティおよびIT専門家の31%が、技術的な問題もあって、現在の職を辞めることを検討しています。 最も高価な人財をなぜ磨り潰すのでしょうか。もし、彼らの技術体験を向上させれば、競争の激しい雇用市場で彼らを引き留めることができるかもしれないのに、です。
DEXを第一に考えた共有プラットフォームとダッシュボードは、部門を超えたコンピテンシーの向上と協力的な理解を意味します。	部門間で共有される直感的なツールセットにより、情報を共有し、問題をシームレスに提示することができます。 このように知識や状況を共有することで、共感が深まり、誤解が減り、各部門の協力体制が向上します。 また、各部門が基盤となるプラットフォームの基本的な理解を共有しているため、スキルは部門間ですぐに伝達されます。
共有された技術スタックによって、毎年最大9%失われる管理者の生産性を取り戻すことができます。	ハーバード・ビジネス・レビュー誌の「トグリング」に関する最近の記事によれば、技術系社員は頻繁に異なるプログラムを切り替えているため、生産時間を大幅にロスしていると指摘されています。 コンピューターベースの知識労働者は、1日に平均1,200回、プラットフォーム、インターフェイス、画面、その他のマイクロタスクを切り替えて（「トグル」して）いるため、1週間あたり推定4時間、年間有給労働の9%を浪費しています。 統合された共有プラットフォーム、少なくとも同様のユーザーインターフェイスとダッシュボードを備えた技術スタック！これにより、セキュリティ管理者とIT管理者の双方にかかる負担が軽減され、気が散ることなく与えられた課題に集中できるようになります。

参考文献

- Australian Cyber Security Centre. (30 June 2017). “Essential 8 Maturity Model”: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). “Shift Left to Risk-Based Proactive Security Management.” CIO’s The Future of Work Summit.
- Center for Internet Security. (2021). “Critical Security Controls Version 8”: https://www.cisecurity.org/controls/v8
- Forrester. (2022). “The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions”: https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). “The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti”: https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) “GDPR Checklist for Data Controllers”: https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). “Automated Patch Management and Team Swarming are Key Security Practices.” Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). “Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs.” Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). “Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). “How Much Time and Energy Do We Waste Toggling Between Applications?”: https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). “7 Experts on What Shift Left Means for IT Departments”: https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). “The NIST Cybersecurity Framework (CSF): Mapping Ivanti’s Solutions to CSF Controls”: https://www.ivanti.com/resources/v/doc/ivi/2694/fa2e133f20a8
- Ivanti. (2022). “The Ultimate Guide to Risk-Based Patch Management”: https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). “Press Reset: A 2023 Cybersecurity Status Report”: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). “ITSM+ Toolkit”: https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239
- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee

- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://www.ivanti.com/resources/v/doc/ivi/2700/4e528f833de3
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://www.sans.org/white-papers/sans-2022-cloud-security-survey
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

セキュリティのシフトレフト

現在のITツールでレスポンシブなセキュリティ環境を
構築する方法

ivanti

より詳しくは、ivanti.com/jaをご覧ください。

Copyright © 2023, Ivanti. All rights reserved. IVI-2778 NH