ivanti

統合エンドポイント管理のためのガイドブック

最新のエンドポイント管理ソリューションがどのようにセキュリティと従業員体験に影響するのか

目次:

ivanti

01

ポストコロナ時代のエンドポイント管理における新しい基準

5 年前、エンドポイントの管理とセキュリティは比較的分かりやすいものでした。

ほとんどの企業では、会社の業務で使うエンドポイントデバイスはオフィスにありました。オフィスは制御可能な環境であり、現場にいる IT およびセキュリティ担当者はほとんどのデバイスを簡単に検出、管理することが期待されていました。

そして、新型コロナウイルスの流行によって、従来のオフィス勤務主体の働き方が一変しました。

コロナ前にもリモートワークを推奨している企業も存在しました。2020 年にすべてがリモート状態になる前に、企業のノートパソコンやモバイルデバイスは、管理されたWi-Fiネットワークで運用されていました。

しかし、コロナの流行を機に、自宅勤務が推奨され、世界中の IT およびセキュリティ部門の方々は、その時にあったテクノロジーやデバイスを活用し、最善の作業体制を構築することに躍起になりました。

ルールの例外であったものが、今や誰にとってもルールとなったのです。

今、世界的な脅威としての新型コロナウイルスが衰退しているのに伴い、多くの雇用主が従業員にオフィス回帰を勧めています。 Ivantiの調査によると、ナレッジワーカーのうち、オフィスだけで仕事をすることを希望する人は 13% に過ぎませんが、経営陣の 56% は、従業員が生産性を上げるためにはオフィスにいることが必要だと考えています。 （Ivanti）

従業員が希望する働き方と、経営陣が従業員に対して効果的になると感じている場所との間にこのようなギャップがあります。それにより、IT とセキュリティ担当者は、難しい状況におり、率直に言って持続不可能な立場に置かれています。

この状況は、2019年のオンサイトでの管理とクローズドプラットフォームネットワークへの完全な復帰が、可能性が低く、賢明でないように思われるときに、さらに高まっていきます。

> 世界的な求人情報サイト Monster.com の 2022 年の調査によると、全従業員の 3 分の 2 が、1 週間フルタイムのオフィス勤務に戻る必要があるのであれば、仕事を辞めた方が良いと考えています。また、全体の40% が「1 週間の 5 日のうち 1 日だけオフィス勤務を義務付けられたら辞める」と回答しています。(Shumway)

> Twitter のCEOであるイーロン・マスク氏は、2022年11月、従業員に対し、週 40 時間、地域事業所のオフィスで勤務するか、辞職するかのどちらかを選択するよう通告しました。 （Yang） 数百人の従業員が彼の虚勢に応え辞職しました。（Bond） 2023 年 1 月初旬には、Twitter のフルタイム従業員数は約 7,500 人から約 1,300 人へと 80% 以上縮小し、フルタイムエンジニアは 550 人を下回っていました。 (Kolodny)

> Amazon の CEO であるアンディ・ジャシー氏が、2023 年 2 月に技術系従業員にフルタイムでオフィス勤務するように命じたとき、従業員は反発しました。 結局、ジェシー氏は、「週 3 日だけはオフィスで勤務しなければならない」と譲歩しました。 (Palmer)

オフィス勤務への回帰が生産性を向上させると信じている人たちに、調査結果はそうではないことを示しています。

- Gallupは、パンデミック時に、過去最高の従業員エンゲージメントレベル 40% を記録しましたが、その後、3 分の 1 未満に低下しています。(Smith)
- 2022 年上半期にかけて生産性が記録的に「低迷」しています。これは、全従業員をフルタイムのオフィス勤務に戻すことを求める企業の圧力が高まっていることと相関しています。 (Tsipursky)

このような傾向から、企業として従業員がオフィス勤務の義務に従っているように見えても、単に静かに辞めていくだけかもしれないことがわかります。従業員は、必要最低限のことをこなしながら、パンデミックの緊急時に最も魅力的であった柔軟な働き方を可能にする新しい機会を求めています。 (Tsipursky)

明白な解決策: リモートワーク、オフィス勤務、または可能なかぎり従業員それぞれに最適な組み合わせた形態で勤務を継続できるようにする。

実際に、2022 年の Integrated Benefits Institute の調査によると、ハイブリッド環境またはリモート環境で働く従業員は、生産性が 21.8% 高く、満足度が 20.7% 高く、エンゲージメントが 50.8% 高いと報告されています。(Bonner)

当然、この新しい要件は、IT とセキュリティの両チームに新たな困難をもたらしますが、ここでは統合エンドポイント管理ソリューションが役立ちます。

つまるところ、企業がリモートワークをまったく考慮せずにオフィス勤務のみの作業環境を考えている、あるいはその目標に向かって努力したいと考えているとしても、IT やセキュリティチームは 100% オフィス勤務とセキュリティの設定では不十分であることを知っています。このガイドで示すように、オフィス勤務ルールの「例外」を考慮する必要があります。

ハイブリッド環境やリモート環境で働く従業員の特長:

オフィス勤務ルールのハイブリッドとリモートの「例外」

企業は完全に「オフィス勤務」が前提であると考えている。そのためパンデミック以前に普及していた従来のエンドポイント管理およびセキュリティソリューションのみが必要ですが、実際には100% オンプレミスで動作します。

もちろん、そうではありません。

IT チームとセキュリティチームは、標準的な手順に対するあらゆるエッジケースを考慮しなければなりません。そのため、ハイブリッドなテクノロジー管理とセキュリティ戦略は、セキュリティと管理が必要な作業環境はオフィス内だけという経営陣の思い込みに従うよりも、より強固になります。

たとえば、ハイブリッド IT 管理やセキュリティ戦略は、オフィス勤務のみのソリューションに対する次のような「例外」に対応します。

- **医療従事者**が週末に待機しており、呼び出しに対応するために患者ファイルにアクセスする必要がある。
- **教師**が自宅で採点したり、時間外に保護者のメールに対応したりする。
- **財務アドバイザー**は安全なサーバー上の電子メールにしかアクセスできないはずなのに、個人のデバイスにその電子メールにアクセスできるアプリをインストールした可能性がある。
- **親**が病気の子供を看病しながら在宅勤務をしようとする。
- **政府職員**が会議に出席したり、インシデント対応で出張したりするが、それでも自宅から政府機関のネットワークにアクセスする必要がある。
- **経営陣**は年功序列による都合の良い免除を求める。

CISO が従業員にリモートワークを許可したことにより、会社が受けたサイバー攻撃が増えたと回答

ivanti

たとえ職場が「オフィス回帰」したと言われても、こうしたエンドユーザーやそのような人々は、Bluetooth が接続できるあらゆるネットワーク経由で、モバイルデバイスから業務データやアプリケーションにリモートアクセスすることを期待するでしょう。

したがって、IT チームとセキュリティチームは、従業員がデバイスやネットワークを効果的に使いこなし、オフィス内外で成功できるような戦略を採用しなければなりません。 つまり、あらゆる場所で、あらゆるネットワーク上の、すべてのエンドポイントとそのエンドユーザーを、すべての組織データに対して保護することを意味します。

しかし、正式なオフィス勤務回帰の状況にかかわらず、事実上のハイブリッド職場環境において、エンドポイントを管理および保護するという新しい要件は、企業が数年前に採用した混乱の中でのパンデミック対策と同様のデバイス管理戦略に頼らざるを得ないというわけではありません。

そのような緊急避難的な解決策は、一時期は有効でした。しかし、長期的なエンドポイント管理、最新のリスクや脆弱性に対する保護では不十分であり、真の統合エンドポイント管理ソリューションを求める組織のニーズが高まっています。

実際に、CISO の 58% は、リモートワークへの移行により、会社が受けたサイバー攻撃が増えたと回答しています。 (Proofpoint)

02

統合エンドポイント管理とは?

統合エンドポイント管理 （UEM） は、IT チームとセキュリティチームが、単一のプラットフォームまたはダッシュボードから、デバイス、ハードウェア、その他のテクノロジーといった複数のエンドポイントを検出、管理、保護することを可能にするテクノロジーです。さまざまなメーカーや開発者の幅広いオペレーティングシステム （OS） とデバイスタイプに対応します。

UEM は、エンドポイント管理ソリューションから進化した最新の形態であり、その中核は、最初のモバイルデバイス管理（MDM）から発展しています。

- モバイルデバイス管理 （MDM） は、現在では「モダンな」デバイス管理と呼ばれることも多いのですが、増え続けるデバイスの管理、実施、セキュリティのジレンマに対処するために、テクノロジー業界が最初に取り組んだものでした。 これらのソリューションにより、IT 部門は MDM APIをサポートするスマートフォン、タブレット、その他のエンドポイントでポリシー、構成、ソフトウェアを制御、保護、強制することができますが、多くの場合は特定のオペレーティングシステムを実行するデバイスに限定されていました。

- エンタープライズモバイル管理 （EMM） は、MDM のテクノロジーを取り入れ、モバイルアプリ管理 （MAM）、モバイルコンテンツ管理 （MCM）、モバイル情報管理 （MIM） などのソフトウェアアプリケーション管理ソリューションと融合させ、デバイス上のソフトウェアのライフサイクル、特定のアプリのデータ、企業データへのアクセスを管理します。

しかし、従来のパーソナルコンピューター、サーバー、その他の主要な企業エンドポイントに加え、IoT デバイス、特殊な作業現場で使用される「耐久性の高い」特殊な機器を含む、現代の組織環境で増加しているエッジユースケースの多くを考慮すると、混在型エンドポイント管理アプローチはまだ十分に堅牢ではありませんでした。

大企業の IT チーム は、macOS、Windows、iOS、Android だけでなく、ChromeOS、Linux、その他の特殊なデバイスや IoT 対応デバイスなど、複数の OS を管理するパッチワークシステムの中にいることに気付きました。

各 OS ベンダーはネイティブ MDM によるコマンドや構成をサポートしていますが、MDM API に含まれていない重要なタスクがいくつか存在します。

- デバイスの状況 （Jailbreak（脱獄、ルート検出））
- 場所
- 通知
- モバイル脅威対策

そして、モバイルと従来のエンドポイント管理の両方において、複数の OS やデバイスタイプにまたがって拡張しながら、追加の機能とアプリケーション制御を提供するという組織のニーズから、統合エンドポイント管理というテクノロジーが生まれました。

03

最新のUEMソリューションの4つの利点

このセクションでは、次の点について説明します。

1. UEMが技術スタックを統合する方法
2. UEMで自動的に把握していない資産を検出する方法
3. UEMでユーザーのコンプライアンスを高める方法
4. UEMで従業員のデジタル体験 （DEX）を改善する方法

ivanti

UEMの違い

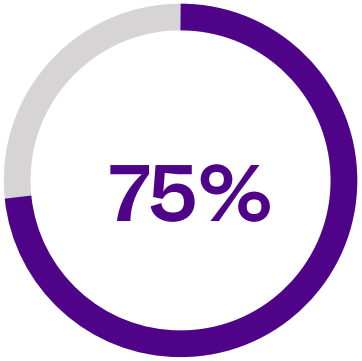
現在、ほとんどの組織では、所有および管理する大量のデバイスを管理するために、すでに少なくとも 1 つのソリューションを導入しています。

2022 年に行われた IT 担当者を対象としたある調査では、回答者の 80% がすでに単一のエンドポイント管理チームに統合しているか、今後 2 年以内に統合する計画であることがわかりました。 また、75% の回答者が何らかの BYOD（Bring Your Own Device）テクノロジーに投資しています。 （Cipolla, Wilson and Silva）

UEM ソリューションは、デバイスレベルのサイロに存在するのではなく、最新の AIと 機械学習 （ML） 機能をより有効に活用することができます。これらのツールは、別のツールから得られるサイロ化した情報ストリームに依存するのではなく、組織全体の同じ基本情報セットを活用して結論を導き出すことができるからです。

最新のUEMソリューションの利点は次のとおりです。

1. 「一元的な管理」のダッシュボードやポータル。IT チームやセキュリティチーム向けに、複数のニッチな製品ではなく、1 つの統合ソリューションを提供
2. 動的な自動資産検出による、把握していないデバイスやいわゆる「シャドー IT」の自動識別および修正。オンプレミスとクラウドの両方に対応
3. 統合デバイス登録および実行による、すべての IT およびセキュリティポリシーへのエンドユーザーの準拠度の向上
4. 自動的かつプロアクティなデバイスの問題の修正による、従業員のデジタル体験 （DEX） を改善し、IT チームのシフトレフトを支援



IT 担当者が自分の組織が BYOD の実現に投資していると回答

1 「一元管理」アプローチは負荷の高い技術スタックを統合します。

経済の不確実性が高まる中、世界中で、投資家や経営陣から、組織は資源投資を減らしながら戦略的成果を最適化し、すべてのツール、従業員、タイムラインから最大限の価値を引き出して、効率を最大化するように求められています。

この義務の一環として、IT チームやセキュリティチームが確実にサポートできる以上の人員と専門知識を必要とするポイントソリューションを求めるのではなく、より汎用的な統合された技術ソリューションを購入する方向に舵を切る組織がますます増えています。

技術スタックの統合に向けたこの戦略的な転換は、特に組織が世界的な燃え尽き症候群と技術労働力の傾向を考慮するとき、理にかなっています。

- 2019 年のグローバル調査で、情報サービス従業員の回答者の 64.4% が燃え尽き症候群だと回答しており、これはあらゆる業界の中で最も高い割合の 1 つです。 また、一般的な「技術」分野の従業員も、60% の回答率で、高いレベルの燃え尽き症候群だと回答しています。（Paychex）
- 調査対象のインシデント対応者の 68% は、通常、一度に 2 件以上のインシデントを担当し、1 件のインシデント解決に平均 2 ～ 4 週間を要すると答えています。また、同じインシデント対応者の 64% は、燃え尽き症候群や不安を治療するために医療支援を要請しています。（Morning Consult and IBM）
- 2022 年に実施されたセキュリティ専門家を対象とした世界規模の調査によると、世界中の組織において、サイバーセキュリティの卓越性を阻む最大の障壁は「技術スタックの複雑さ」で、次いで現在のセキュリティ人材の「セキュリティスキルギャップ」であることが判明しました。（Ivanti）

あるCISOはウォール・ストリート・ジャーナルにこう語っています：

「もし、優れていないとしても、5 つ 6 つのことをかなりうまくこなせる 1 つのソリューションを手に入れなければならないのなら、そのようなソリューションを選びます。 管理も容易で、予算的にも安く、得した気分です。」

Adam Glick 氏
SimpliSafe, Inc. CISO (Rundle)

各デバイス、アプリケーション、インシデントがバラバラのソリューションに現れるのを管理するのに必要なスキルを持った人材が、従業員や転職市場に少なすぎるのです。

最新の UEM プラットフォームは、適切に構成、実装されることで、IT チームとセキュリティチームの両方が、組織全体のエンドポイント環境を最も詳細に一元的に管理し、次の項目に関するレポートを動的に作成することができます。

- 部署レベルとユーザーレベルのデバイスの使用と管理
- 個別のユーザーのアクセスとアクティビティ：全体的な生産性と潜在的なセキュリティの課題を評価
- 現在インストールされているパッチとユースケースを含む、エンドポイントのセキュリティの状態
- 運用に対するデバイスの全体的なコスト：過去のメンテナンスコストとライセンスコストが原因

これらの各ポイントは、デバイスタイプや OS に応じたポイントソリューションで説明することができ、最も最適化された運用のためにさらに細かなレベルまで詳細に説明することができます。

しかし、最新の UEM ソリューションだけが、これらの関連しながらも異なるニーズを、負荷がかかりすぎている IT チームやセキュリティチームが個人のワークフローの中で活用できるよう、単一の管理しやすいダッシュボードに本当に統合することができます。

2 自動化された資産検出により、最小限の工数で隠れたコストを発見することができます。

エンドポイントを管理するために複数のテクノロジーソリューションを使用すると全体的な経費が増加するのと同様に、資産の検出が不十分だと、組織の管理負荷とコストが増加することになります。このようなコストは、情報漏洩の発生場所にかかわらず、最終的に IT チームが負担することになるコストです。

IT チームは、一般的ににシャドー IT と呼ばれる、特定されていない（つまり管理されていない）ハードウェアやソフトウェアの危険性について、ますます認識するようになっています。

- IT 担当者の 36% が、IT インフラストラクチャを最新化するための重要な課題として、シャドー IT の懸念を挙げています。（Insight Enterprises & CIO）
- シャドー IT は、調査対象となった CIO が、ランサムウェア攻撃やサプライチェーン攻撃に次いで、政府の継続性に関する懸念事項として挙げた上位の項目の 1 つです。（NASCIO）
- 調査対象の IT 意思決定者の 41% が、「分散」されたシャドー IT は、近い将来、グローバル組織に影響を与える最大のレンドの 1 つであると回答しています。（Vanson Bourne for Nutanix）

なぜシャドー IT に関する懸案事項が IT 部門の最重要課題として浮上してきたのでしょうか。ハイブリッドな職場や BYODポリシーの進展により、エンドユーザーが使用するデバイスやアプリケーションは増えていますが、必ずしも IT 部門が直接所有、管理するものではありません。

IT 意思決定者を対象としたある調査（Bitwarden）によると、エンドユーザーがシャドー IT を利用している理由は次のとおりです。

1. 組織から提供されたリソースではなく、自分で選んだシャドー IT の選択肢を使うことで、日々の業務がより速く、より簡単になる（63%）
2. 職務上必要と思われるデバイスやアプリを使用するための正しい社内承認がない（48%）
3. IT 部門は、アプリやデバイスへのアクセスに関するリクエストに答えるのが遅すぎる、あるいは複雑すぎて対応できない（38%）

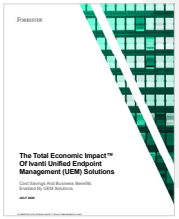
実影響

UEMを使用したテクノロジー・ライセンス統合によって実現される節約

Forrester Consulting が Ivanti の委託を受けて実施した Total Economic Impact™ 調査によると、10,000 のエンドポイントを管理し、毎年 5% の成長を続ける複合企業体の組織は、Ivanti Neurons for UEM の導入により 3 年間で 261% の ROI を達成しました。

複合企業における TEI 調査の推定効果の 36% は、個々のエンドポイント管理ソリューションの廃止と、未使用のアプリケーションのソフトウェアライセンス支出の削減によるものです。（Forrester Consulting TEI 調査）

詳細については、Ivanti Unified Endpoint Management（UEM）ソリューションの Total Economic Impact™ をお読みください。



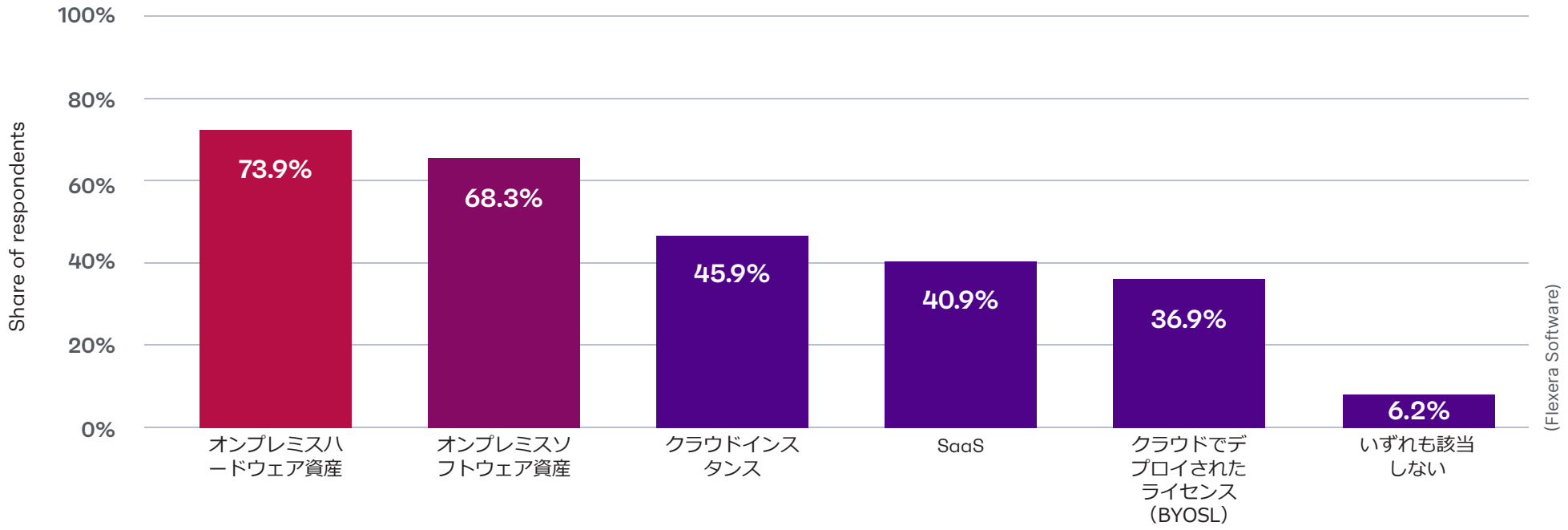
シャドー IT の問題にさらに火をつけるなら、IT 部門は、リモートやクラウドベースの資産よりも、従来のオンプレミスの展開の資産の可視性の方がより効果的に対応することができます。（Flexera Software）

これらの世界的な調査や研究は、Ivanti がクライアントや顧客から聞いた話と相関しており、積極的な資産検出機能を備えた UEM ソリューションの導入後、組織のネットワークにアクセスする不明なデバイスが 25～30% 特定される傾向にあります。

一元管理された UEM プラットフォームで実行される自動資産検出により、IT 部門は以下のことが可能になります。

- すべてのデバイスが組織のインフラストラクチャやネットワークに接続する際に、それらを検出
- 一過性のデバイスが修復やセグメンテーションなしにオンラインになるリスクを低減
- エージェントなしでデバイスをリモートでスキャン
- BYOD ポリシーの柔軟性を保ちながら、有害な不明なデバイスをセグメント化して隔離

Q: 以下の環境について、正確に可視化できていると感じていますか。



3 デバイスの自動登録により、オンボーディングとエンドユーザーのコンプライアンスを迅速化します。

事実上のハイブリッドワーク戦略の一環として、新入社員の最初のオンボーディングを考慮します。オフィスに出社しないかもしれないエンドユーザーの新しいデバイスに適切なソフトウェアとアクセス許可をプロビジョニングする必要があります。

UEM ソリューションでは、ユーザーとデバイスのプロファイルがあらかじめ設定されているため、IT 部門が関与しなくても、採用担当者がセルフサービスポータルにアクセスして必要事項や許可を申請するのと同じように簡単に導入することができます。

エンドポイント登録の自動化により、IT 担当者の通常業務や従業員の通常のワークフローを妨げることなく、新しいデバイスやユーザープロファイルを登録することができます。

また、プライマリ UEM ソリューションから自動的に適用されるポリシーとデバイス構成は、普遍的なポリシーコンプライアンスを保証します。

最後に、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、ユーザーの操作や許可は必要ありません。

実世界への影響

ソフトウェアのインストールと構成にかかる時間は、最大 2 ～ 3 日から 5 ～ 10 分に短縮

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。 （Forrester Consulting TEI 調査）

しかし、Ivanti Neurons for UEM を導入した後、インタビューに応じた人は次のように述べています。「デバイスがイメージ化された後は、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。」（Forrester Consulting TEI 調査）

FORRESTER®

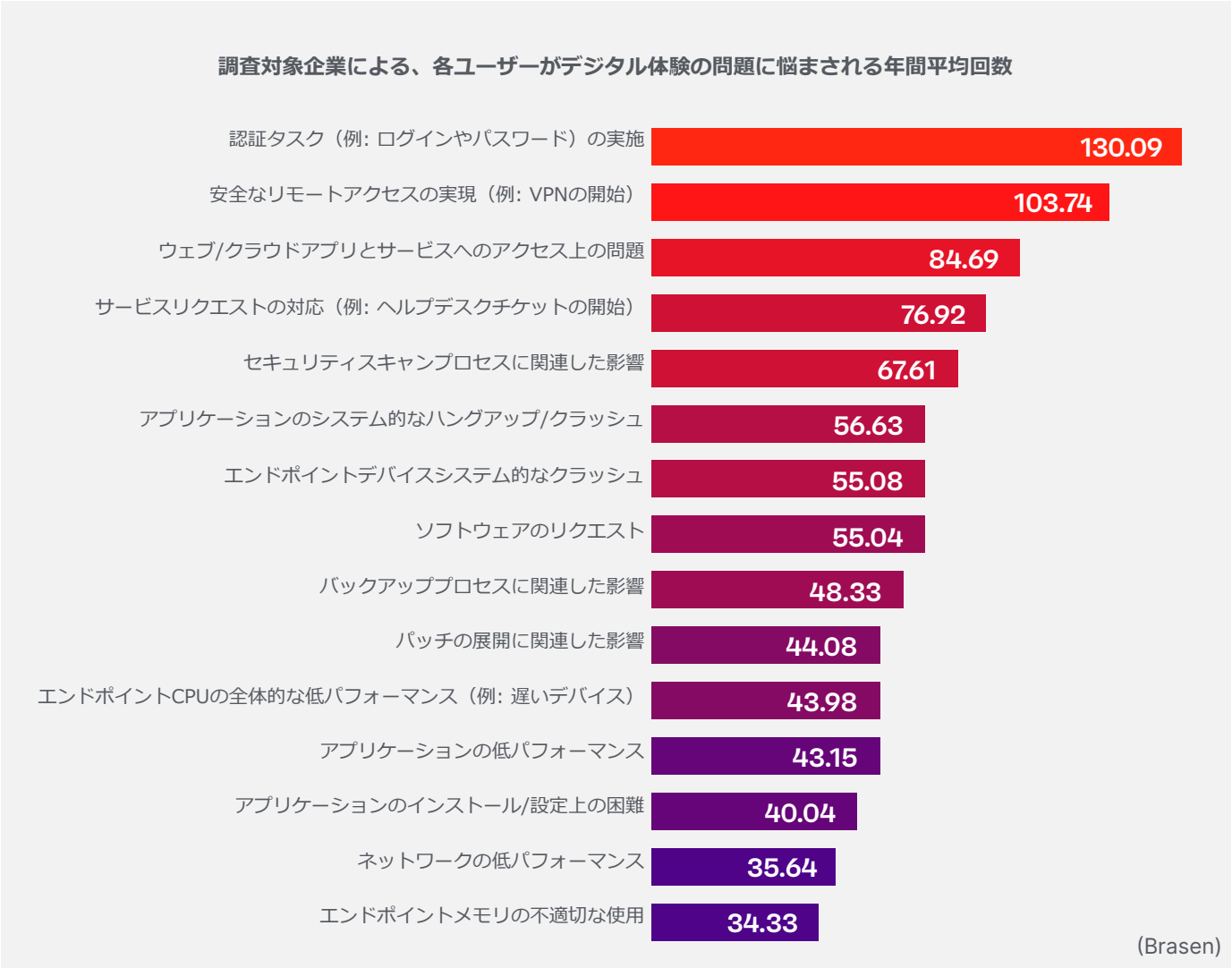
4 エンドユーザーは、デジタル体験の改善と生産性が向上したと報告しています。

従業員のデジタル体験 （DEX） が重要であるという、たった 1 つのシンプルな事実に、IT チームおよびセキュリティチームの全員が同意するでしょう。

この直感的ともいえる事実を裏付けるのが、最近の DEX の調査成果です。

- 調査対象の従業員の 26%、IT およびセキュリティ担当者の 31% が、少なくとも部分的にはテクノロジーに関するストレスを理由に退職を考えたことがあります。（Ivanti）
- 平均的な従業員は、年間 919 件のエンドポイント管理に関する課題の影響を受けており、これは 1 営業日に約 4 件の課題を抱えていることになります。 （Brasen）
- エンドポイント管理の不備やテクノロジー面の問題によって発生した中断を解決するために、ユーザーは 1 回につき 20 分もの時間を要しています。（Brasen）

実際、DEX は非常に重要であり、Gartner のアナリストは、50% の IT 組織が DEX 戦略、チーム、それに伴う管理を 2025 年までに確立すると予測しています。2022 年のわずか 15% からの大きな上昇です。（Wilson, Cipolla and Paulman）



もちろん、適切な DEX 戦略を実行することは、ほとんどすべての状況において困難なことです。 調査対象の経営陣のうち、来年、従業員体験の向上のための予算を積極的に割り当てようと考えているのはわずか 20% に過ぎないため、その実現は極めて困難です。 （Ivanti）

しかし、UEM ソリューションによって、IT チームはデバイスとユーザーの活動をすばやく把握することができ、一目で問題を評価したり、堅牢な分析に深く入り込んでユーザーの不満の根本原因を特定し、迅速な解決を図ったりすることができるようになります。

最新の UEM ソリューションは、カスタマイズされたデバイスやユーザーの動作に関するアラート、あらかじめプログラムされたサービスレベル契約やプレイブックを備えており、こうしたエンドポイント管理の問題の多くを自動的に検出し、プロアクティブに修正することも可能です。

このように、適切に構成された堅牢な UEM ソリューションは、堅牢な DEX 戦略の最も基本的かつ重要な要素の 1 つであり、ユーザーがサポートチケットを登録する前にデバイスの問題を解決することで、IT チームがサービス管理を「シフトレフト」できるようになります。

たとえ、DEX への投資の重要性についてはまだ経営陣が理解する必要があるとしても、IT チームおよびセキュリティチームは、UEM ソリューションなどのプロアクティブなテクノロジープラットフォームを通じて、組織の貴重な時間とコストを節約することができます。

従業員体験の改善に具体的な予算を割り当てる予定の経営者は、わずか 20%

ivanti

04

UEMソリューションを活用した4つのエンドポイントセキュリティ事例

このセクションでは、UEM ソリューションがセキュリティチームをどのように支援するかについて説明します。

1. 優れたセキュリティ行動を奨励する
2. 成長するハイブリッドワーク環境をセキュアにする
3. ポリシーを自動的に施行する
4. パッチ適用やモバイル脅威対策ソリューションと統合する

ivanti

UEMユーザーがエンドポイントセキュリティも考慮しなければならない理由

このガイドでは、IT とセキュリティの両チームについて頻繁に言及していますが、それは偶然ではありません。

サードパーティのアナリストは、パンデミック後の Everywhere Work （場所にとらわれない働き方）がオンプレミスのオフィスだけでなく、リモートやハイブリッドのアプローチを許容することを考慮すると、UEM ソリューションは、現代の脅威要因に対する「プロアクティブかつレジリエントな防御」のためのエンドポイントセキュリティのユースケースを取り入れるように変化すると考えています。 （Cipolla, Wilson and Silva）

エンドポイントセキュリティが、クラウドセキュリティツールと社内ユーザートレーニングに次いで、世界中の企業にとってサイバーセキュリティ投資の最優先事項であり続けていることは、驚くべきことではありません。 （PwC）

（そして、提案された UEM ソリューションがクラウドアプリのセキュリティ確保に役立つのであれば、それは関係者全員にとって大きな利点です。）

UEM ソリューションは、IT とセキュリティの両チームが同じベースライン情報 （組織のデバイス、ユーザープロファイル、ネットワークアクティビティ）をもとに、すべてのエンドポイントを適切に管理、保護、サービス提供できるようにするための独自の出発点となります。

1. DEX に特化した技術スタックに投資することで、エンドユーザーによる優れたセキュリティ行動を奨励できます。

2. 攻撃対象が急速に拡大する組織のセキュリティ対策は、IoT デバイスから不明なインターネット接続まで、これまで以上に多様な脅威ベクトルに対応する必要があります。

3. セキュリティポリシーの施行とユーザー、デバイス、アプリの動作の監視により、侵害されたエンドポイントから組織内ネットワークへの横の動きを防止し、被害が発生する前に初期侵入や潜在的な内部脅威を察知することができます。

4. パッチ管理やモバイル脅威対策ソリューションなどのセキュリティツールは、最新の UEM ソリューションと簡単に統合できるため、セキュリティチームは、通常のユーザーや IT 管理者の業務を妨げることなく、シンプルかつ迅速な方法で優先されたリスクを修正できます。

ただし、UEM のデバイスオンボーディングの自動化やポリシー制御は、基本的なサイバー衛生保護を提供し、デバイスとユーザーの活動ログはセキュリティチームが積極的に活用できる強固な監視機能を備えていますが、ほとんどのプラットフォームでは、エンドポイントセキュリティのための組織の信頼できる唯一の情報源として、その潜在能力を完全に発揮するために、追加の制御とツールが必要です。 （Verizon）

1 UEMにおけるセキュリティのリスクは DEX から始まります。

特に、パンデミック後のハイブリッドな職場において、シャドー IT のリスクやエンドポイントの攻撃対象が拡大し続ける中、セキュリティチームは、IT 部門以外のどの部門よりも、UEM ソリューションを含むよりプロアクティブな DEX テクノロジーへの投資を支持することでしょう。

- CIO は、シャドー IT ソリューションや製品を、世界各国の政府の継続性に対する最大の懸念事項として挙げています。 （NASCIO）
- 2022 年のクラウドベースのサイバー攻撃の 12.8% にシャドー IT が関与しています。 （Shackleford）
- 調査対象のセキュリティ専門家のうち、組織における資産の可視性が「高い」と回答したのはわずか 52% で、10% は資産検出ツールを全く使用していないと回答しています。 （Ivanti）

そして、ハッカーは、セキュリティチームが保護できると認識しているものと、ユーザーが業務をしやすくするために行っているものとの間に存在するこのようなギャップを、すでに利用しています。

12.8% **2022 年のすべてのクラウドベースのサイバー攻撃にシャドー IT が関与しています。**

現実世界への影響

DEX の不備がハッカーによる石油化学プラントの爆破の危機を招く

2017 年、サウジアラビアの石油化学工場 Triconex が脅威アクターによってハッキングされました。 セキュリティチームがシステム侵入に気付いたのは、6 台のコントローラーが誤作動を起こし、アラームが作動したときでした。

インシデント対応の担当者は、誰かが遠隔操作でシステムにアクセスし、マルウェアを仕込んだことをすぐに突き止めましたが、それは不可能と思われていました。

この工場のセキュリティシステムは、遠隔地からの攻撃を防ぐために、すべての構成変更時には工場のコンソールで従業員が物理的なキーを挿入しなければならないように設計されていました。

しかし、この工場の物理的なレイアウトでは、コントローラーと制御室が離れており、オペレーターは変更を実行するために、ある場所と別の場所を行き来する必要がありました。 ある従業員が物理的なキーをコントローラーのコンソールに忍ばせていて、その従業員、そしてハッカーが遠隔操作でコードにアクセスして更新できるようにしていたのです。

もし、他の冗長セキュリティシステムが、ハッカーの活動によって引き起こされた重大な事象を工場従業員に警告していなければ、Triconex の侵害されたコントローラーは、すべての安全システムをオフにし、化学物質の漏出や爆発によって工場従業員の死亡事故を引き起こしていた可能性があります。

このサイバー攻撃は、人命にかかわる最初のハッキングの 1 つとなった可能性があります。すべては、1 人の疲れた従業員と、セキュリティ設計者が「フールプルーフ（Foolproof）」のセキュリティシステムを構築するときに人間の行動を考慮しなかったことが原因です。 （Rhysider）

2

UEMクライアントを経由で、より多様な作業環境と IoTエンドポイントを保護します。

リモートワークというと、コーヒーショップでヘッドホンをつけて仕事をしている従業員を思い浮かべます。もし周りの人に気づかず、ノートパソコンをロックしないでトイレに行った場合、悪用されたりする危険性があります。

人為的なミスは常に残るものですが、ITチームのUEMプラットフォームによって実施されるエンドポイントセキュリティソリューションとポリシーは、地理的に多様化する職場がもたらすリスクの一部を軽減するのに役立ちます。

ここでは、エンドポイントセキュリティの代表的なリスクとして、IoT （モノのインターネット） の普及とパブリックネットワーク環境における中間者攻撃の 2 つについて説明します。

（ネタバレ: いずれのシナリオも、適切な資産の検出、ネットワークのセグメンテーション、デバイスの改善によって改善することができます。これらのすべては、セキュリティに焦点を当てた適切な構成とサポート機能を備えた UEM ソリューションによって実行することができます。）

実世界への影響

想定外のモノのインターネット（IoT）攻撃

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。 （IBM Security）

しかし、調査対象となった IT 担当者の 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。（SAM）

企業やリモートの職場にある IoT 対応デバイスは、比較的簡単なネットワークの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修正することができます。

しかし、このようなデバイスの多くは、組織やエンドユーザーにとって、手遅れになるまでリスク分析で考慮する必要がないものであることが、これらの組織で明らかになりました。

水槽用温度計

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 IoT 対応の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。 （Wei）

医療機器

2017年に発生したランサムウェア攻撃「WannaCry」をきっかけに、メーカーや政府機関は、インスリンポンプやペースメーカーなど、インターネットに接続された医療機器の脆弱性を再考するようになりました。 （Chase, Coley and Connolly）

車両

2015 年: ハッカーが Jeep Cherokee をハイジャックし、高速道路での走行中にエンジンを停止させました。 （Greenburg）

2023 年: テスラのドライバーが、テスラの公式モバイルアプリで、所有していない車両に乗り込み、運転できることを発見しました。 （Day）

2023 年以降: 政府関係者は、電気自動車やその充電器 （SANDIA）、つまり組織の従業員がオフィスへ運転しながらリモートミーティングのために、社内デバイスを Bluetooth 接続する車について、「現在、包括的な [...] サイバーセキュリティのアプローチは存在しない」と警告しています。

実世界への影響

Equifax の （ほぼ） 中間者ハッキング

モバイルデバイスやエンドポイントに対する最も一般的な攻撃のひとつに、中間者攻撃（MitM） があります。 従業員が安全でないネットワークやインターネット接続で機密情報に接続すると、ハッカーはデータの流れの真ん中に身を置き、あらゆる機密情報を「傍受」することができます。

米国の消費者信用調査会社である Equifax が、2017 年に Apple と Google の両方からアプリを削除したのは、MitM 攻撃の可能性があったからです。

同社は、不名誉にも、既知の悪用された脆弱性（Khandelwal） にパッチを適用しなかったことが原因で、約 1 億 4,300 万人の顧客の個人情報を数か月にわたってネットワークに潜むハッカーにさらしました。その後、セキュリティ研究者の Jerry Decime 氏は、この情報漏洩事件後、Equifax は組織全体でセキュリティを強化したのかと疑問を抱きました。

Decime 氏は、Equifax ソフトウェアのモバイルアプリ版を調べました。そして、驚いたことに、アプリがさまざまな重要な分野で初期認証後に HTTPS プロトコルを使用し続けていないことを発見しました。 （Decime）

より機密性の高い個人情報や金融取引情報を含む、ユーザーのデバイスと Equifax サーバーの間で認証後に送信されるあらゆる情報が そのセキュリティが表面的なものであることに気付いた賢いハッカーによって傍受され、流出した可能性があります。

Equifax は、Decime 氏からの連絡に 1 時間以内に対応し、Apple と Google の両方のアプリマーケットプレイスから安全でないアプリを削除しました。 （Weissman）

しかし、この MitM （ほぼ） 攻撃の典型的な例は、ユーザーと企業のサーバー、あるいは従業員と組織の機密情報やネットワークとの間の安全な通信の重要性を強調しています。

UEM ソリューションとパートナーのセキュリティツールは、このような種類の攻撃に対するリスクをプロアクティブに制限できます。

- 堅牢なユーザーアクセスプロファイル
- 資格情報の自動デプロビジョニング
- VPN やゼロトラスト制御など、安全なデータアクセスや通信経路も、UEM ソリューションで展開および監視

3

セキュリティポリシーの施行とデバイスレコードにより、ハッカーが組織のネットワークに侵入する足がかりを獲得することを防ぐ

プロアクティブなサイバーセキュリティ戦略は、ハッカーによる組織ネットワークへの侵入を阻止しようとするだけでなく、悪意のある主体が侵入した場合のことも考慮しています。

USB メモリを例にとります。 営業担当者の必須アイテムです。プレゼンテーションや動画、音楽などの大容量ファイルを保存し、ネットワーク接続を待たずに新しいパソコンでアップロードやダウンロードを行うことができます。

当然、USB メモリが合法的な目的で大容量ファイルを持ち運べるのであれば、マルウェアも持ち運ぶことができます。

UEM ソリューションは、デフォルトでリムーバブルメディアポリシーを自動的に展開し、実施することができます。 このようなポリシーにより、組織のエンドユーザーは、すべてのデバイスとエンドポイントを自動的にこれらの攻撃にさらすのではなく、会社所有のコンピューターでメモリを持ち運ぶデバイスを使用する特別な許可を要求する必要があります。

実世界への影響

Stuxnet: 世界で最も有名なUSBメモリ感染型マルウェア

Stuxnet は、イランの核濃縮プログラムを停止させるために、特定の情報機関によって開発されたとされるコンピューターウイルスの名称です。

この施設は、インターネットや外部のネットワークにアクセスできないエアギャップという厳重なセキュリティのもとで運営されていました。 マルウェアが施設内に侵入する唯一の方法は、すでに信頼されている内部関係者が、施設内のネットワーク上のコンピューターにマルウェアを個人的に接続することでした。

そこで、攻撃者はイランの施設が遠心分離機に使用している産業用制御システムだけを攻撃するコンピューターウイルスを作り、マルウェアパッケージ全体をUSBメモリに格納しました。

汚染されたメモリは、もしかすると会議で、またはその地域の信頼できる従業員の手によって、核科学者たちに届くように地域全体に配布されました。

結局、ある科学者が致命的なミスを犯し、Stuxnet マルウェアが混入した USBメモリを接続してしまったのです。そして、このプログラムは推定 1,000 台の遠心分離機と廃棄物を失い、イラン指導部に圧力をかけて 2015 年のイラン核合意への調印を後押ししました。

Stuxnet の詳細については、以下の資料をご覧ください。

- “Ep 29: Stuxnet” by Jack Rhysider
- “Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon” by Kim Zetter

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、セキュリティの観点からも活用することができます。

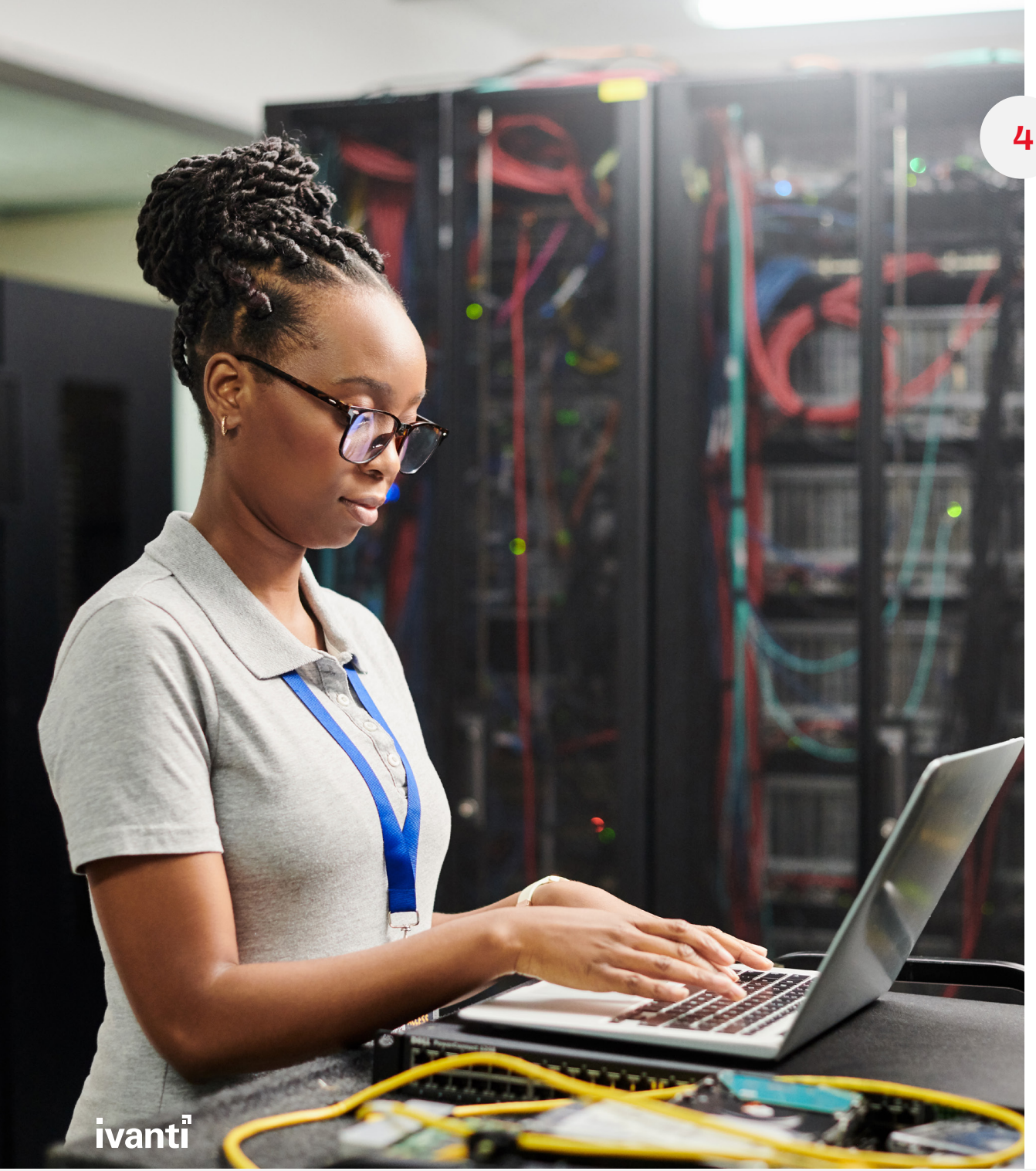
従業員が内部脅威となる可能性があると考えられる場合、セキュリティチームは、PowerShell などのシステム管理者ツールがユーザーのデバイスに不正にインストールされ、使用された形跡がないかどうか、デバイスのレコードを確認できます。

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、より厳格なリムーバブルメディア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、プロアクティブなリスク修正と保険料の低減を図ることが非常に経済的であると考えるかもしれません。 （Breg）



4

容易な統合化は、シンプルに一度で完了するセキュリティ実装を提供します。

統合された UEM プラットフォームは、基本的なサイバー衛生の機会を提供しますが、エンドポイントセキュリティソリューションの絶対的な解決策にはなりません。

しかし、UEM ソリューションは、パッチ管理やモバイル脅威対策ソリューションなどの他のツールが効果的に機能できるようにサポートするという点で非常に優れています。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 DEX や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。

UEM + リスクベースのパッチ管理

たとえば、UEM をリスクベースのパッチ管理ソリューションや脆弱性管理ソリューションと組み合わせることで、現在の環境で活発に悪用された脆弱性を修正するためのシームレスかつプロアクティブなリスク対応を実現できます。

1 セキュリティチームは、最新の脅威情報データを分析し、組織で現在使用されているデバイスやアプリケーションに対して、現在悪用されている脆弱性を実行します。

- UEM のアクティブスキャン機能により、この初期評価で見落とされるデバイスやアプリケーションはありません。

2 セキュリティチームは、組織のリスク環境と優先度に応じて、現在パッチが適用されていない脆弱性の優先度を下げたり上げたりします。また、次の点を考慮する場合があります。

- 影響を受ける可能性のあるデバイス、ユーザー、OS、および組織の重要な機能の優先度
- 脆弱性が拡散している既知の脅威アクターによって活発に悪用されているかどうか
- エクスプロイトが脅威アクターに与える可能性のあるアクセスや権限の種類
- 影響を受ける可能性のあるデバイスやアプリケーションが、受動的または能動的に組織で使用される頻度
- パッチの適用がどの程度難しいか、または他の （修正、隔離、セグメンテーションなど） が必要であるかどうか

3 ITチームは、優先度を設定したパッチの一覧と次の情報を受け取ります。

- 組織特有のリスク要因に基づいたこれらのパッチを導入すべき理由。これにより、IT チームは、セキュリティチームがすべての考えられる脆弱性にパッチを適用するように求めているわけではないと安心できます。
- 特定のデバイスやユーザーを対象に、あらかじめ決められた周期でパッチを展開する
- 確認済みの現在のソフトウェアスイートやワークフローと干渉する可能性

4 IT チームは、UEM プラットフォームを通じて、特定されたデバイスやエンドポイントにパッチを自動的に展開し、エンドユーザーの生産性への影響を最小限に抑えるように更新をスケジュールし、パッチが通常のワークフローに支障をきたすことを示す奇妙な振る舞いに目を光らせています。

リスクベースのパッチおよび修正戦略の詳細については、リスクベースのパッチ管理におけるガイドブックをご参照ください。

UEM + モバイル脅威対策

プロであっても、誰もがフィッシングに遭う可能性があります。

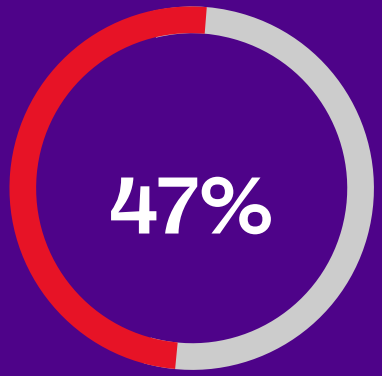
フィッシングキャンペーンは、特にランサムウェア犯罪者集団にとっては入口として知られており、2020 年の時点でランサムウェアの配信方法の 54% を占めています。 （Datto）

ハッカーが大企業の経営幹部をターゲットに特別に開発した電子メールキャンペーンである「ホエール」フィッシング攻撃により、米国企業は 2021 年に推定 24 億米ドルの損失を被りました。 （Verizon）

新しい研究では次の点が明らかになりました。

- IT 担当者の 47% がフィッシング攻撃に引っかかったことを認めています。 （Ivanti）
- 他の業界レポートでは、2021 年に 83% の組織がフィッシング攻撃の成功を経験している （Verizon） にもかかわらず、セキュリティ専門家のうち、過去 24 か月間に自分の組織がフィッシング攻撃を経験したと回答したのはわずか 43% （Ivanti） です。
- 経営陣の 3 分の 1 以上がフィッシングのリンクをクリックした経験があり、これは他の従業員の 4 倍の割合になります。 （Ivanti）

セキュリティチームが考えるフィッシング攻撃の数と、実際に発生したフィッシング攻撃の数には、40 ポイントの開きがあります。



IT担当者がフィッシング攻撃の被害に遭ったことがあります。

もし、

- IT担当者がフィッシングメールに騙される
- セキュリティ担当者が自分の組織がフィッシング攻撃を受けていることに気付いていない
- 経営幹部が高い確率で標的にされ、高い確率でその攻撃に巻き込まれている

... といった場合は、フィッシングキャンペーンによって組織のセキュリティを脅かすユーザーを阻止するには、セキュリティトレーニングや組織の受信トレイの迷惑メールフィルターだけでは十分ではありません。

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。

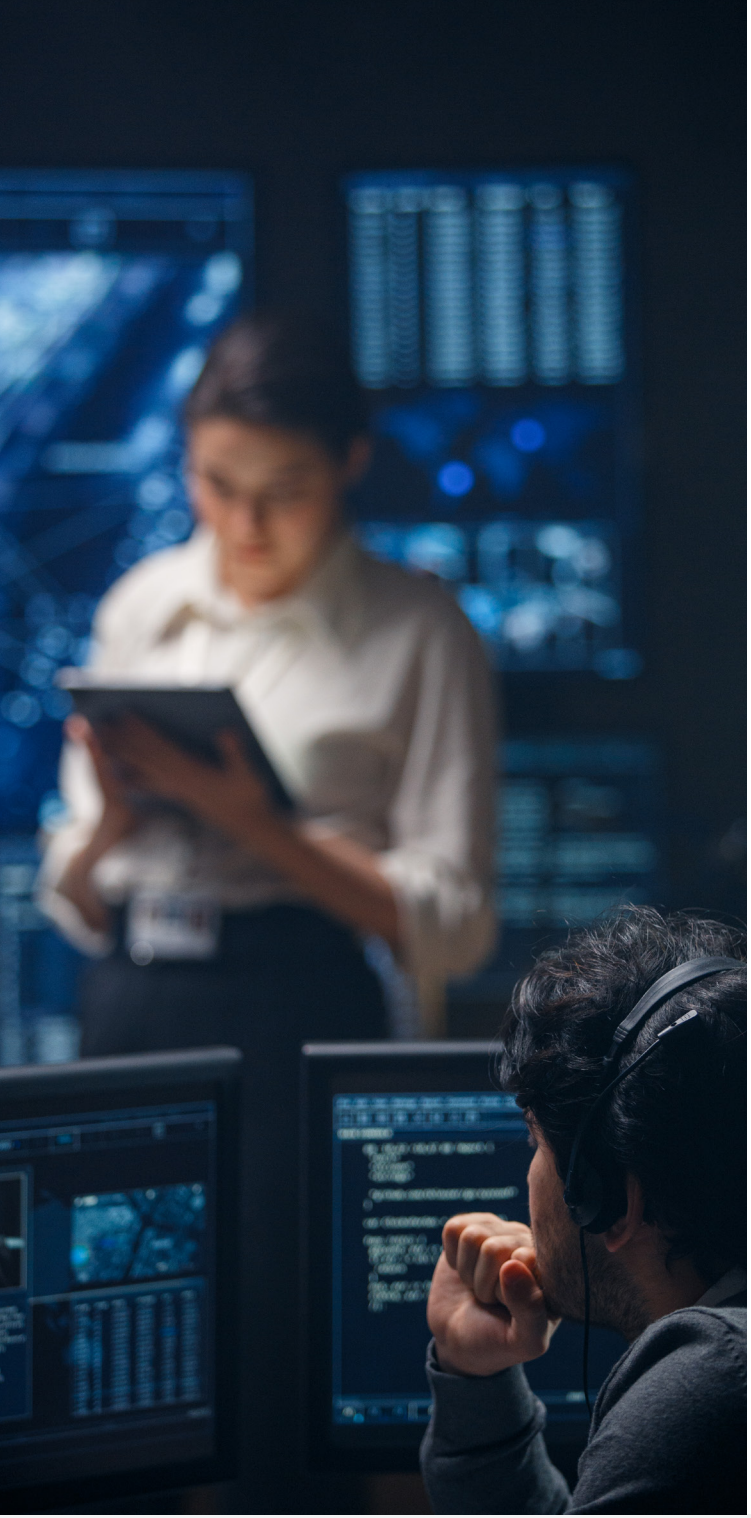
最高のMTDソリューションは、登録されたデバイスのUEMクライアント（企業が所有するもの、または BYOD プログラムの一部） を通じて実行することができ、通常のユーザー活動を妨げたり、追加のメモリを消費したりすることはありません。

MTD ソリューションが次の問題を検出した場合:

- **フィッシングリンクの受信:** システムはただちにその動きをブロックし、ユーザーによるアクションが完了しないことを確認します。
- **潜在的に悪意のあるアクティビティ:** MTD および UEM ソリューションは、特定のアクティビティと潜在的な脅威レベルに応じて、さまざまなレベルの修正を自動的に実行します。 （個人所有のデバイスであっても、ユーザーがアプリを削除するなどして問題を解決するまで、組織のあらゆるアプリケーションへのユーザーアクセスを削除するという修正まで含まれます）
- **インストールされていない OS 更新:** システムは丁寧にプッシュ通知を送信し、ユーザーに更新のインストールを促します。 ユーザーがデバイスを更新しない場合は、組織のアプリや古いデバイスからのアクセスを隔離するなど、修正のレベルも高まっています。

04

UEMソリューションを選定する方法



世の中には、強力なUEMソリューションが数多く存在します。 本ガイドに記載されている基本的な機能を提供するベンダーがほとんどですが、各ベンダーは独自の機能を提供しています。

では、どのようにして組織に合った UEMプロバイダーを選ぶべきでしょうか。 現在の状況に対応することが必要ですが、それだけではなく、組織のニーズが成熟するにつれて、より優れた制御とセキュリティを導入するための新しい可能性を提供できる必要もあります。

望ましい統合エンドポイント管理ソリューションに求められる機能は次のとおりです。

- macOS、iOS、iPadOS、Windows、ChromeOS、Android、Linux など、組織が現在使用している、あるいは将来使用する可能性のあるすべてのデバイスと OS をサポートしている。
- IT とセキュリティの両チームが同じデータを使って作業できるように、デバイスとユーザーアクティビティに関する情報を提供する「一元化された」ダッシュボードを提供する
- （組織が「オフィス勤務のみ」と考えている場合でも） クラウドネイティブアプリケーションを含む、オンプレミスとクラウドの両方の展開をサポートする。
- ユーザーとデバイスの情報を集約し、明確に報告することで、ソフトウェアライセンス契約やリスクに基づくパッチ戦略など、より広範な IT 資産およびセキュリティエンドポイント戦略に役立つ。
- シンプルで自動的なデバイスの登録と展開を容易にする。
- 可能なかぎり、ユーザーの介入を求めず、ユーザーの作業を妨害しないように動作し、エンドユーザーに肯定的なテクノロジー体験を保証すると同時に、問題をプロアクティブに解決することで、IT チームが基本的なヘルプデスクのチケットへの対応ではなく戦略的なイニシアチブにシフトできるようにする。
- UEM プラットフォームは単独ですべてに対応できないため、リスクに基づくパッチ管理や脆弱性管理ソリューション、モバイル脅威防御製品など、関連するエンドポイントセキュリティツールとネイティブに統合する必要があります。それができないベンダーはすべて除外してください。
- デプロビジョニングプロトコル、オンボーディング手順、アクティビティの急増や遅延、悪意のあるアプリの脱獄動作、承認されたパッチの展開など、標準の自動化、サービスレベル契約、アラートを実装する。

実世界への影響

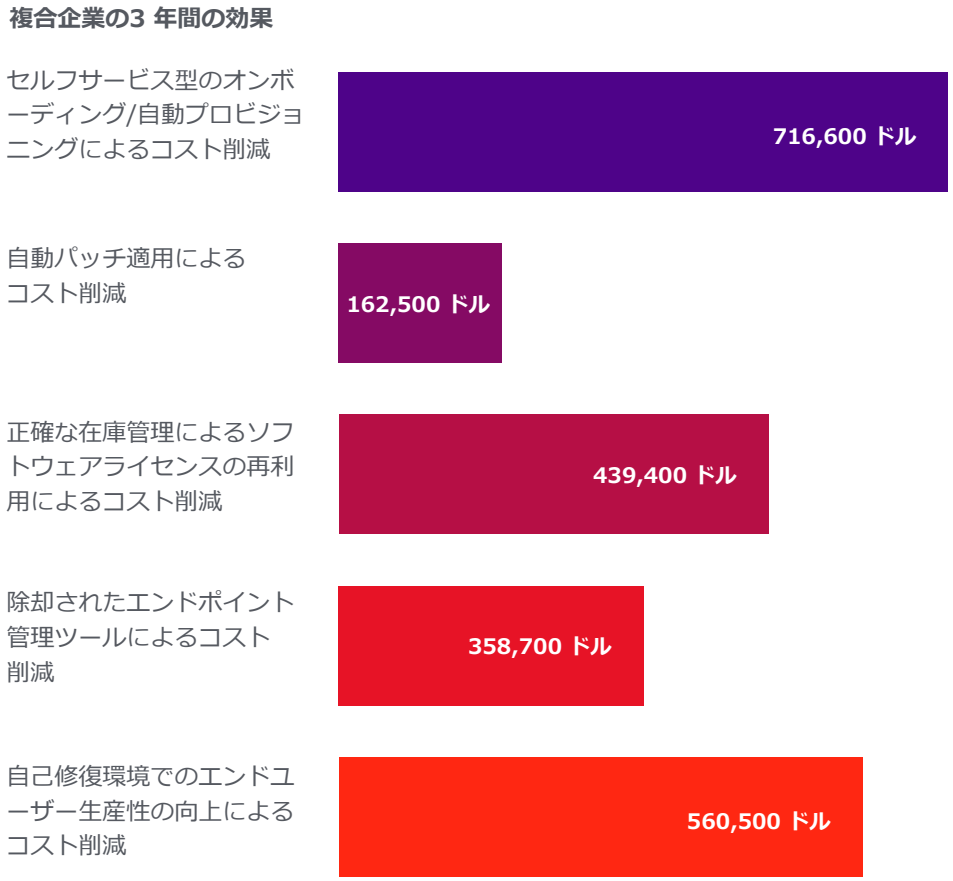
Ivanti Neurons for UEM の Total Economic Impact™ 調査

Ivanti からの委託で 2022 年 7 月に Forrester Consulting が実施した「Total Economic Impact™」調査によると、Ivanti Neurons for UEM を導入することで、10,000 台のエンドポイントを管理する複合企業規模の組織は、毎年 5% の成長率で、3 年間で 619,000 ドルのコストに対して 224 万ドルの効果を実現しました。 （Forrester Consulting TEI 調査）

これらの効果により、正味現在価値 （NPV） が 162 万ドル増加し、3 年間の ROI は 261% にもなり、導入後 6かヵ月で複合組織の初期投資額を回収することができました。 （Forrester Consulting TEI 調査）

同じ委託を受けた TEI の調査によると、これらの効果は次の分野から生み出されています。

- 技術スタックの統合
- ソフトウェアライセンスの再利用
- 自動パッチ適用
- ユーザー生産性の向上
- セルフサービス型のオンボーディングとプロビジョニング



委託されたTEI調査の回答者とのインタビューによると

セルフサービス型のオンボーディングとプロビジョニング
複合企業で 3 年間 716,632 ドルのコスト削減

「Ivanti で開発したのは、管理職がセルフサービスポータルを使って送信できるオンボーディングフォームです。 自動的にチケットを登録し、適切なチームに転送します。 以前のようにチェックリストを実行する必要はありません。」

（さらに、オンボーディングプロセスに費やす IT の時間を 50% 削減できると推定しています。）

- 政府機関のIT 担当者

技術スタックの統合と除却されたレガシーツール
複合企業で 3 年間 358,734 ドルのコスト削減

「私のリモートソリューションは年間 75,000 ドルでした。 私の [IT 資産管理]（ITAM） はさらに 10 万ドルでした。 ナレッジ管理はさらに年間 2 万ドルでした...。 1 つのベンダーに統合して、それらのコストをすべてまとめてしまえば、節約になります。」

- デスケア企業の IT・通信サポート担当役員

パッチ機能と統合の自動化
複合企業で 3 年間 162,515 ドルのコスト削減

「パッチを自動化するための設計や話し合いに 1 か月を要しました。 ポリシーを構築した後は、ロールアウトプロジェクトの設定に 1 時間もかからず、パッチを適用するだけです。 私がその作業をする必要はなく、自分が見ている情報が正確であるという自信があります。」

- 靴小売業者のインテグレーションマネージャー

ソフトウェアライセンスの再利用
複合企業で 3 年間 439,449 ドルのコスト削減

以前は、ソフトウェアを再利用しようとすると、ユーザーに声をかけて、「もうずいぶん使っていないようですが、回収しても良いですか」と確認するのに、非常に長いプロセスが必要でした。ソフトウェアライセンスを EPM ソリューション （Ivanti Neurons for UEM の一部） に取り込むと、ソフトウェアの再利用を自動的に実行できるようになりました。[...] それが、当社の最大のコスト削減になったと思います。」

- 食品製造企業のインフラストラクチャ・エンドポイント提供サービスマネージャー

エンドユーザーの生産性向上
複合企業で 3 年間 560,521 ドルのコスト削減

「古いプロファイルの更新、7 日間再起動しなかったコンピューターの再起動、夜間のパッチ適用など、自己修復を行うことで、コンピューターが以前使用していたリソースを取り戻し、エンドユーザーの生産性を向上させることができました。[...] エンドユーザー側には、1 分単位で節約できるため、経済的な効果があります。」

- デスケア企業の IT・通信サポート担当役員

詳細については、Ivanti Unified Endpoint Management （UEM） ソリューションの Total Economic Impact™ をお読みください。

参考

1. Bitwarden. 2022 Password Decisions Survey. November 2021. https://bitwarden.com/images/resources/2022-password-decisions-survey.pdf.
2. Bond, Shannon. Twitter employees quit in droves after Elon Musk's ultimatum passes. 17 November 2022. https://www.npr.org/2022/11/17/1137413251/twitter-employees-quit-elon-musk.
3. Bonner, Carole. Health and Wellbeing for the Remote & Hybrid Workforce. 20 October 2022. https://8926463.fs1.hubspotusercontent-na1.net/hubfs/8926463/Remote%20Hybrid%20Workforce_Formatted.pdf.
4. Brasen, Steve. Evolving Requirements for Digital Employee Experience (DEX). 4 August 2022. https://www.ivanti.com/resources/v/doc/ebooks/ema-iva009a-ivanti-requirements-ebook.
5. Breg, David. Quarterly Cyber Insurance Update. 10 February 2023. https://www.wsj.com/articles/quarterly-cyber-insurance-update-february-2023-62141c19.
6. Chase, Melissa, et al. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook. 14 November 2022. https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.
7. Cipolla, Tom, et al. Magic Quadrant for Unified Endpoint Management Tools. 1 August 2022. https://www.gartner.com/doc/reprints?id=1-2AQEK9FU&ct=220802&st=sb.
8. Datto. Datto's Global State of the Channel Ransomware Report. November 2020. https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.
9. Day, Lewin. Tesla App Unlocks Someone Else's Car, Lets Them Drive Away in It. 14 March 2023. https://www.thedrive.com/news/tesla-app-unlocks-someone-elses-car-lets-them-drive-away-in-it.
10. Decime, Jerry. Settling the score: taking down the Equifax mobile application. n.d. https://www.linkedin.com/pulse/settling-score-taking-down-equifax-mobile-application-jerry-decime/.
11. Flexera Software. 2021 State of IT Visibility Report. June 2021. https://info.flexera.com/ITV-REPORT-State-of-IT-Visibility.
12. Forrester Consulting study commissioned by Ivanti. The Total Economic Impact™ Of Ivanti Unified Endpoint Management (UEM) Solutions. July 2022. https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf.
13. Greenburg, Andy. Hackers Remotely Kill a Jeep on the Highway—With Me in It. 21 July 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
14. IBM Security. X-Force Threat Intelligence Index 2022. February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ.
15. Insight Enterprises & CIO. Insight intelligent technology report 2022: IT ambions for business transformation. November 2021. https://ca.insight.com/en_CA/content-and-resources/gated-content/insight-intelligent-technology-report-ac1252.html.
16. Ivanti. 2022 Digital Employee Experience Report. 28 June 2022. https://rs.ivanti.com/ivi/2700/4e528f833de3.pdf.
17. —. 9 Must-Know Phishing Attack Trends. 20 July 2021. https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465.
18. —. Getting Started With DEX: Core Areas of Focus to Deliver a Great Digital Employee Experience. 23 Novemer 2022. https://rs.ivanti.com/ivi/2734/f6efbc801083.pdf.
19. —. Government Cybersecurity Status Report. 9 March 2023. https://www.ivanti.com/resources/v/doc/ivi/2747/a856c631661d.
20. —. Press Reset: A 2023 Cybersecurity Status Report. December 2022. https://www.ivanti.com/lp/security/assets/s1/2023-cybersecurity-status-report.
21. Khandelwal, Swati. Equifax Suffered Data Breach After It Failed to Patch Old Apache Struts Flaw. 14 September 2017. https://thehackernews.com/2017/09/equifax-apache-struts.html.
22. Kolodny, Lora. Twitter is down to fewer than 550 full-time engineers. 20 January 2023. https://www.cnbc.com/2023/01/20/twitter-is-down-to-fewer-than-550-full-time-engineers.html.
23. Lutkevich, Ben. Wi-Fi Pineapple. October 2022. https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple.

参考

24. Morning Consult and IBM. IBM Security Incident Responder Study. 3 October 2022. https://www.ibm.com/downloads/cas/XKOY5OLO.

25. NASCIO. The 2021 State CIO Survey. October 2021. https://www.nascio.org/wp-content/uploads/2021/10/2021-State-CIO-Survey.pdf.

26. Palmer, Annie. Amazon employees push CEO Andy Jassy to drop return-to-office mandate. 21 February 2023. https://www.cnbc.com/2023/02/21/amazon-employees-push-ceo-andy-jassy-to-drop-return-to-office-mandate.html.

27. Paychex. Feeling the Burn(out): Exploring How Employees Overcome Burnout. 25 February 2019. https://www.paychex.com/articles/human-resources/impact-of-employee-burnout.

28. Proofpoint. 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. May 2022. https://www.proofpoint.com/sites/default/files/white-papers/pfpt-us-wp-voice-of-the-CISO-report.pdf.

29. PwC. 2022 Global Digital Trust Insights. December 2021. https://www.pwc.se/sv/pdf-reports/cybersecurity/cyber-global-digital-trust-insights-2022.pdf.

30. Rhysider, Jack. Darknet Diaries, Episode 68: Triton. June 2020. https://darknetdiaries.com/transcript/68/.

31. Rundle, James. “Economic Uncertainty Weighs on Cyber Chiefs.” Wall Street Journal 13 January 2023. https://www.wsj.com/articles/economic-uncertainty-weighs-on-cyber-chiefs-11673562985.

32. SAM. IoT Security Landscape Report. July 2022. https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf.

33. SANDIA. Cybersecurity for Electric Vehicles Charging Infrastructure. July 2022. https://www.osti.gov/servlets/purl/1877784/.

34. Shackleford, Dave. SANS 2022 Cloud Security Survey. March 2022. https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security-survey.pdf.

35. Shumway, Emilie. Monster: Two-thirds of workers would quit if forced to return to the office five days a week. 26 September 2022. https://www.hrdive.com/news/monster-two-thirds-workers-would-quit-forced-back-to-office/632690/.

36. Smith, Ray A. Quiet Quitters Make Up Half the U.S. Workforce, Gallup Says. 29 September 2022. https://www.wsj.com/articles/quiet-quitters-make-up-half-the-u-s-workforce-gallup-says-11662517806.

37. Tsipursky, Gleb. The return to the office could be the real reason for the slump in productivity. Here’s the data to prove it. 16 February 2023. https://fortune.com/2023/02/16/return-office-real-reason-slump-productivity-data-careers-gleb-tsipursky/.

38. Vanson Bourne for Nutanix. Nutanix Enterprise Cloud Index: Application Requirements to Drive Hybrid Cloud Growth (2019 edition). November 2019. https://www.nutanix.com/content/dam/nutanix/resources/gated/analyst-reports/enterprise-cloud-index-2019.pdf.

39. Verizon. Mobile Security Index 2022. 2022 August 2. https://www.verizon.com/business/resources/reports/2022-msi-report.pdf.

40. Wei, Wang. Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer. 16 April 2018. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

41. Weissman, Cale Guthrie. Here’s Why Equifax Yanked Its Apps From Apple And Google Last Week. 15 September 2017. https://www.fastcompany.com/40468811/heres-why-equifax-yanked-its-apps-from-apple-and-google-last-week.

42. Wilson, Dan, et al. Market Guide for DEX Tools. 31 August 2022. https://www.gartner.com/doc/reprints?id=1-2B07Z49S&ct=220902&st=sb.

43. Yang, Mary. Elon Musk gives Twitter employees an ultimatum: Stay or go by tomorrow. 16 November 2022. https://www.npr.org/2022/11/16/1137105935/twitter-elon-musk-ultimatum.

統合エンドポイント管理のためのガイドブック

最新のエンドポイント管理ソリューションがどのようにセキュリティと従業員体験に影響するのか

ivanti

ivanti.com/ja
03-6432-4180
contact@ivanti.co.jp