ivanti

ITの拡張性と可視性

常にネットワークにアクセスするすべての資産を特定し、IT資産全体を一元管理する方法

目次:

Everywhere Work の拡大により、組織は急速に成長することができました。 同時に、その背後では、IT 環境が急速に複雑化しています。 各従業員は平均で 2.6 台のデバイス を使用して、日常の業務を遂行しています。 つまり、IT チームは、ネットワークにアクセスするすべての資産を常に把握し、環境に変化があってもそれを維持できるようにしなければなりません。

この eブックでは、
包括的な概要、実践的な手順、および例示的なユースケースについて説明し、可視化の視野を広げ、所有している資産を真の意味で把握できるようにします。

この eブックは、ITSM+ Toolkit の一部です

ivanti

課題

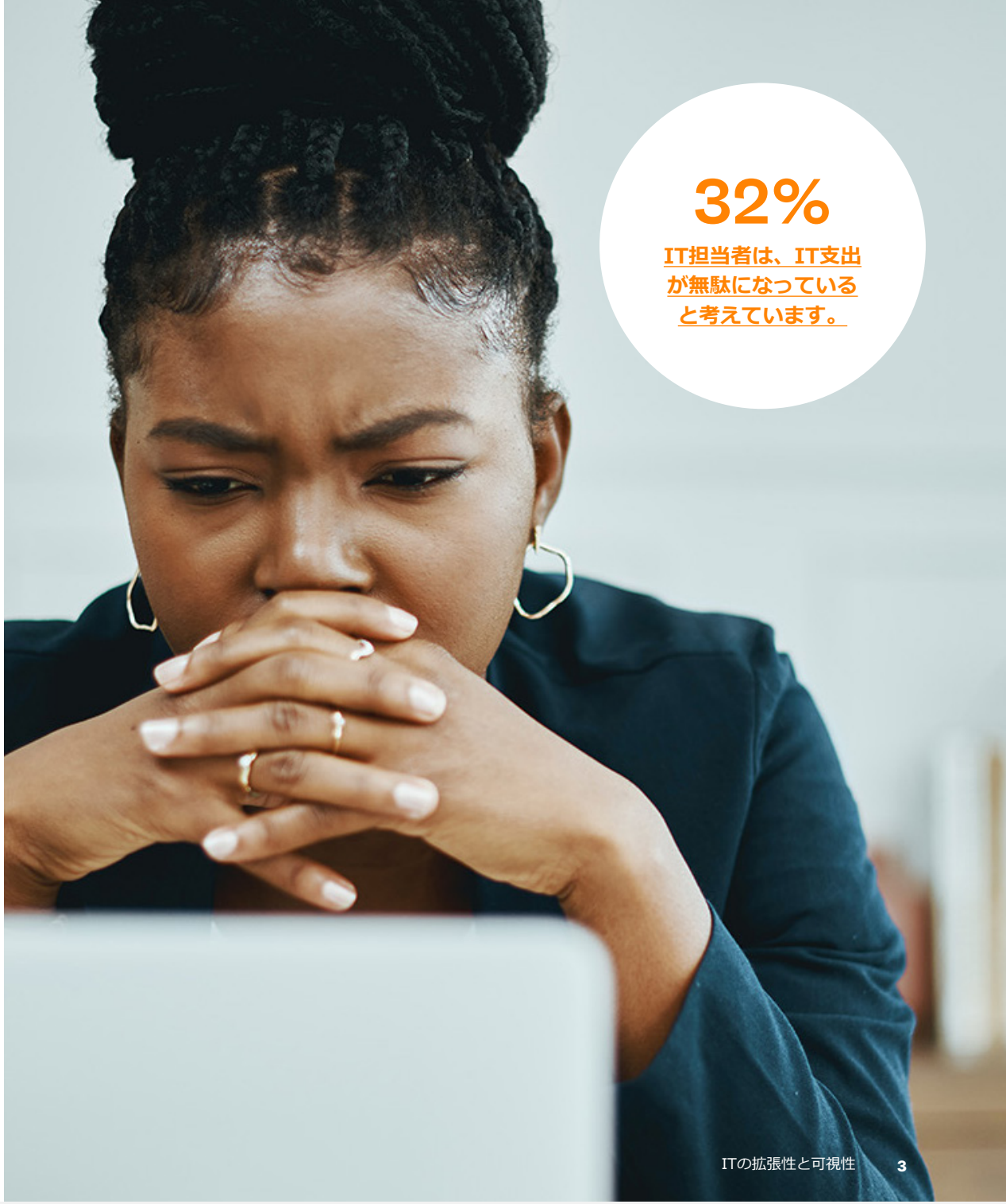
ネットワークに常時アクセスしているすべての資産を特定する。

今所有している資産を保護し、将来に備えるためのツールやプロセスの適切な組み合わせを探しているのでしょう。 つまり、把握できていない資産を保護したり管理したりすることはできません。

エンドポイントやサーバーを含むすべてのIT資産とサービスを完全に可視化できなければ、増え続けるサイバー脅威から組織を守りながらITサポートリクエストを効果的に解決すること、コンプライアンスを維持することに関して、常に一歩遅れをとることになります。 エンドポイントが従来の境界をはるかに超え、エッジまで広がっている今、エンドポイントの検出と保護はきわめて複雑な課題となっています。さらに、IT支出を最適化する機会も逃している可能性があります。

知っていますか?

ネットワークへのアクセスを試みるすべてのデバイスを完全に可視化できていると回答したIT担当者は、わずか47%です。



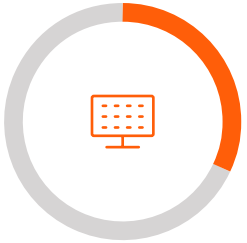
ivanti

解決

IT資産全体を一元的に把握することで、すでに所有している資産の全貌を把握し、進化するIT資産もわかるようになります。

スプレッドシートを追跡する必要も、幽霊資産もなくなります。 全体像がわかると、それぞれの資産がどのようにつながっているのかが **明確に可視化**されます。サービスデスク担当者は、すべてのIT資産に関する **包括的な情報にアクセスできる** ため、多数のスプレッドシートに目を通すことなく、問題を迅速に特定し、解決することができます。さらに、問題が起きたときに、それが全体の環境に与える潜在的な影響を確認でき、ネットワークに大きなリスクがある場合は ITセキュリティチームにアラートすることができます。

チームは、未使用の資産や活用しきれていない資産を特定し、そのような資産を交換が必要な資産と入れ替えたり再割り当てしたりすることで、**組織のIT 支出の最適化**を容易に実現することができます。 このようにして、組織はIT投資から最大の価値を得ることができます。 そして、時間を節約することで、IT チームはテクノロジーの現状だけでなく、今後の方向性にも時間を費やすことができるようになります。



32%

IT担当者はまだスプレッドシートを使用してデバイスを管理しています。

方法

資産のアクティブ検出だけでなく、パッシブ検出も可能なソリューションを探します。

エージェントレスアプローチにより、すべての IT 資産の全体像を迅速に把握することができ、重要な時間を節約して IT の生産性を高めることができます。IT資産に直接ソフトウェアをインストールする必要はありません。この機能は、帯域幅が限られている場合などに特に有効です。 サービスマッピング を使用して、基盤のデータセンターサービスとアプリケーションの間の関係と依存関係を浮き彫りにすることで、問題の根本原因を迅速に判断して、その影響度を評価し、ビジネスにとってのリスクを評価できます。

どのくらいの頻度で新しい資産をスキャンすべきなのか?

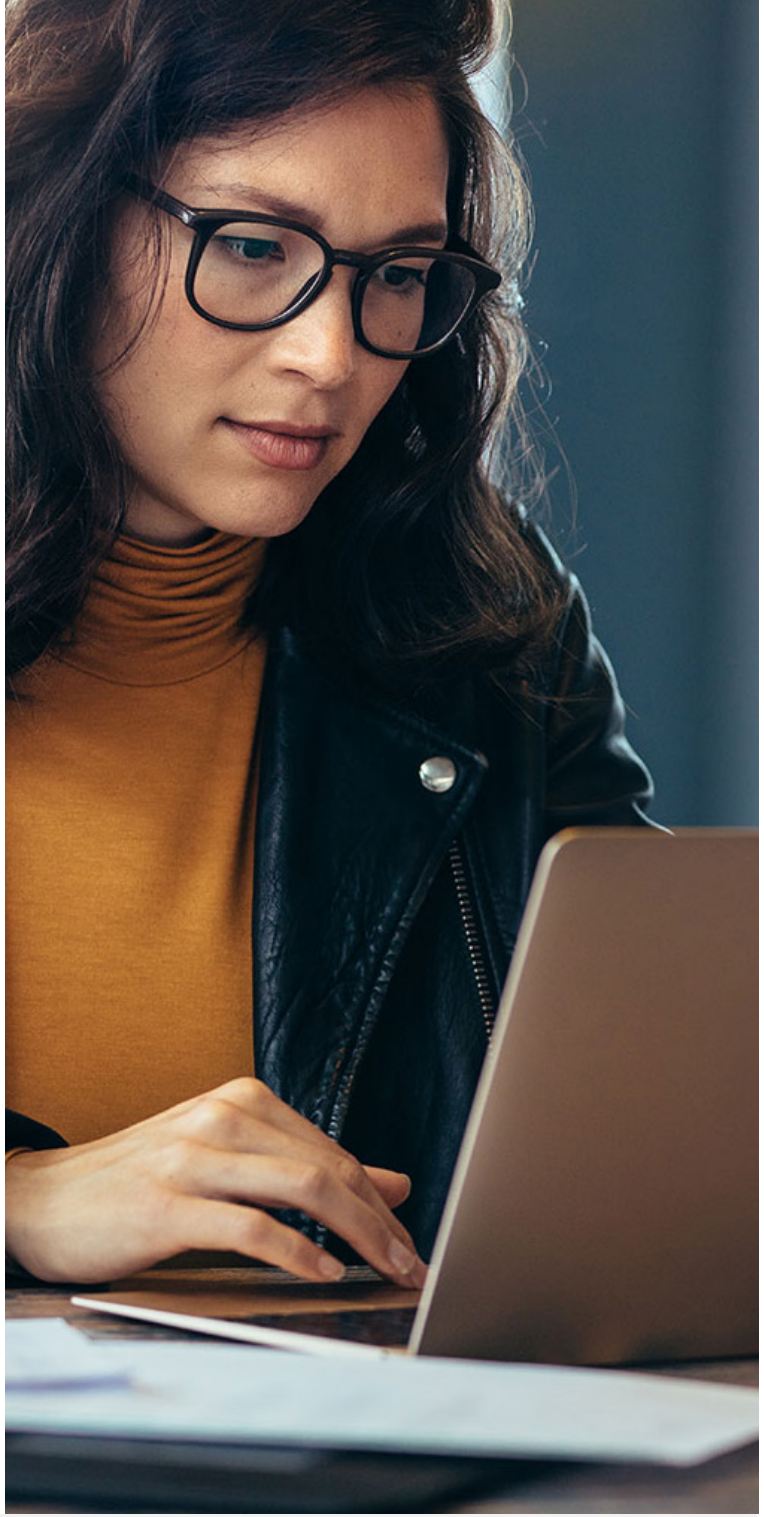
新しい資産を定期的にスキャンするよりも、新しい資産がIT環境に接続されたときに **新しい資産をリアルタイムで検出**できるツールを活用することを検討してください。 これにより、すでに存在していることが分かっている資産を検出するだけでなく、幽霊資産、つまり想定外のデバイスをすばやく検出できるようになります。

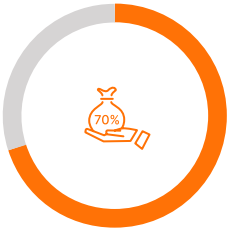
なぜアクティブ検出だけでは不十分なのか?

アクティブ検出はすでに特定されている資産しかスキャンしません。つまり、把握できていない資産は管理できません。そして、これが重大なセキュリティリスクにつながります。パッシブ検出では、IT環境に存在していたことさえ気付いていなかった資産も検出されます。一般的に、このような資産は、認識していた資産よりも、20% ～ 30% も多くなっています。 また、施設内の 1つ以上の資産への不正アクセスを取得した悪意のあるアクターも特定できます。 アクティブ検出とパッシブ検出の両方を採用することで、すでに把握している資産だけではなく、**すべての資産を特定して保護** することができます。

利点

- IT資産全体をリアルタイムで可視化する
- サービスとアプリケーションとの間の依存関係を明確にする
- すべての資産に関する正確なデータを一元的に管理する
- ITの生産性の向上
- IT支出の最適化





70%

以前のベンダーと比較したコスト削減額(最新のITSM およびITAMソリューションを導入したあるエネルギー企業)。

「Ivanti Neurons for Service Mappingによってインフラストラクチャとデータフローの全体像を把握したことで、事業継続モデルで可用性の優先度を設定し、エンドユーザーに最も影響を与えるビジネスクリティカルなサービスを迅速に復旧するための知見を得ることができました。」

Robert Hanson（ロバート・ハンソン） 氏：
The First Bank社 情報技術担当ディレクター

次のことを想像してみてください。

可視化される範囲が広がりました。

ITアナリストは、IT環境の安全性を評価しながら、組織の資産の75%しか把握できていないことがわかりました。

さらに悪いことに、資産は管理されなくなりつつあり、多くの資産は誤って構成されていたり、最新のパッチが適用されていなかったりする状態です。

アクティブ検出とパッシブ検出を活用してエンタープライズサービス管理をサポートすることで、迅速に正確なインベントリを作成し、実際に直面しているリスクをより効果的に管理できるようになります。

完全版 ITSM+ Toolkit の次のステップをご覧ください。

Toolkit を表示

ivanti

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