ハイパーオートメーション

IT体験とユーザー体験を同時に向上させながら、コスト、迅速性、正確性を改善

ivanti Neurons

はじめに

このホワイトペーパーは、以下のポイントをご紹介しています。

特にIT部門は、予算やリソースを増やすことなく、より多くのことをこなさなければなりません。例えば、多世代にわたる従業員への対応、ITにおけるやり取りの好みの変化、いつでもどこでも仕事をする環境などは、サービス提供やサービス体験に対する従来のIT部門のアプローチに対して課題を投げかけています。さらに、エンドポイントや職場の重要なIoTデバイスが接続され、通信し、エッジでデータ生成されることと、セキュリティ脅威の増加と相まって、IT資産とそれを利用するユーザーのセキュリティとサービスの進化が必要となっています。

Ivantiは、こうしたトレンドに対応するため、企業が手動または半自動化されたプロセスからハイパーオートメーション（自動化）へと移行することを支援するアプローチをとっています。自動化によって、IT環境はデバイスを継続的に自己修復、自己保護し、パーソナライズされたセルフサービスのエンドユーザー体験を提供します。企業のIT部門は、自動化されたボットと連携して、自律的に問題を検知、予測、修正し、従来のデバイスと最新のデバイスのセキュリティとサービスの安全性を担保できるだけでなく、長期的な競争優位を図るために、従業員を中心とした体験の向上を目指せます。

このホワイトペーパーについて

このホワイトペーパーでは、Ivanti Neuronsのハイパーオートメーションプラットフォームが、どのようにプロアクティブなサポートを実現するか、従業員へ貢献するか、脅威への対応を加速させるか、IT資産と支出に関する情報を迅速、正確、かつ実用的に提供するかを説明します。これらの例から、エンドユーザーとITスタッフのIT体験を向上させ、組織内のすべての人により良い結果をもたらす方法をご覧いただけます。

2022年までに、

企業で生成されるデータの50%以上が、データセンターやクラウド以外で生成され、処理されるようになります。[1]

Kingston University London

ロンドンのキングストン大学の学生とスタッフは、ノートパソコンのバッテリーが古くなり、故障し始めたときに生産性を失っていました。

Ivanti Neuronsでは、保証期間内のマシンのヘルスステータスが40%を下回ったときには、サービス管理でインシデントが発生するように設定し、ハードウェアベンダーにバッテリー交換を手配するメールを送信するというルールを設けました。

ivanti

プロアクティブなサービス

インシデントに対処する最善の方法は、インシデントが発生する前に解決することです。もし、追加作業なしでそれができ、なおかつすべての信用を得ることができるとしたらどうでしょう？

ハイパーオートメーションプラットフォーム 「Ivanti Neurons」 は、潜在的な問題を常に監視する多くのボットを搭載しており、潜在的な問題にフラグを立て、ユーザーに代わってそれらを解決します。ボットがそれらのシナリオにフラグを立てる準備ができているのであれば、なぜユーザーからパフォーマンスについて苦情が来るのを待たなければならないのでしょうか？ユーザーのファイアウォールやBitLockerが誤ってオフになった場合にオンに戻すなど、「単純な」操作を自動的に行うことができ、それによって、潜在的なセキュリティの脆弱性を排除することができます。これらの自動解決はすべて追跡され、パフォーマンス指標と満足度スコアに追加されます。これは、ハイパーオートメーションで実現できる成果のほんの一例です。

Ivanti Neuronsは、アラートとトレンドレポートにより、劣化したバッテリーの充電サイクルの制限など、組織が定義したパラメータ以外のアクティビティが発生した場合に、オペレーションを通知し、時間の節約とエクスペリエンスの向上を実現します。

デバイスの保証期間が切れる前にバッテリーなどの消耗品を更新することで、どれだけの時間とコストを削減できるでしょか。 Ivanti Neuronsのエージェントをインストールすれば、IT部門が管理するすべてのデバイスにクエリを実行し、簡単にリアルタイムのインサイトを得ることができます。 ITアナリストは、この相互作用的な報告の回答を深く掘り下げ、個々のデバイスに関する詳細な情報を取得し、予測に基づいた対策を講じることができます。 またOSの異常による「ブルースクリーン」が多すぎるなど、一般的な他の苦情などに対して先を見据え措置を追加することで、エンドユーザーへの対応を迅速に行えます。

さらに、Ivanti Neuronsは、セキュリティを一切損なうことなく、IT部門から複雑な仕事を取り除き、より優れたサービスをより迅速に提供しながらIT担当者の作業負荷を軽減し、先を見据えたサービスを実現します。

「シフトレフト」

1stレベルスタッフに権限を付与する

もし、インシデントのエスカレーションの80%がファーストコールで解決できると思ったらどれだけ時間や負荷が減るでしょうか。エスカレーションは、毎日のITライフの一部です。しかし、エスカレーションされるチケットの数を制限することができれば、作業の中断が減り、より多くの時間を本来必要な業務に費やすことができるようになります。Ivanti Neuronsにより、より多くの時間をユーザーのために費やすことができ、誰もが快適に業務を遂行できます。

Ivanti Neuronsは、これまでITスペシャリストにエスカレートされたインシデントを検出、診断、および修復するのにも役立ちます。 Ivanti Neuronsは、検出、自動化されたボット、リアルタイムの資産分析情報をパッケージとして統合しているため、大半のエスカレーションに伴う複雑性、長い待機時間、高コストの削減を実現します。 これにより、エンドユーザーは、迅速で高品質な解決策を得ることができ、業務を中断することなく、優れた体験を享受できます。

「シフトレフト」 の取り組みが実現すれば、ユーザーはより多くのツールを自分で活用できるようになり、フロントラインのサポートアナリストは、従来スペシャリストへのエスカレーションが必要であったタスクを実行できるようになります。IIT部門は、さまざまな指標における改善を実現します。 IT部門は、ユーザーの満足度とインシデントにかかるコストをそれぞれ改善しながら、終了までの平均時間を短縮し、エスカレーションの数を減らすことができます。

遅延の問題を診断し、解決するのに時間をかける必要はありません。Ivanti Neuronsは、定義された最大閾値を超える遅延を検出し、修正措置を講じて、結果を検証できます。 それでも解決されない場合、Ivanti Neuronsは、診断と試行された修正を含むヘルプデスクチケットを作成します。 そこから、サポートアナリストは、あらかじめ組み込まれたリモート機能とアクションを使用して、ITスペシャリストにエスカレーションすることなく、潜在的な根本原因の範囲を絞り込んでトラブルシューティングを行うことができます。

遅延の問題を診断し、解決するのに時間をかける必要はありません。Ivanti Neuronsは、定義された最大閾値を超える遅延を検出し、修正措置を講じて、結果を検証できます。

14日間のSLAを達成

パッチが提供されているにもかかわらず適用されていない脆弱性が、セキュリティ侵害の実に60%を占めています。[2] 脅威の特性を正確に把握することで、リスク要因が最も高い脆弱性に優先順位をつけることができ、5件のインシデントのうちの3件を排除できる可能性があります。

Ivanti Neurons は、機械学習アルゴリズムを通して、より迅速な脆弱性修復を支援します。 これは、セキュリティの脅威が深刻化し、頻度も増している中、脅威に直面しているSecOpsチームにとって自動化の重要な「手助け」になります。 セキュリティチームやその他のITチームは、監査を実施してコンプライアンスに準拠していないシステムを特定し、コンプライアンス・レポートを迅速かつ容易に受け取ることで、より効率的に調整できます。

ハイパーオートメーションにより、リスクに優先順位を付け、脅威への対応を迅速に行うことができます。 14日間のSLAは、もはや長期的でもなく意欲的な目標ではありません。 セキュリティチームは、パッチの信頼性を高めるデータと実用的な情報を得ることで、パッチ適用までの時間を短縮することができます。 データは、クラウドソースで公開されている様々な場所から取得され、適応的なセキュリティを促進する高品質なインサイトを提供します。

脅威アクターは、1ヶ月以内に脆弱性を悪用することができるようになりました。 Ivanti Neuronsは、企業が危険にさらされる時間を短縮することを支援します。 セキュリティチームは、信頼できる公開ソース全体にデータをプールすることによって、脅威に優先順位を付け、脆弱性の修正の迅速化を図り、コンプライアンスをより効果的に確保するためのインサイトを得ることができます。

セキュリティチームとITチームの連携が向上し、重複した作業を排除するとともに、脆弱性修正に費やす時間を最大で75%削減することができます。

迅速で正確に、かつ実用的な資産と支出に関する情報

エッジデバイスが急増し、従来のノートパソコンやスマートフォン、IoTデバイスにまで拡大する中、企業はそれらすべてを検出、管理、サポート、保護する準備を整えなければなりません。

IT関連の固定資産の平均30%は「幽霊」資産であり、見つけることができない行方不明の資産です。[3] 未知の、もしかしたら使用権限の無いデバイスのセキュリティリスクをどの程度まで負担できますか？ データの正確性の問題を解決するために、組織は、週に平均10時間を費やしています。組織の32%は、なんと、週に25時間以上もの時間を費やしています。[4] IT資産とそのコストを正確に把握し、資産管理のスプレッドシートを更新することなく、僅か数分間のうちに把握することができるとしたら、どうでしょうか？

Ivanti Neuronsは「点と点」をつないで、複数のデータソースから正確な資産情報を収集して集約します。 ネットワーク上のすべてのデバイスにエージェントをインストールしなくても、Ivanti Neuronsはネットワークをスキャンすることができます。 完全に自動化された正規化および照合プロセスにより、[1]人当たりの人件費を25%以上削減することができます。IT資産内のあらゆるシステムと相互作用するデバイス間の相互参照と照合作業を必要せずに、重大なセキュリティリスクをもたらす見つからないデバイスの紛失や所在不明なデバイスを特定するのに役立ちます。Ivanti Neuronsは、正確な資産と支出情報を提供し、既存資産の有効活用とセキュリティの向上によるコスト効率の改善につなげます。

例えば、これまで適切に会計処理されていなかったが、企業のデータソースにアクセスするために使用されていた何万ものIT資産が自動照合により報告された場合の認識価値を考えてみましょう。このような可視性の向上により、ハードウェアやソフトウェアの資産管理を大幅に削減したり、これらのデバイスのいずれかが許可された従業員の手に渡っていない場合、潜在的なセキュリティ脅威を明らかにすることができます。これは、その社員が戦略的なプロジェクトを完了させるために時間を使えるようになること以上の利点があります。

ある大手の鉄道会社では、Active DirectoryとMicrosoft Endpoint Configuration Managerを使用しており、インベント情報には自信を持っていました。しかし、別のソリューションを使用し、ネットワークの検出スキャンを行ったところ、社内データとの不一致が判明しました結果、この鉄道会社では、想定していたよりも30%多くのデバイスを検出しました。つまり、デバイスがどこにあり、どのように使用され、セキュリティが確保されていないのか、認識していない資産が30%もあったのです。

IVANTI NEURONS

クラウドからエッジまで、自己修復、自己保護、セルフサービスのためのハイパーオートメーション

Ivanti Neuronsは、指数関数的に増大するIT要件を満たすように設計されたハイパーオートメーションプラットフォームであり、自己修復、自己保護、セルフサービスといった一連のソリューションを提供し、ITが提供するサービスのコスト、スピード、精度を向上させます。 自動化を駆使したボットは、問題を検出し、スペシャリストレベルのアクションを提供することによって、ITインシデントを「シフトレフト」します。

Ivanti Neuronsは、先を見据えた解決策でIT部門を支援し、ユーザー体験を向上させます。Ivanti Neuronsは、既存のシステムの価値を高め、Ivantiとサードパーティのシステム間で正確なデータを取得し、ITチームが単一のプラットフォームから検出、管理、保護、サービスを行えるようにします。簡単な設定で、管理コストの削減と結果が出るまでの時間を短縮します。

Ivanti Neuronsは、強力な自動化機能を備えたITのパートナーであり、「シフトレフト」 計画やセルフサービス計画をより身近なものにします。Ivanti Neuronsは、迅速性、正確性、コスト削減、および以下のような優れた体験を通じて、より優れた意思決定を行い、自動的な解決策と規範的なアクションを提供し、ユーザー体験を向上させるための賢明なアドバイスとインサイトを提供します。

- 30%以上の資産を検出し、セキュリティ体制を強化
- 脆弱なデバイスの数を最大50%削減
- 計画外の停止時間を最大63%削減
- ユーザーが報告する前に、エンドポイントの問題を最大80%解決
- セキュリティ更新の導入時間を最大88%短縮

Ivanti Neuronsは、セキュリティを損なうことなく、より優れたサービスをより迅速に提供し、ITスペシャリストの作業負荷を軽減することで、ITの複雑さを排除します。ITチームは、ネットワークからエッジまで、従来のエンドポイントと最新のエンドポイントを管理し、サービスを提供できます。

Ivanti Neuronsの機能

Ivanti Neurons for Discovery
Ivanti Neurons for Discoveryは、正確で実用的な資産情報を数分で提供します。 これによって、アクティブおよびパッシブスキャンとサードパーティコネクタを使用してリアルタイムでの可視化を実現し、正規のハードウェアおよびソフトウェアのインベントリ情報、ソフトウェアの使用情報、構成管理および資産管理データベースに効率的にフィードするための実用的なインサイトを提供します。

Ivanti Neurons for Edge Intelligence
Ivanti Neurons for Edge Intelligenceを使用すれば、IT部門は、自然言語処理（NLP）を使用してすべてのエッジデバイスにクエリを実行し、企業全体のリアルタイム情報を僅か数秒のうちに取得できます。 Ivanti Neurons for Edge Intelligenceは、センサーベースのアーキテクチャを活用して、迅速な運用認識、リアルタイムのインベントリ情報、およびエッジ全体のセキュリティ構成を提供します。

Ivanti Neurons for Healing
Ivanti Neurons for Healing は、構成ドリフト、パフォーマンス、およびセキュリティの問題を予測的に検出、診断、および自動修正し、エンドポイントのコンプライアンスを維持するための大量の自動化ボットを提供します。 日常業務の自動化は、時間とコストを削減し、従業員体験を向上させながら、本当の自己修復環境に向かう道を開きます。

Ivanti Neurons for Patch Intelligence
Ivanti Neurons for Patch Intelligence は、機械学習アルゴリズムにより、脆弱性修復のためのSLAをより迅速に達成できることを支援します。 パッチ管理プログラムの調査、優先順位付け、より良いインサイト情報を一箇所で取得できます。 実用的な情報を自動的に提供するパッチ信頼性データを活用して、脅威への対応を迅速化し、パッチ適用までの時間を短縮します。

Ivanti Neurons for Spend Intelligence
Ivanti Neurons for Spend Intelligenceは、オンプレミス、クラウド、エッジ環境におけるソフトウェアの状況とアプリケーション支出に関するインサイトを瞬時に提供し、業務スピードと資産の可視性、利用率、コストの改善を支援します。複雑なソフトウェアライセンスツールとは異なり、簡単で直感的に使用でき、結果がでるまでの時間が短縮されます。数分以内に、ライセンス、購入、およびインスタンスの魅力的なダッシュボードに表示される詳細な分析を入手し、購入履歴、今後のライセンス更新、契約期限、および継続的な支出をより効率的に追跡できるようにします。潜在的な支出超過の問題と自動再利用の機会を明らかにします。

Ivanti Neurons Workspace
Ivanti Neurons Workspaceは、デバイス、ユーザー、アプリおよびサービスを360度（全方位的）網羅できるため、リアルタイムなデータを提供します。 これにより、これまでスペシャリストにエスカレーションされていた問題を、フロントラインのアナリストが解決できるようになります。ユーザーとデバイスの画面は、複雑性、長い待機時間、高いエスカレーションコストを削減し、エンドユーザーの迅速な解決と生産性の向上を実現します。

詳しくはお問い合わせください

弊社は、お客様の業務を改善し、より良い結果を達成するために必要なソリューション、専門サービス、および教育を支援する準備ができています。 詳細については、お問い合わせください。

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp

参考:

1. Gartner, Inc. in Hype Cycle for the Internet of Things, 2020, Alfonso Velosa, Dale Kutnick, Benoit Lheureux, Roger Williams, July 15, 2020.

2. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

3. M. Day and S. Talbot, “Data Validation the Best Practice for Data Quality in Fixed Asset Management”

4. https://www.enterprisemanagement.com/research/asset.php/3311