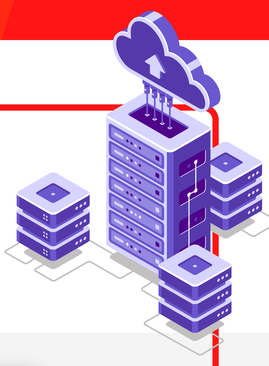
ivanti

サイバーセキュリティジャーニー

リモートワークへの迅速なシフトに伴い、新しいEVERYWHERE WORKPLACEにおいて多くのセキュリティにおける脆弱性が表面化しており、潜在的な脅威を最小限に抑えるための包括的でスケーラブルなサイバーセキュリティ戦略が必要となっています。

ここでは、堅牢なサイバーセキュリティ戦略を立てるために考慮すべき、重要な6つのポイントについてご紹介します。



1. アセットを完全に可視化する

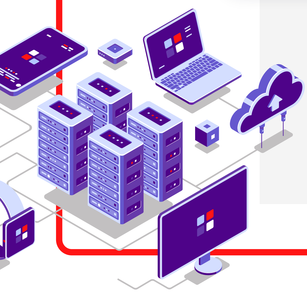
なぜ:

把握していないものは管理することができません。

正確なIT資産のインベントリ（クラウド、ソフトウェア、ハードウェア）がないと、組織はセキュリティリスクに対して脆弱になります。

どのように:

接続されたすべてのデバイスをリアルタイムで完全に可視化することで、ITインフラストラクチャの管理、整備、最適化を実現できます。



2. デバイス管理を近代化する

なぜ:

ソフトウェアを最新の状態に保ち、問題を迅速に解決するなど、セキュアな運用には、リモートユーザーとデバイス全体のコンプライアンスを監視することが重要です。

どのように:

セキュリティ戦略の一部としてUEMを取り入れる。

3. デバイスのハイジーンを確立する

なぜ:

すべてのデバイスに共通するセキュリティ要件を確立することにより、問題の診断をより迅速により簡単に行うことができます。

どのように:

自動化することにより、デバイスハイジーンに関連するセキュリティ問題をプロアクティブに検出して管理します。

4. ユーザーを保護

なぜ:

パスワードにはコンテキスト（デバイス、アプリ、ネットワーク、脅威）がないため、許可されたユーザーと許可されていないユーザーを区別することは困難です。

どのように:

ゼロサインオン：パスワードがないため、ログイン認証/パスワードが盗まれることはありません。

5. 適切なアクセスを提供する

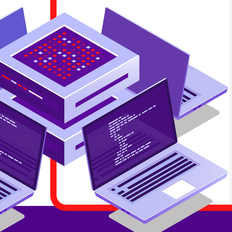
なぜ:

ユーザーを必要なビジネスリソースのみに限定することで、アクセスベースのセキュリティ脅威を最小化します。

どのように:

ゼロトラストネットワークアクセスで、企業データへのユーザーのアクセスを追跡、監視、コンテキスト化します。

6. コンプライアンスとリスク管理を自動化する



なぜ:

手動での管理は時間がかかり、非効率的で、セキュリティリスクも高くなります。

どのように:

リアクティブではなく、プロアクティブへ：コンプライアンスとリスク管理のための包括的で自動化された戦略を導入します。

堅牢なサイバーセキュリティジャーニーの構築についてご興味をお持ちですか？「管理、自動化、優先順位付け（M.A.P）サイバーセキュリティジャーニー」はこちらから：

e-bookをダウンロードする

ivanti