CISCO
SECURE

ハイブリッドワークフォースの安全を守るための 5 つのヒント

ハイブリッド環境で常に働く傾向が世界的に強まっており、そうした柔軟な環境が、雇用者と従業員に新たな利点と課題の両方をもたらしています。しかし、オフィス、リモート環境、外出先など、どのような場所で仕事をしていても、柔軟性を高めるためにセキュリティを妥協する必要はありません。以下は、従業員と企業資産の安全を確保しながらハイブリッドワークというカルチャーを維持するための 5 つの簡単なヒントです。

1 安全な仕事のプラクティスを従業員に伝える

どこで働いていてもテクノロジーが使える環境が求められていますが、働く場所を柔軟に選べるようになると、従業員も企業も新たな脅威にさらされることになります。そのため、IT チームとセキュリティチームは、セキュリティの確保や潜在的なリスクの認識について従業員を教育し、どのようなエンドポイントでも安全なハイブリッドワークを行えるようにしなければなりません。

2 本人確認を行う

多要素認証（MFA）はシンプルな、セキュリティの最初のレイヤであり、企業が資産へのアクセスを許可する前に必ず必要なものです。MFA では、本人の持つ情報（ユーザー名やパスワード）と機器（電話機）を使って ID とデバイスの健全性を確認します。

3 どこからでもセキュアなアクセスを実現

VPN は、ユーザーとアプリケーションをつなぐ安全なトンネルです。従業員は外出先や自宅での仕事中も、生産性と接続性を維持できます。適切なレベルのセキュリティを提供しながらもユーザーエクスペリエンスを損なうことなく、承認されたユーザーのみがアクセスできるようにします。

4 あらゆるエントリポイントでセキュリティ脅威から防御

ほとんどのセキュリティ侵害はエンドポイントのユーザーをターゲットとしているため、DNS レイヤでの最前線の防御と、そこをすり抜ける脅威に対する最終的な防御が必要です。最初のレイヤでは、悪意のある動作に関連するドメインがネットワークに侵入する前にブロックするか、マルウェアがすでに内部に存在する場合は封じ込めます。また、さらに高度な脅威は最後のレイヤで防御します。

5 シンプルな統合プラットフォームでセキュリティ対策を統合

個別のセキュリティ製品が混在したり、ユーザー体験に一貫性がなかったりするセキュリティ対策は、お勧めできません。SecureX なら、簡単かつ効果的なセキュリティ対策を実現できます。このシームレスに統合された組み込みプラットフォームによって、ご利用の Cisco Secure 製品とインフラストラクチャを連携させることができます。

Cisco Secure Hybrid Work を導入すると、従業員がどこで働いていても、データを安全に保つことができます。このシンプルな統合ソリューションにより、あらゆる場所でセキュリティを確保し、どこでも働ける環境を実現できます。

詳細については、cisco.com/go/securehybridwork をご覧ください。

cisco The bridge to possible