TeamViewer

リモート IT
セキュリティ チェックリスト

適切なリモート技術への投資には時間がかかります。
このチェックリストには安全なリモート IT サポート提供に不可欠な項目が網羅されています。
今すぐ、項目を確認しましょう。

強固なパスワード ルールの導入

シングル サインオン（SSO）を導入して、従業員の安全プロトコルを確保します。
SSO により、従業員は一つのパスワードだけで安全にログインできるようになります。
これにより、複数の脆弱なパスワードを作る（そして忘れる）必要がなくなります。

認証レイヤーの構築

多要素認証MFA）で不正アクセスを防ぎます。
アカウント、デバイス、システムへのユーザー アクセスを許可する前に、
複数の形式による認証を行います。

リモート入力を無効化

リモート入力を無効化することで、リモート セッションの安全性を確保するとともに、
中断を防ぐことができます。
リモート接続中、サポート対象のエンド ユーザーがフローの妨げとならないことを確信できます。

画面ののぞき見を防止

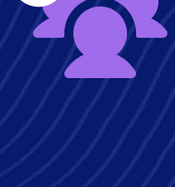
ブラック スクリーン機能がなければ、安全なリモート サポート ソリューションとはいえません。
アクセス中にリモート デバイスの画面を黒く覆うことができます。

セキュリティ基準を維持

BYOC (Bring Your Own Certificate) ポリシーによって
デジタル証明書を使用してクラウド サービスとアプリケーションを保護することができます。
これにより、さらなるセキュリティ基準とコンプライアンスの制御が可能になります。

アクセスの許可、制限、取り消し（自分のやり方で）

ルールベースの機能である条件付きアクセスでは、
ユーザー資格情報、場所、時間、デバイスなどをもとにしてアクションを行うことができ、
さらに厳格なリモート セキュリティが実現します。



アクセスの許可は選択的に

詳細なアクセス制御によって、組織内の特定のデバイスにどのユーザーが
アクセスできるかを完全に制御できます。
チーム、個人、デバイスへ、特定の権限とライセンスを適用し、ポリシーを割り当てます。

より安心できる
安全な IT サポートを提供しませんか？

さらに詳しく