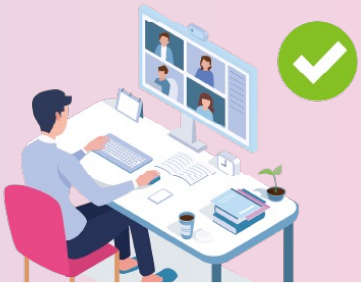
Check Point UTM でできる！

テレワークのセキュリティ対策

近年の新型コロナウイルス感染症の拡大をきっかけに、テレワークの導入が企業にとって身近なものになりました。
しかし、いざテレワークを導入する際に、「情報漏洩や不正アクセスのリスクはないか？」といった懸念を抱く企業様も多いのではないでしょうか。
本資料では、Check Point UTM を活用した**中小企業様に最適なテレワークソリューション**をご紹介します。



課題　テレワークの導入における様々な課題

テレワークは 日常業務における利便性の向上のみならず、緊急事態において業務を継続するための重要な手立てとなります。
しかしその反面、セキュリティや運用の手間 、コストといった課題も存在します。

セキュリティ面の課題

● 社外ネットワークの脅威にさらされる

社内ネットワークであれば、統一的なセキュリティ管理によって社員や端末を守ることができます。しかし社外ネットワークでは、無防備なまま様々な脅威にさらされる危険性があります。

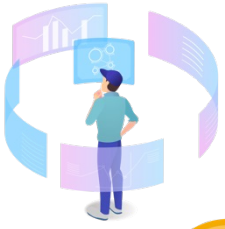
● 公衆Wi-Fiの危険性

公衆Wi-Fiは不特定多数が利用するため、同じ Wi-Fi に接続している悪意あるユーザーによって通信を傍受される危険があります。

● 社内に脅威を拡散

テレワークでマルウェアに感染した端末が社内ネットワークに接続すると、社内に脅威を拡散させるリスクもあります。

運用面の課題



リモートVPNの利用にはアカウント管理が欠かせません。専任の担当者が不在の中小企業においては、こうした運用の手間が導入においての大きな障害となります。運用面を考慮せずに導入した場合、不要なアカウントが削除されずに残るなど、新たなセキュリティリスクに繋がる場合もあります。

コスト面の課題

リモートVPNの利用には、専用のアプライアンスやサービスの新規導入、あるいは既存機器への追加ライセンス購入といったコストが必要となる場合があります。予算の限られる中小企業では、利用規模に合わない仕様で機器やサービスを選定してしまうかもしれません。

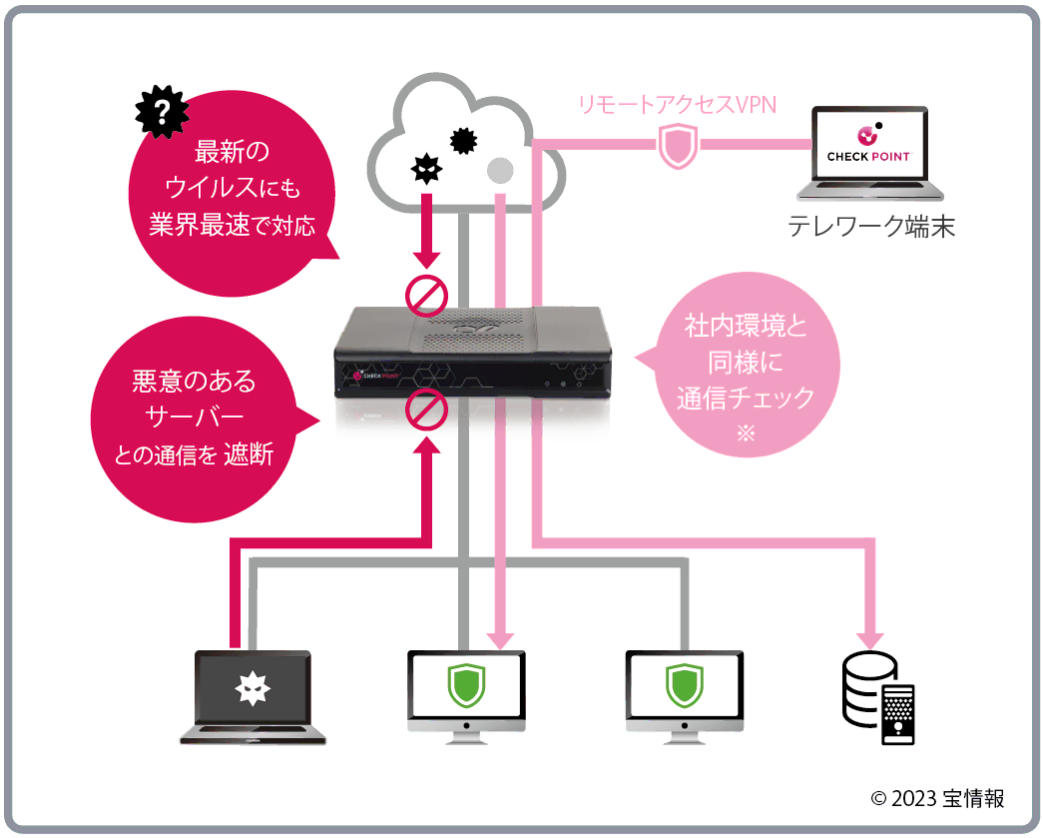
Check Point UTM には

リモートVPN機能が標準搭載！

Check Point UTM には、「リモートアクセスVPN」が標準でバンドルされています。
中小企業に対して最適解となるテレワーク環境を提供。社外から安全な接続を確立します。

解決！　セキュリティ面の課題

Check Point UTM は、インターネットVPN 接続も可能なセキュリティ対策製品です。
Check Point UTM に標準搭載されている「リモートアクセスVPN」機能を利用すれば、社内環境と同様に通信がチェックできるため、接続端末をインターネット上の脅威から保護します。



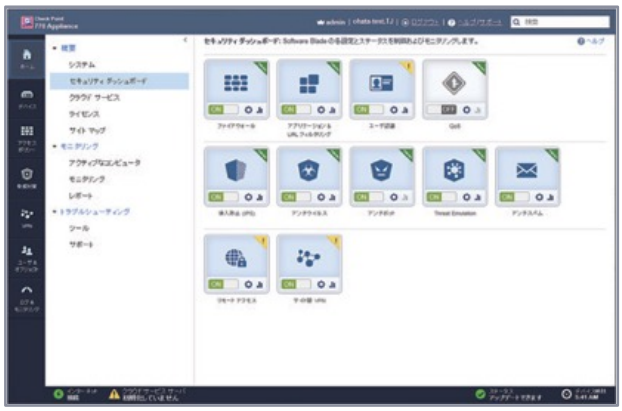
※ UTM側の設定が必要となります。

UTMとは？

UTM とは、Unified Threat Management の略で、日本語では「統合脅威管理」と呼びます。
様々な脆弱性を突いてくる脅威に対抗するためには、複数のセキュリティ機能が必要です。一般的に利用されるファイアウォールは通信のアドレスと種類だけで防御しているため、通信の内部にマルウェアが仕込まれているかどうかまではチェックできません。
UTM は通信の内容までチェックするため、ファイアウォールを通過してしまう攻撃もブロックすることができます。

解決！　運用面の課題

Check Point UTM は、ほとんどの設定を Web GUI から行うことが可能です。
シンプルで操作性のよい Web GUI により、専任の担当者のいない中小企業様にも運用が可能です。



解決！　コスト面の課題

Check Point UTM では十分な同時接続数のリモートVPNライセンスが標準で提供されています。
UTM である同モデルであれば、「リモートアクセスVPN」機能以外にも各種のセキュリティ対策に対応します。
リモートVPNの課題だけでなく、オフィスのゲートウェイセキュリティを1台の UTM に集約することで、高いコストパフォーマンスのもとセキュアな環境をオフィスと社外で実現することが可能です。

お問い合わせはこちら