

大切なビジネスを守る「ハッキング対策」を



製品概要

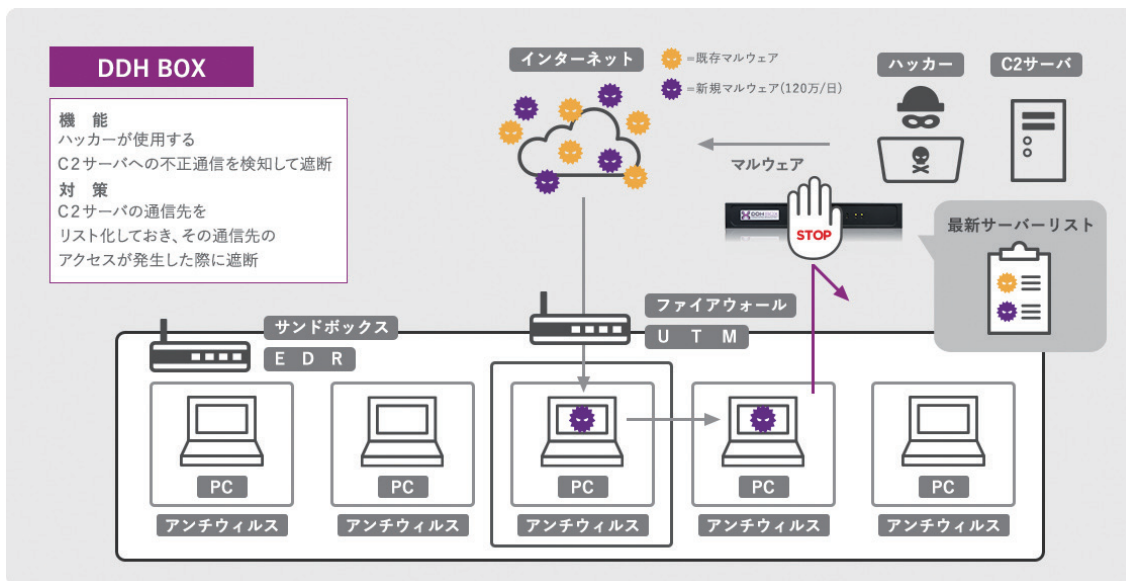
「DDH BOX」は、ハッカーが使用するC2サーバへの不正通信を検知して遮断する、出口対策製品です。これまでの、一般的なセキュリティ対策ではサイバー攻撃を100%ブロックすることはできません。ウイルスの脅威情報を検知し、侵入をブロックする「入口対策」や、怪しい動きをするプログラムを検知・停止する「内部対策」ではなく、感染しても外に出さない「出口対策」の強化が重要なのです。

特徴

1. 検知したC2サーバとの不正通信を即時に遮断

C2サーバとの不正通信を検知した時点で、通信そのものを停止します。お客様が通信の停止を判断する必要はありません。また、ランサムウェアの攻撃(※)の場合も、通信を遮断します。

※システムを乗っ取り、利用者の利用を制限。制限を解除するために、身代金を要求する攻撃。



2. ハッカーが使用する最新の不正通信を検知

LACが誇る国内最大級のセキュリティ監視センターで毎日更新される、最新のC2サーバリストを取り入れ、C2サーバとの通信を見逃しません。

株式会社ラック：サイバーセキュリティ分野のリーディングカンパニーとして、官公庁・企業・団体などのお客様に業界屈指のセキュリティ技術を駆使した、先端のITトータルソリューションサービスを提供。累計8,000社を超える企業でのサービス採用、1,000団体を超える官公庁・地方公共団体などでの実績。

3. アラートの発報後は、お客様へ脅威情報を報告

アラート発報後、即時にお客様へ情報の通知が入ります。攻撃されたPCをネットワーク環境から外すことで拡散を防ぐことができます。毎月のご利用状況、脅威情報を月次レポートとして報告します。

4. インシデント発生後のサポート

インシデント発生後の情報流出調査や、セキュリティ対策などを全面サポートします。サポート時に発生する対策費用は、年間300万円までサイバー保険を適用できます。また、弊社の事業実績を生かした、データの流出調査（データフォレンジック）、消去・改ざんされたデータ復旧についてもお任せください。

販売価格

個別見積

商品番号 1001284 DDH BOX