商品カテゴリー　セキュリティ （総合セキュリティ）

シリーズ

セキュリティサービス

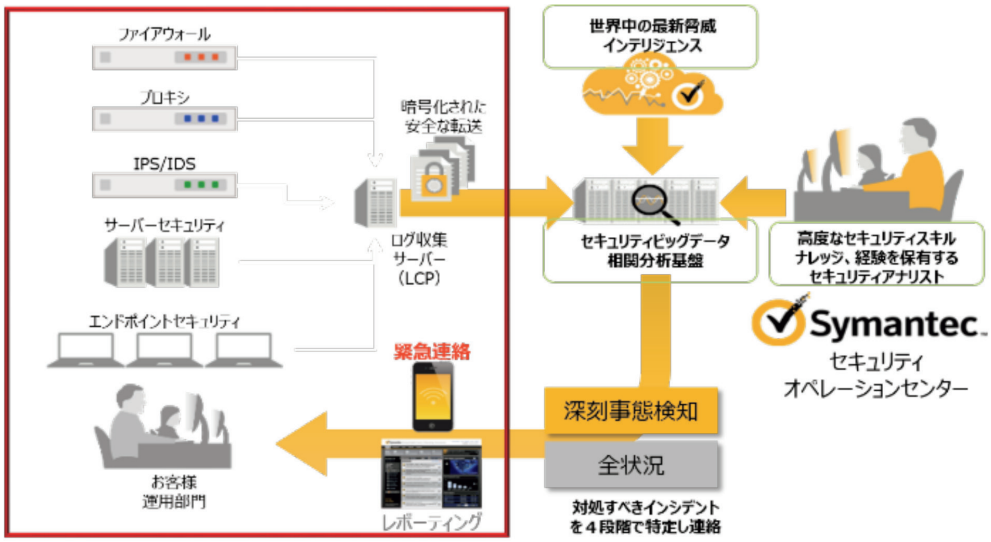
サイバー攻撃防御を強化

製品概要

業界最先端の脅威インテリジェンス、高度な監視、インシデントレスポンスサービスにより、攻撃ライフサイクルのあらゆるステージに対応します。（60 社、120 種以上のプラットフォームに対応）

商品番号 1001760 **Managed Security Service(MSS)**

セキュリティアナリストが 24 時間 365 日、貴社のネットワーク環境全体（ファイアウォールからアンチウィルスソフトが導入されている端末まで）を網羅的、且つリアルタイムに監視するサービスです。



Module	解説
Alert Module	主にIPS/IDS、OS、アプリケーション、及びクライアントウイルス対策に適用され、セキュリティ製品が検知したアラートをベースに、インシデントを特定するモジュール
Scan Module	主にファイアウォールに適用され、全ての許可、遮断された通信を相関して、インシデントを特定するモジュール
Hot IP Module	記録されたログのIP、ポート番号を、MSSがもつ既知の悪意のあるIP、ポート番号と照らし合わせ、一致した場合にインシデントを生成するモジュール
Malicious URL Module	記録されたURLを、MSSがもつ既知の悪意のあるURL情報と照らし合わせ、一致した場合にインシデントを生成するモジュール（ドメインや、ドメインに限らず引数以降の文字列なども正規表現を用いて検知）
Malware Module	ウイルス対策の検出ログからインシデントを特定するモジュール
Suspicious Traffic Module	規定された、悪意のある通信パターンを検出し、インシデントを特定するモジュール
Brute Force Module	規定された時間内に、一定以上の同じイベントが検出され、悪意のある行為と考えられる場合にインシデントを特定するモジュール
IP Reputation Datafeed	シマンテックの持つ、Global Intelligence Networkから得られた悪意のあるIPリストと照らし合わせ、ボットネットのコマンド＆コントロールとの通信や、Phone Home通信を検出する
URL Reputation Data Feed	シマンテックの持つ、Global Intelligence Networkの情報と照らし合わせ、ボットネットのコマンド＆コントロールのURLリクエストを見つけ出す
Anomalous Traffic Detection	監視下にある全てのIP（全てのポート）から発信、または受信した通信から、30日間の通信量のベースラインを割り出し、急激な通信の増加など不審な通信を検出する
Domain Generation Algorithm	ランダムに生成されたドメインが一定期間生成された場合に検出するモジュール。学習機能により誤検知を軽減。

販売価格

個別見積

商品番号 1001760 Managed Security Service(MSS)

商品・サービスのお問合せ、お見積りはこちら▼