

Deep Discovery™ powered by Express5800

デイープ ディスカバリー

標的型攻撃対策アプライアンス



標的型攻撃で利用される新型ウイルスなどを検知し、ネットワーク内の感染状況を可視化することで、機密情報漏えいなどの被害を防ぐ。

適用効果

新型ウイルスを検知(入口対策)

従来のパターンファイルだけでは検知できない新型ウイルスを、複数のロジックによる挙動分析と、仮想化環境(Sandbox)による動的解析で検知します。

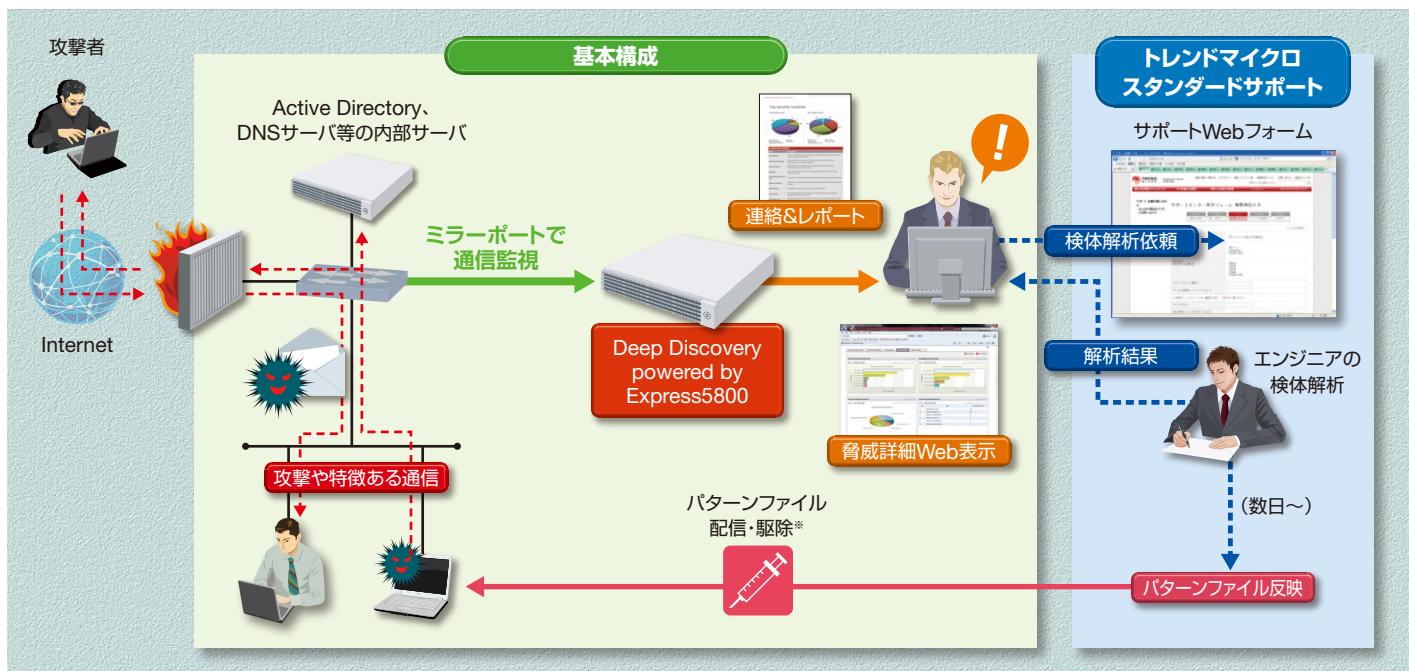
ウイルス感染PCを検知(内部通信・出口対策)

ウイルスの特徴のある通信・挙動や接続先を分析することで、ウイルスに感染したPCを脅威として検知し、ネットワーク内の感染状況を管理者へ通知します。

脅威の可視化・分析レポート

脅威をリアルタイムに通信ログとして可視化し、分析結果をレポートとして自動作成します。また、エンジニアによる脅威分析などを提供します(オプション)。

システムイメージ



機能一覧

多段解析(静的解析・動的解析)

PDFやWordなど文書ファイルの脆弱性攻撃の検出や挙動分析、URL判定等による脅威分析(静的の解析)と、不審なファイルを仮想化環境上で動作を再現する動的解析(Sandbox機能)^{*1}、多段解析により脅威を検知します。

脅威を可視化

外部からの通信や内部通信に対し多段解析を実施し、脅威として現れる通信をフルローカライズされたWebコンソールにより、リアルタイムに可視化が可能です。また、脅威として解析された通信を相関分析し、レポートを自動的に作成することで、ウイルスに感染した端末を脅威として可視化できます。

ネットワーク監視型アプライアンス

ミラーポートを利用したネットワーク監視により、既存システムに影響無く、未知や既知のウイルスに感染した端末を検知します。クライアントに対してエージェントの展開作業も不要です。

復旧支援(オプション)と解析対象のチューニング

感染端末の復旧支援や、脅威の詳細分析による感染端末の洗い出しを実施する「トレンドマイクロ プレミアムサポート」をオプションにてご用意しています。また、お客様にて詳細分析を実施する際にも、解析対象を絞るといったチューニングの実施が可能です。

*1 NS版にはSandbox機能はございません。

仕様^{*2}

	Deep Discovery powered by Express5800 通常版 / NS版	Deep Discovery powered by Express5800 Advanced版
CPU	インテル®Xeon®プロセッサー E5ファミリー ×1	インテル®Xeon®プロセッサー E5ファミリー ×2
メモリ	8GB	16GB
内蔵HDD	500GB(RAID1)	
標準ネットワークインターフェース	1000BASE-T LANコネクタ ×6(含 管理ポート1)	1000BASE-T LANコネクタ ×8(含 管理ポート1)
外形寸法(W×D×H mm)	439.8×722.0×43.4(1U) ※突起物／フロントベゼルを含まない	
重量	12kg	
消費電力	450W(冗長構成)	
温度条件	動作時:10~40°C、保管時:-10~55°C	



*2 2014年2月現在の仕様となります。最新の仕様はWebをご覧ください。

製品構成

製品名		概要
Deep Discovery powered by Express5800 Advanced版	入口・内部通信・出口対策を行うためのネットワーク監視アプライアンス。1年間のソフトウェア利用許諾ライセンスを含みます。 ^{*3}	
Deep Discovery powered by Express5800	Advanced版と同機能でハードウェアスペックを抑えたNEC専用の低価格モデル。1年間のソフトウェア利用許諾ライセンスを含みます。 ^{*3}	
Deep Discovery powered by Express5800 NS版	Sandbox機能を除き、内部通信・出口対策を専門にしたNEC専用モデル。1年間のソフトウェア利用許諾ライセンスを含みます。 ^{*3}	
Deep Discovery powered by Express5800 更新	Deep Discovery powered by Express5800の2年目以降における1年間のソフトウェア利用許諾ライセンスです。 ^{*4}	
アドバンスト オプション	基本サービス(1年)	専用ポータルWebサイト「Threat Management Service Portal (TMSP)」へ通信ログを送付することで、日次/週次/月次レポートをご提供。レポートに関するお客様からのお問い合わせの受付、早期に対応が必要なイベントが発生した場合の通知を行います。
	インシデント通知サービス(1年)(週次/月次)	TMPSへ通信ログを送付し、トレンドマイクロのエンジニアがその通信ログを確認。お客様の脅威動向を把握した上で、優先対応が推奨されるイベントを選別して、メールにて通知を行います。
トレンドマイクロ プレミアムサポート for Enterprise Threat Management Gold / Silver	お客様担当のテクニカルアカウントマネージャによるサポートやインシデント発生時の迅速な支援と優先的な復旧サポート、セキュリティリスクを抑止する事前対策支援等により、お客様の組織内に潜む脅威を可視化し、セキュリティリスクを最小化するための支援を提供します。	

*3 ソフトウェア・サポートサービス、ハードウェアサポートは、別途契約が必要となります。

*4 NS版、Advanced版に関しても更新ライセンスが別途ございます。

●価格やその他オプションサービスなど、詳細につきましてはお問い合わせください。

人と地球にやさしい情報社会へ

REAL IT PLATFORM G2

クラウド・コンピューティングを支える次世代IT基盤

お問い合わせは、下記へ

NEC プラットフォームビジネス本部

〒108-8424 東京都港区芝五丁目33番8号(第一田町ビル)

TEL : 03(3798)7177

【受付時間】9:00~12:00 13:00~17:00 月曜日~金曜日(祝日・NEC所定の休日を除く)

<http://jpn.nec.com/soft/trendmicro/dd/>

●カタログ中の社名、製品名は各社の商標または登録商標です。

●本製品(ソフトウェア含む)が、外国為替及び外国貿易法の規定により、規制貨物等に該当する場合は、日本国外に持ち出す際には、

日本国政府の輸出許可申請書等必要な手続きをお取りください。

●本紙に掲載された製品の色は、印刷の都合上、実際のものと多少異なることがあります。また、改良のため予告なく形状、仕様を変更することがあります。