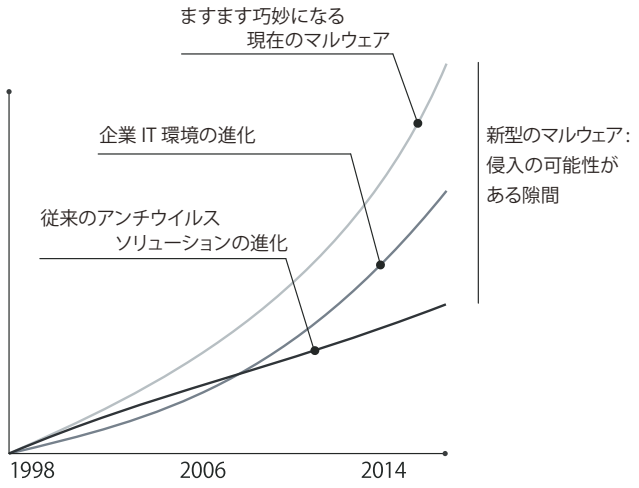
Adaptive Defense 360

本質を見出し、問題を解決する

保護、検出、対応、そして修復までをシングルソリューションで統合する完全なエンドポイントの防御

セキュリティ攻撃からエンドポイントを守ることは容易ではありません。エンドポイントの保護には、従来のウイルス対策 / マルウェア対策、パーソナルファイアウォール、Web ＆電子メールのフィルタリング、デバイス制御、ランサムウェア対策など、幅広い防御が必要です。そして、検出が困難なゼロデイ攻撃や標的攻撃、最新のランサムウェアに対しては、さらなる防御策を講じる必要があります。これまで IT の常識では、エンドポイントを守るために、いろいろなベンダーからさまざまな製品を入手し、維持する必要がありました。

Adaptive Defense 360 は、業界で初めて、EPP（エンドポイント保護）と EDR（エンドポイント検出＆対応）の機能をひとつに組み合わせて提供する、類のないソリューションです。**Adaptive Defense 360** は、IT 運用の負担を軽減する機能も自動化しています。**Adaptive Defense 360** は、シンプルで集中管理されたセキュリティ、応急措置のアクション、リアルタイムモニタリングとレポート、プロファイルベースの保護、集中型デバイス制御、Web モニタリングとフィルタリングなどを含む、Panda Security の業界最高水準の EPP ソリューションとして提供を開始します。



しかしながら、上記の図に示した状況は始まりにすぎません。マルウェアと IT セキュリティを取り巻く環境は、量と巧妙さの点において大きな変化を遂げてきています。毎日 200,000 を超える新種のウイルスが出現し、防御を通り抜けマルウェアを隠すための技術が巧妙になり、企業のネットワークではこれまで以上にゼロデイ攻撃や標的型攻撃への脆弱性が高まっています。

従来のエンドポイント保護ソリューションは、シグネチャファイルとヒューリスティックアルゴリズムに基づく検出手法を用いることで、既知のマルウェアのブロックには効果的です。 しかし「マルウェア侵入の可能性がある隙間」つまり、「新しいマルウェアの出現」と「セキュリティ企業が提供する対処法のリリース」との時間差の隙間を利用するゼロデイ攻撃や標的型攻撃は防御しません。ウイルス、ランサムウエア、トロイの木馬、その他各種のマルウェアを企業ネットワークに侵入させるためにハッカーが悪用する隙間は広がる一方です。このような日常的な脅威の拡大が、機密文書を暗号化して身代金を要求したり、産業スパイが機密データをたやすく収集することを可能にします。

「適応型防衛（Adaptive Defense）」というのが、ランサムウェアや標的型攻撃など、あらゆるタイプの攻撃に対抗するための Panda Security のソリューションです。 Adaptive Defense は、組織内で実行されているすべてのアプリケーションを正確に分類し、正規のプログラムのみを実行できる EDR サービスを提供します。Panda Security の **Adaptive Defense 360** の EDR 機能は、次にあげる 3 つの原則「企業のコンピュータ / サーバー上のアプリケーションの継続的な監視」「クラウド上の弊社ビッグデータプラットフォームの機械学習を使用した自動分類」そして最後にオプションの「自動分類されていないアプリケーションについて、企業システム上で実行されるすべての動作を確実に特定するために、当社専門技術要員が分析を行う」に基づくセキュリティモデルから成ります。

これらの機能が現在は Panda Security の業界最高水準の EPP ソリューションに統合され、**「自動防御」「自動検出」「自動フォレンジック」「自動修復」**で構成される、適応型でマルウェアを保護する隙間のないサイクル（上図）を形成します。

起動されている全アプリケーションのセキュリティを保証する ただひとつのソリューション

完全で頑強な実証された保護機能

Panda Adaptive Defense 360 の 2 つの運用モード：

- **標準モード：**グッドウェアとしてカタログ化されたすべてのアプリケーション、そして Panda Security や自動化されたシステムによりカタログ化されていないアプリケーションと共に実行を許可。
- **拡張モード：**グッドウェアの実行のみ許可。「ゼロリスク」セキュリティ対策に取り組む企業にとって理想的な保護手段。

フォレンジック情報

- マルウェアに起因するすべてのイベントを明確に理解するための実行**イベントグラフを表示**。
- マルウェアコネクション、作成されたファイル、その他の情報から得られる地理的ソースに関するヒートマップから可視化された情報を取得。
- ネットワークにインストールされた既知の脆弱性のあるソフトウェアの位置を特定。

脆弱なオペレーティングシステムとアプリケーションの保護

開発元のサポートが終了しパッチが当てられず脆弱な Windows XP などのシステムは、ゼロデイ攻撃や新世代の攻撃にとって格好の餌食となります。

さらに、Java、Adobe、Microsoft Office、ブラウザなどによるアプリケーションの脆弱性は、マルウェアの 90%で悪用されています。

Adaptive Defense 360 の脆弱性保護モジュールは、企業がアップデートされていないシステムを保有していたとしてもセキュアな環境で作業できるように、コンテクスチュアル（状況に即した）ルールと振る舞いルールを適用します。

完全な EPP 機能

Adaptive Defense 360 は、Panda Security の最も洗練された EPP ソリューション Panda Endpoint Protection Plus を統合し、以下のような完全な EPP 機能を提供します。

- 修復措置
- 集中型デバイス制御：複数のデバイスタイプをブロックすることでマルウェアの侵入やデータ損失を防止
- Web の監視／フィルタリング
- Exchange サーバーのウィルス対策／スパム対策
- エンドポイントのファイアウォールなど

ネットワーク上の全エンドポイントに関する継続的なステータス情報

ネットワーク上でマルウェアが検知された時点で、場所、感染したコンピュータ、マルウェアが起こしたアクションの詳細を含む包括的なレポートによる緊急アラートを入手します。
サービスの毎日の活動について、電子メールによるレポートを受け取ります。

SIEM 対応

Adaptive Defense 360 は、システム上で実行されるすべてのアプリケーションのアクティビティに関する詳細なデータを提供する SIEM（Security Information and Event Management）ソリューションと統合されています。
SIEM ソリューションを持たないクライアント用に、**Adaptive Defense 360** は、リアルタイムで収集されたすべての情報を分析するセキュリティイベントを保存し管理するための独自システムを組み込むことができます。

100% の運用管理

隔離作業や疑わしいファイルを処置したり感染したコンピュータの駆除や復元を行うために、技術者に投資する必要はありません。
PandaLabs のエキスパートによる継続的な監視の元で、当社ビッグデータ環境の機械学習により、**Adaptive Defense 360** がすべてのアプリケーションを自動的に分類します。

テクニカル要件

Web コンソール

- インターネット接続
- Internet Explorer 7.0 以降
- Firefox 3.0 以降
- Google Chrome 2.0 以降

エージェント

- オペレーティングシステム
  - ワークステーション
    Windows XP SP2 以降（Vista、Windows 7, 8, 8.1, 10）
  - サーバー
    Windows Server 2003、Windows Server 2008、Windows Server 2012
- インターネット接続（ダイレクト接続またはプロキシ経由）

機能制約付きサポート（EPP 機能のみ）

- Linux、Mac OS X、Android

ps-japan

PS Japan株式会社 **www.ps-japan.tokyo**

〒104-0033　東京都中央区新川1-11-8　第１小高ビル３階
TEL 03-4530-8151　FAX 03-6862-8618

©2017 Panda Security. All rights reserved.　本カタログに掲載されている会社名および商品名は、一般に各社の商標または登録商標です。本カタログ掲載の各製品の仕様などは、予告無く変更される場合があります。

PSJ004-01-17March/PDF