データシート

FireEyeエンドポイント・セキュリティ

EPP、EDR両方を実現するコンパクトなエージェントで、脅威を多角的に分析

特長

- エンドポイントを標的としたほぼ全てのサイバー攻撃に対応
- セキュリティ侵害を検知、ブロックし、攻撃の影響を軽減
- 脅威を明らかにすることで、素早い対応を実現
- 端末への影響を最小限に抑えるコンパクトなエージェント
- PCI-DSSやHIPAAなどのレギュレーションに準拠
- オンサイト、クラウドのどちらでも利用可能

シグネチャなどを用いた従来型のエンドポイント・セキュリティでは、APT攻撃（Advanced Persistent Threat）などの新しくて高度なサイバー攻撃に対応することができません。エンドポイントを安全に保つには、最新の脅威に対する迅速な解析と対応が不可欠です。

FireEyeエンドポイント・セキュリティは、従来型のセキュリティ製品のよいところを活かし、さらにファイア・アイの技術、経験、インテリジェンスを用いて機能を高めたソリューションです。

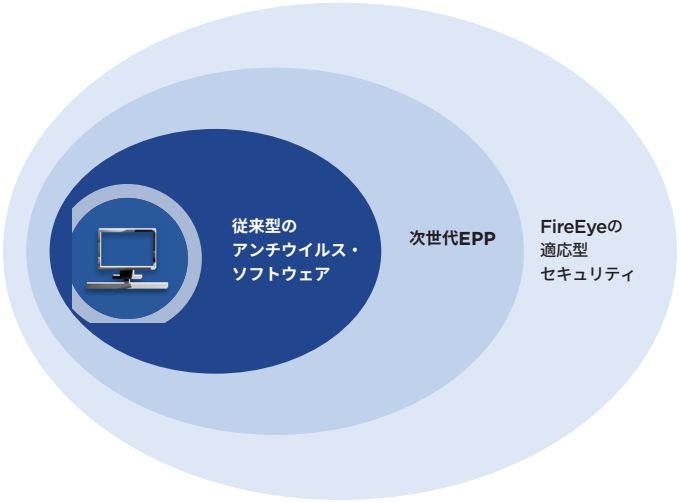
FireEyeエンドポイント・セキュリティには、4つのエンジンが搭載されています。まず、シグネチャベースのEPP（Endpoint Protection）エンジンが、既知のマルウェアを検知、ブロックします。また、サイバー攻撃の現場で収集された脅威情報を機械学習するエンジン、MalwareGuardは、シグネチャがまだ存在していない、未知の脅威に対応します。さらにEDR（Endpoint Detection and Response）機能では、振る舞い解析エンジンを用いて高度な脅威を検知します。そしてIOC（Indicators of Compromise）により、すでに侵害が発生している端末を見つけ出します。これらのエンジンが脅威に多角的にアプローチし、エンドポイントを守ります。

しかし、セキュリティ対策に「絶対」はありません。上記のエンジンのほか、業務への影響を最小限に抑える現実的な対応策として、FireEyeエンドポイント・セキュリティは以下の機能を提供しています。

- すべての端末に存在する既知/未知脅威を、僅かな時間で検索し、調査
- 侵入経路の特定
- 発生した脅威、あるいは現在進行しつつある攻撃の範囲を特定
- 侵害の侵攻を時系列と継続時間でまとめ、流れを把握
- 封じ込めが必要なエンドポイントを特定し、被害の拡大を防止

ITは大学にとって、学生たちの効率的な教育を後押ししてくれる、戦略的ツールです。FireEyeエンドポイント・セキュリティのおかげで、ITシステムをいつでも安全に利用することができます。これは、私たちのミッションを実現する上でとても重要なことです。

— James D. Perry II氏
最高情報セキュリティ責任者、米国サウスカロライナ大学



「ウイルス感染が発生してしまったら、会社はもうおしまいだ」と信じ込んでいる人が経営層には少なくありません。FireEyeにより、問題の本質を見極め、ウイルスは管理と封じ込めが可能なものであるということを証明することができるようになりました。「未知」が「既知」に変われば、誰もがプレッシャーから開放されるのです。

— Michael Hennessy氏、テクノロジー・サービス担当ディレクター、
Alpha Grainer Manufacturing, Inc

主な機能

- 複数のエンジンを搭載したコンパクトなエージェントが、脅威を効率よく検知し、ブロック
- 脅威の分析と対応を、エンドポイント・セキュリティ内で完結
- アンチウイルス機能による既知脅威の検知、機械学習システムによる未知脅威の検知、振る舞い解析によるファイルレス攻撃の検知、IOCによる影響範囲の特定など、エンドポイントに必要とされている機能を網羅
- 脅威の徹底的な調査および解析を実現（Triage Summary、Audit Viewer）

拡張的機能

- 疑わしい活動や脅威活動を迅速に発見し、詳細を把握（Enterprise Security Search）
- エンドポイントに対する詳細な検査の実施と、期間を絞り込んだ解析（Data Acquisition）
- 脅威の検索と特定、影響度の特定
- 対応を早めるために役立つ、迅速な検知、調査および封じ込め機能
- エンドポイント上で発生した疑わしい活動への素早い対応を可能にするユーザーインタフェース

サポートされるオペレーティング・システムと環境	
Windows	XP SP3、2003 SP2、Vista SP1以降、2008、Win7、2012、8、8.1、10、Server 2016
Mac	OS X 10.9以降
Linux	Red Hat Enterprise Linux 6.8+、7.2+ CentOS 6.9+、7.4+

導入形態： オンサイト利用のハードウェア・アプライアンスおよび仮想アプライアンス、FireEye Cloud Serviceなど

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 |
03−4577−4401 |
Japan@fireeye.com

会社概要

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。