エンドポイント・セキュリティ

オンサイト/リモートのエンドポイントを
未知のセキュリティ威脅およびエクスプロイトから保護

概要

高度化した今日のサイバー攻撃は、ファイアウォールやアンチウイルス・ソフトウェアなど、長年にわたり利用されてきた従来型のエンドポイント・セキュリティ対策を容易にすり抜けます。従来型の対策で既知の脅威を防御できた場合でも、攻撃の目的までは把握できません。FireEyeエンドポイント・セキュリティ（HXシリーズ）は、アプライアンスをオンプレミスで運用しながら、自社ネットワーク内外のエンドポイントを保護するセキュリティ・ソリューションです。HXシリーズには次の機能が備えられており、既知および未知のセキュリティ脅威を検知し、被害の拡大を防ぎ、攻撃の特性や目的を把握できます。

- Triage ViewerおよびAudit Viewer： セキュリティ脅威の存在を示す証拠や痕跡（インジケーター）を検査、解析
- エンタープライズ・セキュリティ・サーチ： セキュリティ脅威を迅速に検索、発見、封じ込め
- Data Acquisition： エンドポイントを詳細に検査、解析
- Exploit Guard： エンドポイントに対するエクスプロイト攻撃を検知、報告

FireEyeエンドポイント・セキュリティは、エンドポイントを攻撃する既知および未知のセキュリティ脅威を予防的に検査、解析して封じ込め、被害を最小限に抑えます。

エンドポイントの保護に脅威インテリジェンスを活用

脅威インテリジェンスは、攻撃発生の時点で利用できなければ、あまり意味がありません。HX Endpoint Detection and Response（EDR）は、他のFireEye製品が備える脅威インテリジェンス機能をエンドポイントまでシームレスに拡張する技術です。あるFireEye製品がネットワーク上で攻撃を検知した場合、その情報をエンドポイントに自動配信し、セキュリティ侵害の証拠や痕跡である侵害インジケーター（IOC）の有無をエンドポイントで検査できるようにします。

エンドポイントを詳細に可視化

アラート発生の根本原因を特定し、セキュリティ脅威の詳細解析を実施するためには、エンドポイントの可視化が欠かせません。FireEyeエンドポイント・セキュリティの履歴キャッシュ機能を使用すると、エンドポイントで発生した過去および現在のアラートを検査、解析できます。また、Triage Viewerでは、フォレンジック分析で使用するイベントのタイムラインが自動生成されます。

自社ネットワーク内外のエンドポイントを包括的に保護

オンサイトまたはリモートのどちらのエンドポイントにも、サイバー攻撃を受ける可能性があります。FireEyeエンドポイント・セキュリティは、これらすべてのエンドポイントの保護に対応しており、インターネット接続の種類を問わずインテリジェンスをプッシュ配信できます。このため、VPN接続を別途利用することなく、世界中に分散するエンドポイントを調査し、侵害を受けたエンドポイントを隔離できます。

ハイライト

- オンプレミス型のアプライアンスとエンドポイント・エージェント・ソフトウェアの組み合わせで、オンサイトおよびリモートのエンドポイントを監視
- FireEye Dynamic Threat Intelligence（DTI）により、コア・ネットワークと同等の高度な脅威対策をエンドポイントで実現
- エンドポイントを詳細に調査してタイムラインを作成、IOCを特定してセキュリティ脅威を封じ込め
- 数万台規模のエンドポイントがオンサイトやリモートに存在する場合でも、わずか数分でセキュリティ脅威を検索、検知、特定、封じ込め
- あらゆるエンドポイント活動を単一のインタフェースで効率よく検証。エクスプロイトを検知して解析し、封じ込めや対応を実施
- Common Criteriaおよび米連邦標準規格のFIPSに準拠
- 最新のアラート、システムの詳細、その他、最新情報を単一のインタフェースで把握、ホストベースのワークフローを一元化
- 重要なコンテキスト情報に基づき、既知および未知のセキュリティ脅威に素早く対応
- オンプレミス/オフプレミス、ネットワーク内外、ネットワーク・アドレス変換（NAT）の有無を問わず、すべてのエンドポイントを保護
- リモート調査を実施しながら、ワンクリックでセキュリティ脅威と侵害デバイスを封じ込め
- Audit Viewerでワークフローを強化、FireEyeエンドポイント・セキュリティ内で包括的な脅威解析を実施
- 各インシデントの特性に合わせて機能をカスタマイズ
- 複数のDMZをサポート

FireEye
SECURITY REIMAGINED

侵害を受けたエンドポイントを隔離、ネットワーク内での被害の拡大を阻止

エンドポイントから始まった攻撃は、瞬く間にネットワーク全体に広がる可能性があります。FireEyeエンドポイント・セキュリティでは、攻撃を検知した後、セキュリティ侵害を受けたエンドポイントを即座に隔離して攻撃を遮断し、被害の拡大を阻止します。しかも、一連の操作はすべてワンクリックで実行可能です。その後、感染の拡大を心配せずに、落ち着いて詳細なフォレンジック調査を実施できます。

水面下で展開されるエクスプロイト攻撃を検知

攻撃の特徴をデータベースと比較する従来型の技術であるEPP（Endpoint Protection Platform）では、エクスプロイトの検知は困難です。一方、FireEyeエンドポイント・セキュリティは、Exploit Guard機能により柔軟性に優れたデータ主導のエクスプロイト・インテリジェンスを提供します。EDR（エンドポイントの検知と対応：Endpoint Detection and Response）機能を提供するExploit Guardは、従来型のエンドポイント・ソリューションでは発見できない領域の詳細情報を収集。FireEye独自の詳細なインテリジェンスに基づいて、一見無関係な複数の活動を相関分析してエクスプロイトを検知します。

FireEyeエンドポイント・セキュリティの動作の仕組み

FireEyeエンドポイント・セキュリティは、数万台規模のエンドポイントが対象となる場合でも、わずか数分で既知および未知の脅威を検索、調査できます。FireEyeのエンドポイント・セキュリティ製品やネットワーク・セキュリティ製品、ログ管理製品が発したアラートを、Dynamic Threat Intelligence経由で相関分析します。

FireEyeエンドポイント・セキュリティでセキュリティ脅威を検証すると、次の点を明らかにできます。

- エンドポイントへの侵入に使用された攻撃経路
- 攻撃が発生、持続したのは、特定のエンドポイントに限定されているかどうか
- 他のエンドポイントにも被害が拡大した場合、そのエンドポイントの特定
- エンドポイントがセキュリティ侵害を受けていた期間
- 外部に送信されていた知的財産の有無
- 被害拡大を防止するために隔離する必要のあるエンドポイントおよびシステム

FireEyeエンドポイント・セキュリティのシステム要件

オペレーティング・システム	最小システム・メモリ（RAM）
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1以降	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2008（R2を含む）	2 GB（64ビット）
Windows 7	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2012（R2を含む）	2 GB（64ビット）
Windows 8	1 GB（32ビット）、2 GB（64ビット）
Windows 8.1	1 GB（32ビット）、2 GB（64ビット）
Windows 10	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2008～2016	2 GB
Red Hat Enterprise Linux（RHEL）バージョン6.8、7.2、7.3	2 GB

注： FireEye エンドポイント・セキュリティには、クロック周波数 1 Ghz 以上の Pentium 互換プロセッサ、300 MB 以上の空きディスク容量が必要です。サポートするオペレーティング・システムは上記のとおりです。

ハードウェア・アプライアンスの仕様

仕様	HX 4402	HX 4400D
ストレージ容量	1.8 TB 4台、RAID 10、2.5インチ	600 GB 4台、SAS、2.5インチ、フィールド交換対応
エンクロージャ	1RU、19インチ・ラックに適合	
シャーシの寸法（幅×奥行×高さ）	437×706×43.2 mm	
AC電源	冗長電源（1+1）750W、100～240 VAC	
消費電力（最大）（ワット）	313W	
平均故障間隔（時）	3万5,200時間	
重量（アプライアンスのみ）	15 kg	

注： FireEye エンドポイント・セキュリティは、クラウド経由で、または仮想 / オンプレミスのハードウェア・アプライアンスとして導入できます。1 台のアプライアンスは、最大 10 万台のエンドポイントをサポートします。

ネットワーク・レベルのアラートを元にエンドポイントに対する攻撃を検知

FireEyeエンドポイント・セキュリティは、他のFireEye導入環境との連携を通じて、潜在的なセキュリティ・インシデントに関する的確な意思決定を支援します。

詳細については、FireEyeのWebサイトをご覧ください。
www.FireEye.jp

FireEyeについて

FireEyeRはインテリジェンス主導型のSecurity-as-a-Serviceのリーダー企業です。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、インシデントレスポンスといった、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。FireEyeは「Forbes Global 2000」企業の4割以上を含む、世界67か国以上の5,800を超える組織で利用されています。

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com