All for SMB Security

総合エンドポイントプロテクション

Exosphere

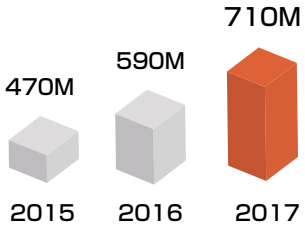
Endpoint Protection

JSECURITY

現在の脅威状況

近年のサイバー攻撃はますます洗練され、一般的なアンチウイルスなど多くのセキュリティソリューションが時代遅れになっています。さらに悪いことに、最近の高度なサイバー攻撃は、金銭の不正取得が目的となって、データ侵害が発生しています。このような攻撃は、大手企業や政府機関だけではなく、中小企業もサイバー攻撃の重要なターゲットになっています。

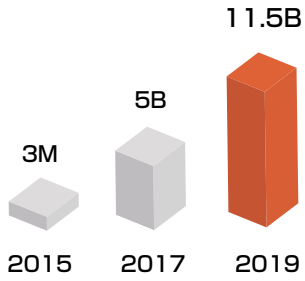
マルウェア件数



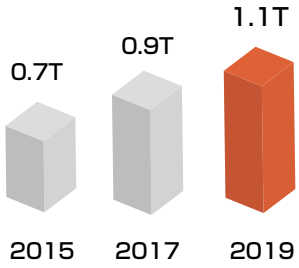
クリプトランサムウェア in 2017

*変形されたランサムウェア

ランサムウェア被害総額($)



データ被害の年間コスト($)



しかし、マルウェアは日々増加する様々な攻撃のひとつにすぎません。マルウェアにはランサムウェアのような、新たな脅威が含まれます。また調査によりますと、内部関係者による不正行為や情報漏洩も対応しなければならない重大な脅威となっています。

企業は、既知と未知の脅威と脆弱性に対応する必要があります。古いアンチウイルスだけでは、これらの脅威に対して適切に対応できません。

2017年のタイプ別のインシデント

最新の脅威パターン

進化したマルウェア

進化したマルウェアは、事前にテストして作られており、ほとんどの一般的なアンチウイルスソリューションを通過することが出来ます。このようなマルウェアには、サンドボックス回避、コマンド制御、データ漏洩などの洗練された機能が含まれています。従来のシグネチャベースのアンチウイルスは進化した高度なマルウェアを検出または停止することはできません。

情報消失

マルウェア、ランサムウェア、ヒューマンエラー、またはハードウェアの障害によってデータが消去または破損する可能性があります。 アメリカでは毎週140,000台のHDDディスクがクラッシュし、深刻な損失が発生しています。

ランサムウェア

2017年には、ランサムウェアはサイバー攻撃の重要な役割を果たしました。ランサムウェアは、企業がデジタル通貨でデータの身代金を支払うまでユーザーシステムのデータを暗号化して使用することを制限する悪質なコードの一種です。WannaCryとPetyaは、近年にグローバルパニックを引き起こした2つのタイプのランサムウェアです。

インサイダー脅威

インサイダー（内部関係者）の脅威は、外部からの攻撃よりもさらに深刻な脅威となります。従業員が、企業のデータをUSBドライブにコピーしたり、外部の者に転送したりして、ビジネスを危険にさらす可能性があります。ですからインサイダーの脅威を100%防ぐのは難しいのが現状です。

フィッシング

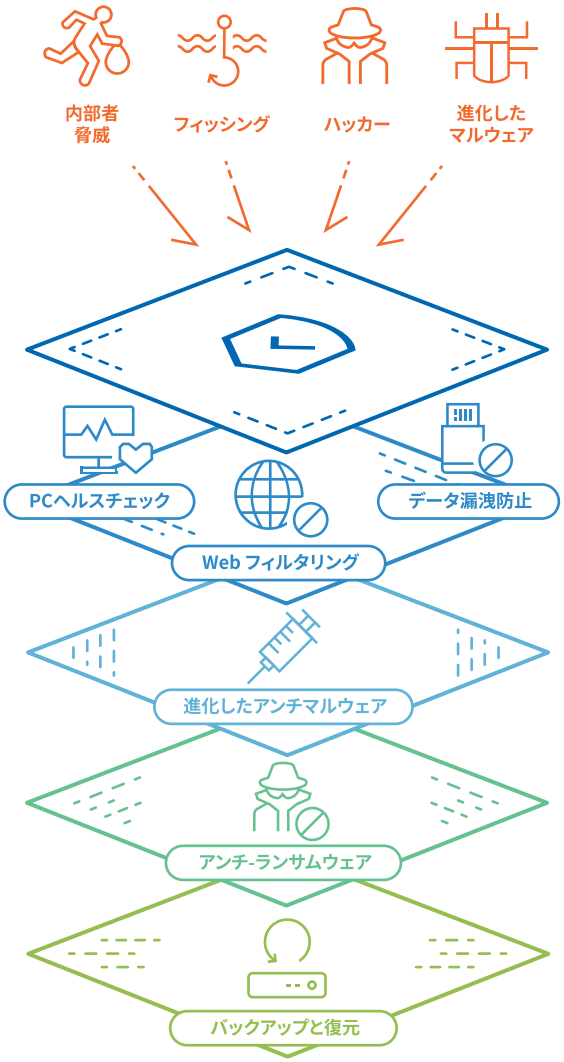
フィッシングは、サイバー攻撃の最も一般的な方法です。サイバー攻撃の90%以上がフィッシングメールです。フィッシングは電子メールを送付してWebサイトに誘導した後、ユーザーアカウント情報を騙し取ります。また、悪意のある実行ファイルを添付し、実行された場合ユーザーのアカウント情報を盗み取り、組織に侵入します。

PCを最新の状態に

最後に、セキュリティの最も重要なポイントの1つは、PCが最新のセキュリティ状態を保つことです。 Gartnerによると、サイバー攻撃の0.1%未満は未知の脆弱性を使用します。 言い換えれば、OSシステムやアプリケーションの既知の脆弱性にパッチを当てることで、攻撃の99.9%を防ぐことができます！ですから、常にシステムを最新に更新し、ファイアウォールやマルウェア対策ツールの実行を確実にすることが重要です。

Exosphere™
総合エンドポイント プロテクション

Exosphere（エクソスフィア）エンドポイント保護エージェントは、すべての脅威に対してシンプルなオールインワンの対策案を提供します。複数の種類の保護を階層化して企業内外の様々な脅威からビジネスを守ります。一つの管理画面から管理者はPCとデータを保護するためのあらゆる面のセキュリティを設定し、管理することができます。これにより、複数のセキュリティソリューションを導入する場合に発生するコストと管理費用が削減されるので小規模な企業にも包括的な解決策が提案できます。



Exosphereの機能

進化したマルウェア対策

Exosphereは進化した高度なマルウェア対策エンジンを使用してファイルをリアルタイムでスキャンします。エンジンは、シグネチャベース、経験蓄積およびエミュレーション方法を適用する多層検出を提供します。Exosphereのアンチマルウェアエンジンは5億5千万以上のエンドポイントから収集された脅威情報から迅速に更新します。

データ漏洩防止

Exosphereは、従業員の機密情報共有を制御する様々な機能を提供します。 ユーザーのPCデータ検出、USBデバイス遮断、ファイル転送および印刷ドキュメントに透かしマーク追加などの機能が含まれています。

Webフィルタリング

Exosphereの最初の防衛ラインはWebサイトのフィルタリングです。Exosphereは、1億4千万以上のWebサイトURLデータベースを使用して、従業員がマルウェアやフィッシングに使用される可能性のある危険なWebサイトへアクセスするのを防ぐことができます。 管理者は、10個のURLカテゴリ別にアクセスを許可することができますので、生産性の改善やリスクを低減することができます。

アンチ-ランサムウェア

Exosphereアンチ-ランサムウェアは信頼できないアプリケーションやプロセスのファイルアクセスを遮断してデータを保護します。そうすることによって　ランサムウェアが浸透していたとしてもランサムウェアがファイルにアクセスし上書きすることができなくなります。

PCヘルスチェック

約0.1%の脅威は未知の脆弱性を悪用します。したがって、OSシステムと重要なアプリケーションを最新の状態に保ち、構成が正しいことを確認することがシステムの侵害を防ぐ最善の方法です。ExosphereはPCをスキャンしてパッチ処理を自動化し、設定を確認して既知の脅威を止めることができます。

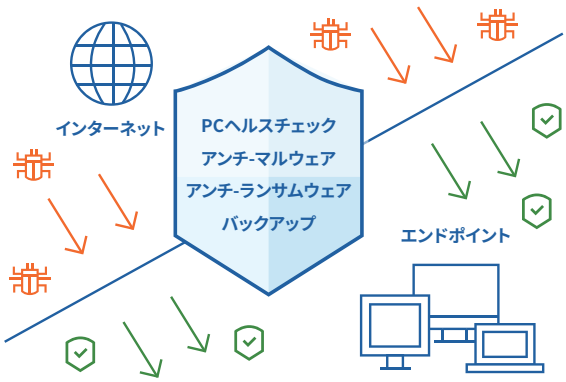
バックアップと復元

Exosphereは最終防衛策としてファイルのバックアップを行います。 ランサムウェアまたは悪意のあるコードから被害が発生したとしても破損したユーザーデータをバックアップから復元することができます。 バックアップストレージは効率性とセキュリティを確保するために暗号化、重複排除されます。

使用事例

ランサムウェア対策

最近話題になった「WannaCry」では150カ国の23万台以上のコンピュータが感染しました。これは既知のWindows脆弱性を悪用して広がっていました。感染したPCのファイルを暗号化し身代金としてBitcoinを要求しました。

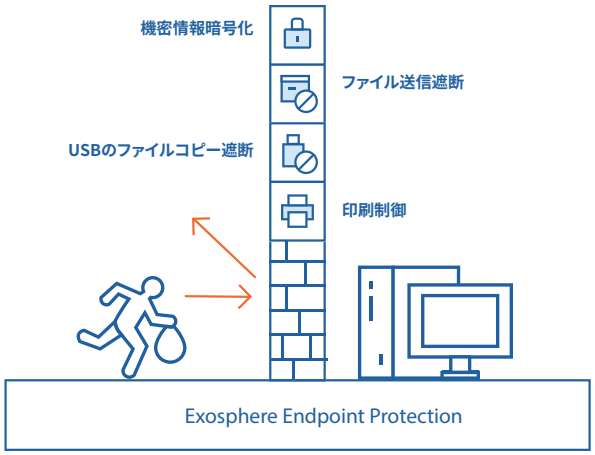


Exosphereの堅牢な防御機能はこのような攻撃から守ります。

PCヘルスチェック	PCヘルスチェックが設置されている場合、OSに定期的にパッチを適用し最新の状態に保つため、既知の脆弱性を悪用するWannaCryや他のランサムウェアからPCを守ります。
アンチ-マルウェア	進化したアンチマルウェアは、脅威が見つかった時、即時に対処します。
アンチ-ランサムウェア	Exosphereのアンチ-ランサムウェア機能は、WannaCryのようなランサムウェアがユーザーデータに不正アクセスできないようにデータファイアウォールを実装します。
バックアップ	全ての防衛、対策が無効化された場合でもランサムウェアからユーザーファイルを保護する対策としてExosphereはバックアップ機能を提供しますので、簡単にデータを復元することができます。

悪意のある内部関係者から知的財産を保護

近年、多くの企業の知的財産漏洩事件が相次ぎました。CADファイルや製品仕様などの機密情報がUSBデバイス、電子メール、またはオンラインクラウドサービスを介して漏洩しました。



Exosphereは、このような課題に簡単に対処できます。

機密情報の検出と保護	Exosphereはすべてのユーザーデバイスをスキャンして、機密文書（例えば、CADファイル、クレジットカード情報などが含まれたファイル）を検出し、自動暗号化することができます。
USBデバイスを遮断	USBストレージデバイスを使用して大量のデータを会社外に持ち出すことができます。Exosphereは機密データ（またはすべてのファイル）が含まれたファイルをUSBデバイスへコピー、移動を制限するデバイス制御ポリシーを適用することができます。このポリシーは、すべてのユーザーまたは特定ユーザーグループに適用することができます。Exosphereは、USBデバイスに移動された機密情報ファイルを自動的に暗号化することもできます。

ファイル転送遮断	ファイルは電子メール、メッセンジャーまたはオンラインサービスを介して転送されることがよくあります。Exosphereは、これらすべてのファイル転送を遮断することができます。業務上ファイルの転送が必要な場合は管理者に転送許可を要求することができます。
不正印刷防止	Exosphereは、印刷文書に透かしマークを適用することができます。また、印刷遮断設定など会社のポリシーに従って制御ポリシーを適用することができます。

最後に

ビジネスにとって最終的に最も重要なことはデータのプライバシーと完全性を保護することです。 マルウェアなどの単一の脅威に対応するだけでは十分ではありません。 各脅威に個別対応するためには多くのコストとリソースが必要になり、小規模な組織には実用的ではありません。Exosphereは進化した高度なマルウェア対策機能とデータ保護機能を提供しビジネスを安全に保つことができるソリューションを提供します。

Exosphere

Exosphereは、複数のサイバー脅威からあなたのビジネスを守ることに専念しています。 私たちの使命は、最適化されたエンドポイント保護ソリューションを提供し、お客様のビジネスを安全かつ効果的に改善することです。

Exosphere × amazon.com web services

Exosphere

“エンドポイントを保護して
あなたのビジネスを安全に守ります”

getExosphere.com

日本総代理店

JSECURITY

株式会社 JSecurity

東京都港区東新橋二丁目12番1号 PMO東新橋7階
TEL:03-6826-1915　FAX: 03-6826-1916
E-mail : sales@jsecurity.co.jp

URL : https://www.jsecurity.co.jp

お求めは信頼の