F-SECURE ELEMENTS

より柔軟に、よりシンプルに
必要な機能をひとつにまとめたセキュリティプラットフォーム

今日のビジネス環境は急速に、しかも絶え間なく変化しており、これはサイバー脅威についても同じです。あらゆる業界で企業がクラウドに移行し、新しいデジタル的な働き方を模索する中、攻撃対象領域は拡大しており、攻撃者はさらに高度かつ効率的な方法でこの状況を悪用しようとしています。

新しい脅威に対応するために多くの企業で採用されている手法は、単一の機能を持つ個別のテクノロジーやソリューションを複数のベンダーから調達し、それらを組み合わせて複雑なソリューションを構築することです。このように単機能のツールを複雑に組み合わせる場合、運用が大変になるだけでなく、セキュリティホールを残してしまう危険性があります。

- これらのソリューションの多くは、効果的に運用するために非常に高度な（そして希少な）スキルを必要とします。
- これらのような単機能のソリューションは、相互に補完し合ったり、データを共有したりすることはありません。そのため、データのサイロ（孤立）化と検知機能の制限を引き起こす可能性があります。

F-Secure Elementsは、ビジネス環境と脅威ランドスケープの変化に柔軟に対応できる、オールインワン型のセキュリティプラットフォームです。これは一体化されたクラウドネイティブなプラットフォームでもあり、セキュリティバリューチェーンの重要なすべての領域（エンドポイント保護、エンドポイントにおける検知と対応、脆弱性管理、Microsoft 365保護）をカバーしています。相互補完的な個別のテクノロジーを選択することも、すべてのセキュリティ対策を有効化しシームレスに利用することもできます：お客様のニーズにあわせて、必要なソリューションを必要な時だけ使用ください。

- **単一の管理画面：**比類のない可視性と全体的な状況認識能力を提供します。
- **シームレスな統合：**すべてのソリューションは単一のデータレイクを共有し、複数の攻撃経路を相互に関連付け、卓越した検知能力を実現します。
- **F-Secure Elements Security Center：**単一の統合コンソールですべてのソリューションを一元管理し、運用を効率化します。
- **クラウドネイティブなプラットフォーム：**ハードウェアやミドルウェアは必要ありません。クリックするだけで導入できます。
- **各ソリューションをフルマネージドサービスまたはセルフマネージプラットフォームとして利用可能：**エフセキュアのパートナーと協力、または社内で管理するかを選択できます。どちらを選んでも、エフセキュアがバックエンドからお客様をサポートします。

F-Secure Elementsの特長

フレキシブル、モジュラー化、スケーラブル

個々の機能を別々に選択して利用することも、ワンクリックで完全なスイートにアップグレードすることもできます。

オールインワンで必要な機能をひとつに

最先端の保護技術を統合し、セキュリティバリューチェーンの全体に適用することで、リスクを最小限に抑えます。

高い状況認識能力

高度で複雑な攻撃の点と点を結びつけ、状況を意味と共に可視化します。

強化された対応

エンドポイントとクラウドにおける複数の攻撃経路を横断して対応します。

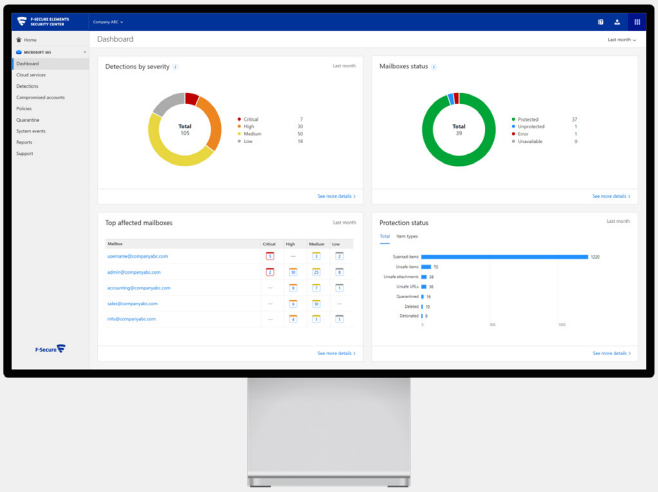
シンプルな管理

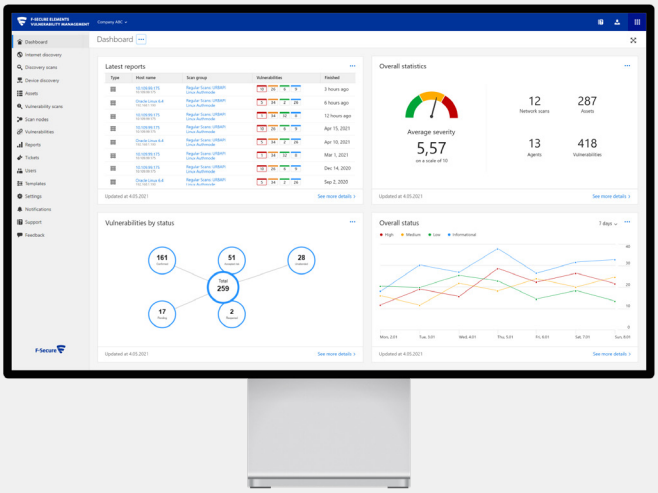
簡素化された集中管理により、生産性を向上させます。

クラウドによる軽量化

クリーンなクラウドネイティブの実装により、導入時間と運用コストを削減します。

F-Secure





F-Secure Elementsは、すべての機能がシームレスに連携しているオールインワン型プラットフォームです：

- **自動パッチ管理**により、脆弱性に起因する侵害を阻止します。
- 優れた脅威ハンターによる24時間365日のオンデマンドサポートを含むガイダンス付きの自動対応オプションにより、最も高度な脅威を**迅速かつ明敏に検知**します。
- 最新のマルウェアやランサムウェアから**プロアクティブに保護**します。
- リアルタイムの脅威インテリジェンスと分析を活用し、新たに出現した脅威を数分以内に特定します。
- **攻撃対象領域と攻撃経路を完全に可視化**します。
- Microsoft 365環境向けの**高度なクラウドセキュリティ**を提供します。

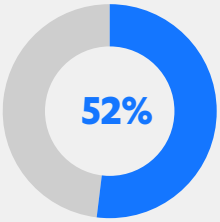
F-Secure Elements Endpoint Protection

最新のマルウェアやランサムウェアに対抗する先進的エンドポイント保護

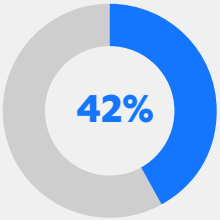
攻撃者は、ネットに接続されたデバイスを常にスキャンして、パッチが適用されていない脆弱性を探しており、チャンスを見つければそれを逃しません。ほとんどのサイバー脅威は、最新の脆弱性パッチを迅速かつ漏れなく適用し、効果的なエンドポイント保護ソリューションを活用することで防ぐことができます。

F-Secure Elements Endpoint Protectionは、ランサムウェアや未知のマルウェアによるゼロデイ脆弱性の侵害を阻止するために、自律的な保護を提供します。モバイル、デスクトップ、ノートブック、サーバーをカバーする包括的なセキュリティを実現し、その優れた正確性によりビジネスの中断を最小限に抑え、復旧に必要なIT作業も少なくすることができます。アラートのフィルタリングと高度な自動化によって最大効率が実現できるため、重要な作業のために貴重な人的リソースを割当てることができます。

- **自律的な保護**は24時間365日稼働するため、人手による作業や専門的な知識はほとんど必要ありません。
- ヒューリスティックおよび行動分析、高度な機械学習、リアルタイムの脅威インテリジェンスを使用して、**未知の脅威やエクスプロイトに対抗**します。
- パッチ管理を完全に自動化し、**セキュリティパッチがリリースされた際はすぐに適用**します。
- ペネトレーションテスターが作成したルールまたは管理者が定義したルールに従って、**アプリケーションとスクリプトの実行を阻止**します。
- 悪意のあるWebサイトへのアクセスなど、**ユーザーがオンラインの脅威に騙されることを阻止**します。
- DeepGuardおよびDataGuardテクノロジーを使用して**ランサムウェアを検知し、データの破壊や改ざんを阻止**します。
- ハードウェアデバイスを介してシステムに**脅威が侵入したり、データが流出したりすることを阻止**します。
- 不正なアプリケーションが**許可なくファイルやシステムリソースにアクセスすることを阻止**します。



52%の企業が、過去2年間にデータ侵害を経験しました。



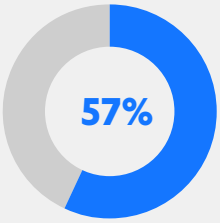
2020年に起きたデータ侵害の42%は、パッチが存在するにも関わらずそれらが適用されていなかったために発生しました。

F-Secure Elements Endpoint Detection Response

標的型攻撃を阻止するEDR

サイバー脅威の影響を受けずに済む人は誰もいませんし、脅威を完全に阻止することも不可能です。現代の最も高度な攻撃は、最も強力な予防的制御さえも回避することができるのです。また、これらの攻撃は見逃されやすいため、攻撃者は大混乱を引き起こしたりデータを侵害したりするための時間を十分に確保することができます。

F-Secure Elements Endpoint Detection and Responseは、業界をリードする検知機能を備え、高度な標的型サイバー攻撃に対抗します。企業の回復力を維持し、すぐに役立つインサイトとわかりやすいガイダンスにより、迅速にコントロールを取り戻すことができます。



57%の企業は、どの脆弱性が最もリスクが高いかを理解していません。

F-Secure

- エンドポイントで何が起こっているかを、**リアルタイムに可視化**します。Windows、macOS、Linuxを横断したテレメトリを提供します。
- Broad Context Detectionにより、**脅威を迅速かつ正確に検知**します。一見無害に見えても、疑わしい行動はすべて見つけ出します。「アラート疲れ」を起こさせません。
- イベントの検索とフィルタリングにより、**脅威を効率的に捕捉**します。
- シンプルな可視化により、**イベント間の関連を把握**します。
- リスクベースのホスト隔離を含む**自動対応アクションにより、迅速に脅威に対応**します。
- **攻撃を封じ込め**るためにわかりやすく実用的なガイダンスを提供し、解決が難しい場合にはエフセキュアの脅威ハンターに24時間365日体制でエスカレーションできるオプションを提供します。
- 侵害から72時間以内の報告を義務づけている、PCI、HIPAA、およびGDPRの**規制要件を満たすことができます**。

F-Secure Elements for Microsoft 365

フィッシングおよびメールベースの脅威からMicrosoft 365を保護

現代はデータの黄金時代です。ビジネスメールには機密情報が大量に含まれており、Microsoft SharePointのようなクラウドストレージは企業の知的財産の宝庫です。そしてビジネス用のメールアカウントは、多くの場合複数のビジネス上重要なアプリケーションと連携しています。ユーザーのクレデンシャルが攻撃者の手に渡ることは、なりすましや企業システムの侵害を引き起こすことを意味するのです。

Microsoft 365は、世界で最も使われているEメールサービスです。そのため攻撃者は、Microsoft標準のセキュリティをすり抜ける方法を見つけ出そうとしています。Microsoftが提供するEメールセキュリティ機能は基本的なもので、高度な攻撃や高度なフィッシングに対抗するための防御機能としては十分ではありません。

F-Secure Elements for Microsoft 365は、Eメール、カレンダー、タスク、およびSharePointにおけるMicrosoft標準のセキュリティ機能を強化し、高度なフィッシング攻撃や悪意のあるコンテンツから保護します。この高度な検知機能には、受信トレイの異常検知とEメールアカウントの侵害検知が含まれます。このクラウドネイティブなソリューションはMicrosoft 365のために専用に設計されており、Elementsエンドポイントセキュリティソリューションをシームレスに拡張したものです。

- 多階層のアプローチにより、**コスト効率の良い事業継続性を実現**します。
- エンドユーザーがどのデバイスからアクセスしてくるかに関係なく、**持続的な保護**を提供します。保護が中断したり、Eメールゲートウェイが停止したりすることはありません。
- エンドポイントとクラウド全体を統合したセキュリティ管理により、**ワークフローを効率化**します。
- クラウド間のシームレスな統合のおかげで、**簡単に導入**することができます。ミドルウェアのインストールや煩雑な設定などは必要ありません。
- マルウェア、ランサムウェア、フィッシング詐欺などの**悪意のあるコンテンツを阻止**します。
- 疑わしいファイルを隔離されたサンドボックス環境で実行して分析することにより、**最も高度なマルウェアでさえも検知**することができます。
- **ビジネスアカウント**が侵害されたかどうかを、「何が」「何時」「どのように」「どれくらいの深刻度で」という包括的な情報と共に検知します。
- **受信トレイの信頼性を高め**、悪意のある転送ルールなどの異常な行動を検知します。
- 自動スキャンで**効率を高め**ます。

プラットフォームの特長：

エンドポイントとクラウドサービスを保護

マルウェアとランサムウェアを阻止

脆弱性の発見とパッチの適用

脅威を検知してハント

Microsoft 365でフィッシングや高度な脅威を阻止

侵害されたビジネスアカウントの検知

自動化とガイダンスおよび24時間365日のサポートで攻撃に迅速に対応

F-Secure

F-Secure Elements Vulnerability Management

重要なシステムを安全に保つために 脆弱性を管理

ビジネス向けのIT環境はダイナミックで複雑であり、攻撃対象領域は拡大する傾向にあります。攻撃者はパッチが適用されていないシステムを侵害して、貴重な情報に不正にアクセスできるチャンスを常に探しています。新しいセキュリティパッチは毎日のようにリリースされており、それらを迅速かつ確実に適用する事は、データを保護し事業継続性を維持するために重要です。サイバーセキュリティ体制の強化は、IT資産と構成を知ることから始まります。

F-Secure Elements Vulnerability Managementは、企業が持つIT資産を把握し、それらに内在する脆弱性、および最も重大なセキュリティホールがどこにあるのかを正確に特定することで、攻撃対象領域とリスクを最小限に抑えることができます。攻撃者よりも早く、社内および社外の脆弱性を見つけてください。

- すべての資産、システム、アプリケーション、およびシャドウIT全体を**包括的に可視化**し、正確にマッピングします。
- 脆弱なマネージドおよび非マネージドシステム、ソフトウェア、および設定ミスを特定することにより、**攻撃対象領域を削減**します。
- インシデントが発生する前に予測的および予防的措置を講じることにより、**リスクを軽減**します。
- 計画的な自動スキャンにより、**ワークフローを効率化**します。組み込まれたリスク評価機能を使用して、修復に優先順位を付けます。
- Windowsエンドポイントエージェントを使用して、**脆弱性スキャンをネットワーク外のリモートデバイスにも適用**します。
- セキュリティ態勢やリスクに関するレポートで、事業継続性の**価値を明らかにし、正当性を証明**します。
- PCI ASV認定の脆弱性スキャンソリューションとカスタマイズされたレポートにより、**コンプライアンス要件を満たし**ます。

「私たちはSIEMソリューションではなく、エフセキュアのソリューションを選択しました。それは、機械学習ベースのアプリケーション行動検知システムが誤警報の量を大幅に減らし、分析と意思決定をはるかに容易に行えるアラートを提供してくれるためです。」

Jeovane Monteiro Guimarães, IT Supervisor, Móveis Itatiaia

私たちは、他のどの企業よりもサイバーセキュリティを知っています。
調査・研究を主導とするアプローチでサイバー犯罪と戦ってきた30年の経験があり、
それは独立した第三者機関が評価する確かな実績によって証明されています。

PCI　MITRE | ATT&CK　AV-TEST AWARD BEST PROTECTION

f-secure.com/elements | twitter.com/fsecure | linkedin.com/f-secure

エフセキュア株式企業
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.f-secure.com/

F-Secure