Microsoft

Microsoft 365 Enterprise で実現する
セキュリティ & コンプライアンス

Microsoft Security Solution

Microsoft Security は、人々とデータをサイバー脅威から保護するための力となり、安心をお届けします

企業を狙うサイバー攻撃はその数だけでなく、巧妙さも上昇しています。急速にテクノロジ導入が進み、ハイブリッド ワークが増加していますが、予算の制約やセキュリティ専門の人材不足という悩みを持つ組織にとってはリスクが増大します。また、マルチクラウドの利用増加や多様な規制環境への対応が求められており、組織はこれまで以上に厳しいセキュリティの課題に直面しています。

*1「Cyber Resilience」、2021 年 5 月、Microsoft Security Insider　*2「The State of Ransomware 2021」、Sophos、2021 年 4 月

マイクロソフトが提供する業界最高レベルのセキュリティ

監視
140 以上 *4
脅威グループの数
40 以上 *3
国家主導グループの数
全世界の数十億のお客様にサービスを提供して学習し、今後の動向を予測

65 兆 *5
分析
1 日に分析される脅威シグナルの数

370 億 *5
ブロック
1 年にブロックされるメール脅威の数

200 億ドル *3
今後 5 年間の投資
知識の向上と共有、インサイトの獲得、サイバー犯罪への対応に向けた投資

時間とリソースを節約しながら、お客様のセキュリティを確保

60%↑
マルチベンダーのセキュリティ ソリューションと比較した場合の平均コスト削減率

1.5 万 *3
セキュリティ エコシステムのパートナーの数

86 万 *5
自社を保護するためにマイクロソフトのセキュリティを選んだお客様の数

全世界で信頼され、組織のマルチクラウドおよびマルチプラットフォーム インフラストラクチャを保護

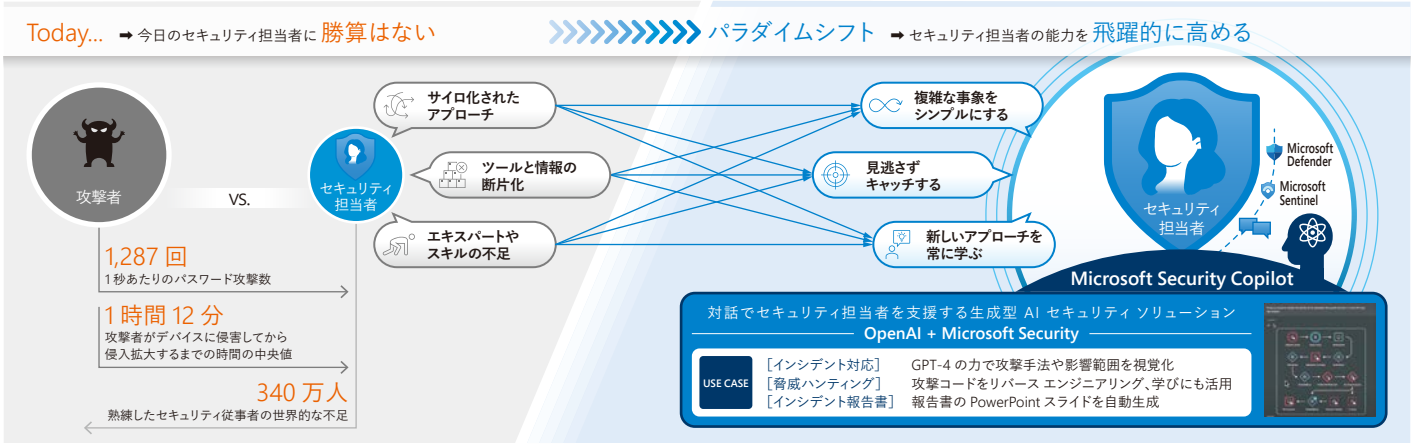
*3 決算プレス リリース、22 年度第 4 四半期 2022 年 7 月 26 日、マイクロソフト IR
*4 決算プレス リリース、22 年度第 2 四半期 2021 年 12 月 16 日、マイクロソフト IR
*5「Microsoft Security が新たなマイルストーンに到達 — インクルーシブで顧客志向のソリューションが成果をもたらす」、Microsoft Security ブログ

Microsoft の XDR - Microsoft 365 Defender

エンドポイント (EDR) やネットワーク (NDR) だけでなく、組織の ID、クラウドアプリ、メール、ドキュメント、インフラ、クラウド プラットフォーム、IoT のすべてにわたって、脅威検知と対処の機能を統合的に提供します。

Microsoft Security Copilot

Microsoft Security Copilot は、マイクロソフトの膨大な脅威インテリジェンスと業界をリードする専門知識を組み合わせ、使いやすい AI アシスタントを通じてセキュリティ専門家を支援します。



包括的なセキュリティ機能で、人、データ、インフラストラクチャの安全を守る Microsoft Security

Microsoft Security は、セキュリティ、コンプライアンス、ID、管理、プライバシーの機能をひとつに集め、マルチクラウドおよびマルチプラットフォーム、エンドポイント、デバイスを含めたエンドツーエンドを効果的に保護します。Microsoft Security による包括的なセキュリティへのアプローチは、比類なき可視性、自動化、インテリジェンスをお客様に供与し、次の 4 つを実現する能力を提供します。

あらゆるものを保護

組織全体を安全に守る統合型のビジネス セキュリティ ソリューションです。さまざまなプラットフォームやクラウド環境を横断して機能するように作られています。

複雑なものをシンプルに

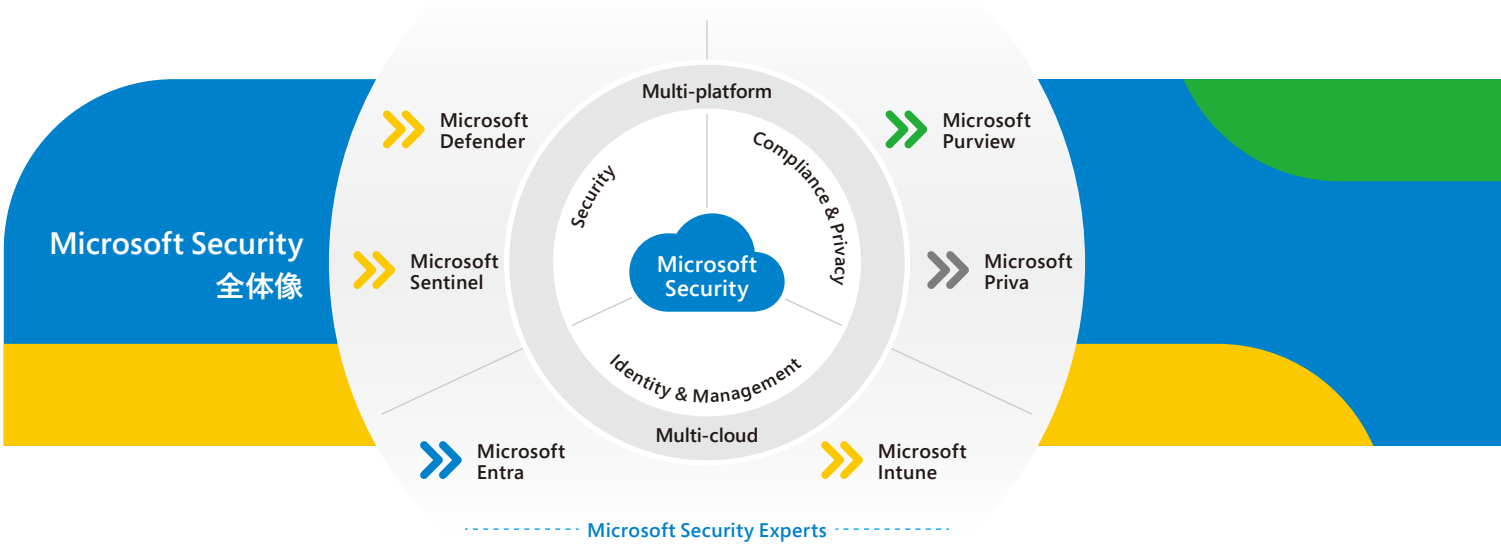
リスクの優先度付けを適切に行うための統合管理ツールは、組織内のエキスパートが持つ知識と経験を最大限に活用するように作られています。

他が見逃すものもキャッチ

先進的な AI、自動化、エキスパートの知識が、組織の脅威をすばやく検出し、効果的に対応し、セキュリティの状態を強化するのに役立ちます。

組織の未来をさらに広げる

包括的なセキュリティ ソリューションで得られる安心感は、組織のビジネスの成長、創出、イノベーションの自由につながります。



Microsoft Security を構成する製品サービス (2023 年 8 月時点)

ID & アクセス制御

Microsoft Entra

接続された世界への安全なアクセス

Microsoft Entra は、マイクロソフトの ID およびアクセス製品の新しい製品ファミリの名称です。Microsoft Entra により、マルチクラウド ID およびネットワーク アクセスのソリューションを使って、すべての ID を保護しながらリソースに対するアクセスのセキュリティを維持することができます。

多要素認証

強力な認証によるユーザー ID の検証

- 多要素認証は、サインイン プロセスに保護レイヤーを追加することで、ID 攻撃の 99.9% を防止
- アカウントやアプリにアクセスする際に、指紋のスキャンや電話で受信したコードの入力など、追加の ID 検証によって強力なセキュリティを実現
- Microsoft Entra ID (旧 Azure AD) は、テキスト、通話、生体認証、ワンタイム パスコードなど、さまざまな柔軟な多要素認証方式を提供

パスワードレス認証

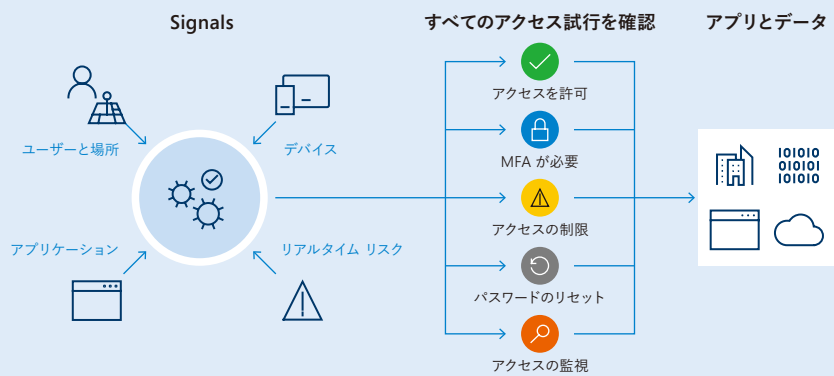
標準でパスワードなし認証を利用

- パスワードを使用せずに、一連のユーザーアクションで認証を完了
- 本人確認 + デバイスのユニークな組み合わせを要素として利用
- 利用するデバイスに PIN を設定し、第三者のなりすまし利用を防ぐ
- Windows Hello for Business では、デバイスの TPM と証明書を利用して認証
- Microsoft Authenticator では、アプリを介したワンタイム パスコードを使って認証
- FIDO2 セキュリティ キーでは、FIDO2 対応デバイスを使用して Microsoft Entra ID アカウントで Windows にサインイン可能

条件付きアクセス

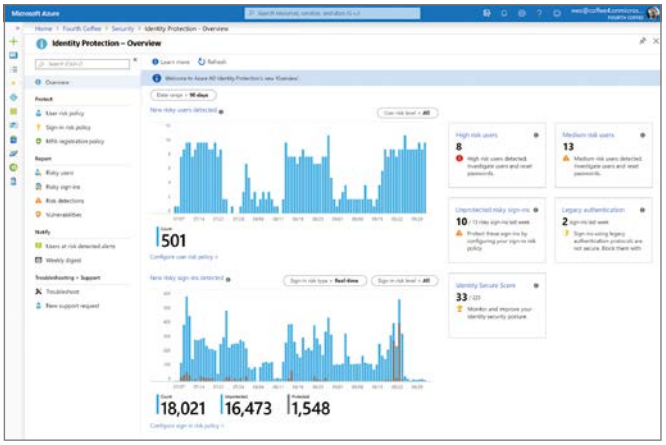
強力な認証と適応型ポリシーによるゼロトラストの実現

- コンテキストに応じたユーザー、デバイス、場所、セッションのリスク情報に基づいてアクセス ポリシーを柔軟に調整
- 多要素認証、利用規約、アクセス制限などの追加要素を使用して、アクセスの許可、拒否、制御するかどうかを決定可能
- 機械学習を使ったシグナル分析により、アクセスの許可、制限、ブロック、追加の検証手段など、アクセスを申請するための適切なポリシーを決定



ID の保護

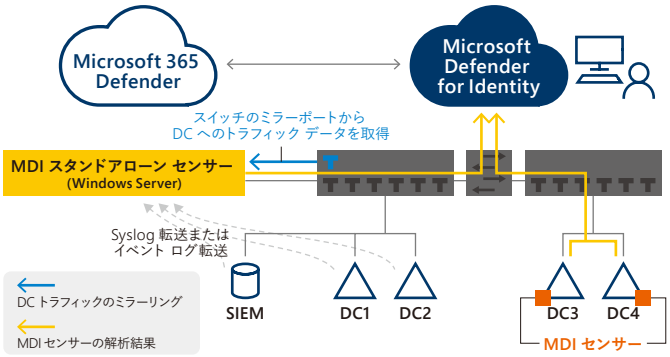
侵害されたアカウントを インテリジェントに検出して対応



- 環境内の疑わしいユーザーやサインインの動作を 24 時間 365 日通知
- 特定のしきい値を超えるサインインを自動的にブロック、一般的な対応シナリオを自動化
- 危険なユーザーとサインインを調査して、潜在的な脆弱性に対処
- アラートを他の Microsoft ソリューションと関連付けて、より詳細な調査と対応も可能

Microsoft Defender for Identity

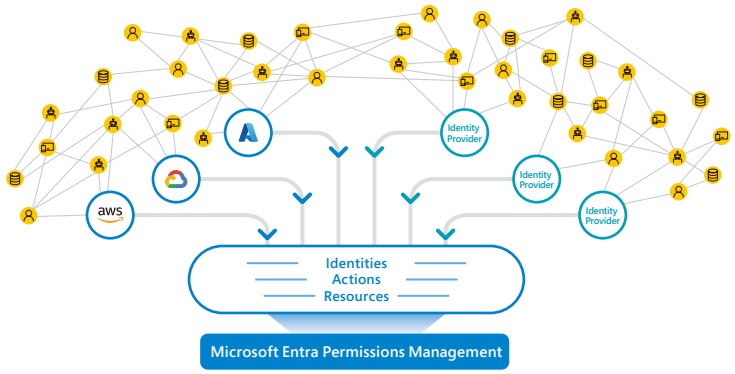
オンプレミスの ID の保護に役立つ クラウド インテリジェンス



- クラウド サービスのため、管理サーバーの設置や更新作業が不要に
- 機械学習によって通常時と異なる認証フローや関連する異常行為を検出
- ID のセキュリティ状態の評価をスコア表示することで、脆弱性を可視化して攻撃を未然に防止
- リアルタイムの分析とデータ インテリジェンスが脅威に優先順位を付け表面化、より迅速な検出と真の脅威への注目を支援
- ドメイン コントローラーに MDI センサーを導入した場合は、オンプレミス環境へのサーバー設置は不要
- ポート ミラーリングを行う場合は、MDI スタンドアローン センサー サーバーを設置 (オンプレミスにサーバーが必要)

Permissions Management

セキュアなマルチクラウド アクセス許可



- Permissions Management は、すべての主要なクラウド サービス プロバイダーと連携し、マルチクラウドにおける権限管理の合理化と迅速なリスク検出を実現
- 包括的かつ詳細な可視性を取得することでセキュリティ体制を改善し、最小特権の原則を適用し、ゼロトラスト セキュリティを強化
- 簡単な操作で過剰な権限や未使用の権限を適切なサイズに調整可能、オンデマンドでのアクセス許可にも対応
- アクセス許可の誤用や悪意ある操作によって引き起こされるデータ侵害を、疑わしいアクティビティを警告する異常値などによって防止

外部ID の効率的な管理と Verified ID

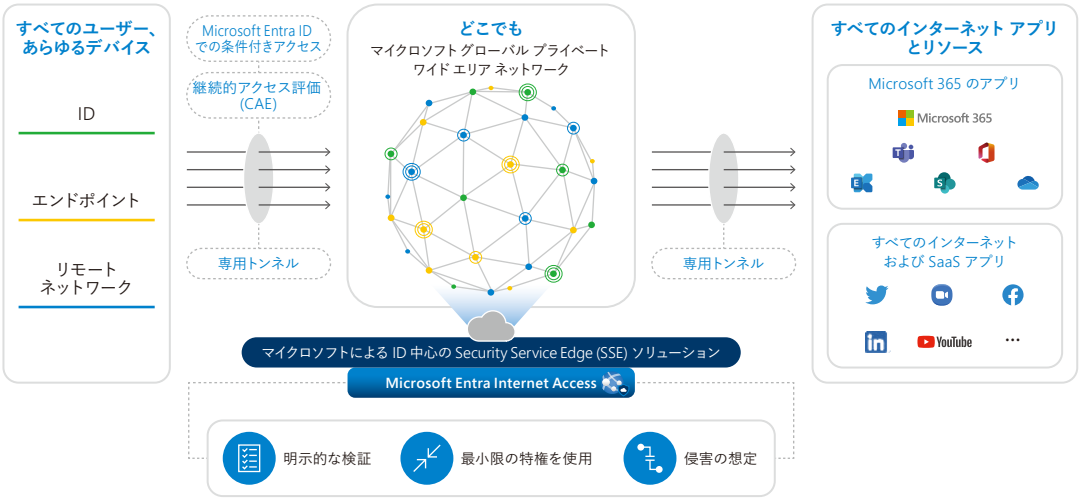
従業員、パートナー、顧客に安全なアクセスを許可

- Microsoft Entra ID External Identities は、自社の企業データの管理を維持しながら、リソースまたはアプリを組織外のユーザーと共有できる一連の機能を提供
- Verified ID は、セルフサービス機能や迅速な資格情報のチェックなどにより、プライバシーを尊重しながら、より安全で確実な本人確認プロセスを実現

Microsoft Entra Internet Access プレビュー

ID 中心の Secure Web Gateway (SWG) ソリューション

- すべてのインターネット、SaaS、Microsoft 365 アプリへのアクセスを保護し、ID 中心のセキュア Web ゲートウェイ (SWG) を使用して悪意のあるインターネット トラフィックから保護
- すべてのアクセス制御を 1 つの統合された条件付きアクセス ポリシー エンジンに一元化
- 条件付きアクセスの ID、場所、デバイスの制御をネットワーク セキュリティ スタック全体にシームレスに拡張
- 継続的アクセス評価により、ネットワーク ポリシーはユーザー リスク スコアやデバイス コンプライアンス ステータスなどの変化する条件に動的に適応可能
- Windows クライアントのサポートから段階的に他の OS をサポート予定



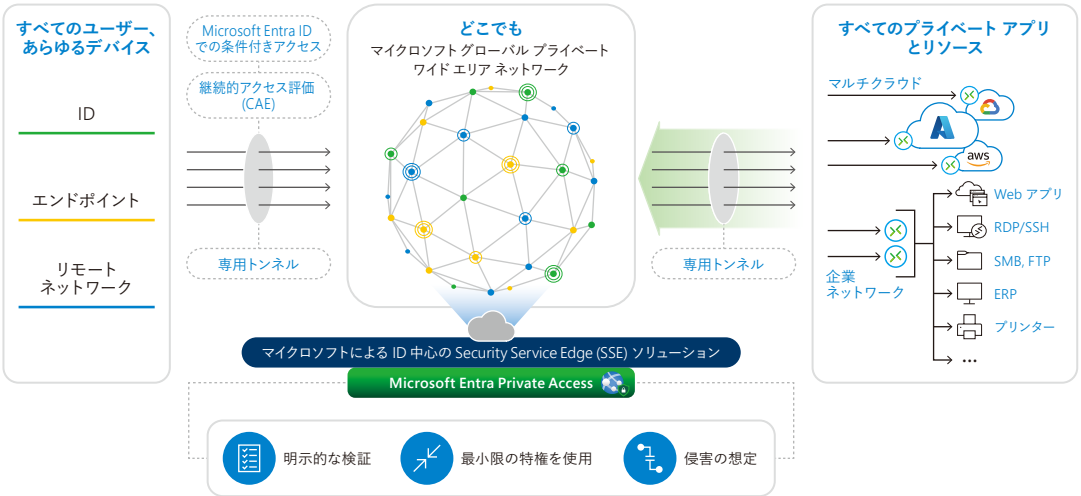
Microsoft Entra Private Access 一部プレビュー

ID 中心の Zero Trust Network Access (ZTNA)

- ゼロトラストの原則に基づく構築によって、従来の VPN のリスクや運用の複雑さを排除してユーザーの生産性を向上
- RDP、SSH、SMB、FTP などを含むすべてのTCP / UDP に対応し、すべてのプライベート アプリへの安全なアクセスを提供予定
- 条件付きアクセス ポリシーを使用してアクセスを制御、継続的アクセス評価でアクセスの取り消しも可能に

(2023 年 8 月時点ではプライベート Web アプリについてはすでに利用可能)

- セグメント化されたアプリ アクセスにより、従来の VPN のように完全なネットワークではなく、特定のアプリへのアクセスを有効化
- インテリジェントなローカル アクセスにより、企業ネットワーク内でもリモート接続でもゼロ トラスト ネットワーク アクセスを実現



エンドポイント デバイス管理

Microsoft Intune

すべてのエンドポイントを把握できる統合ソリューション

Microsoft Intune は、クラウドおよびオンプレミスで、データを安全に保つために不可欠な管理機能を提供します。モバイル デバイスをはじめ、デスクトップ コンピューター、仮想マシン、組み込みデバイス、サーバーを管理および監視するためのサービスとツールが含まれており、ゼロ トラスト戦略の実装を支援します。

モバイル デバイス管理 (MDM)

多様なプラットフォームへの対応と柔軟なデバイス管理

- Windows、Android、Android Enterprise、iOS/iPadOS、macOS デバイスの機能と設定を制御
- 組織が所有するデバイスや個人所有のデバイス (BYOD) を登録して組織が管理および制御可能
- ブラウザーの設定、Bluetooth やカメラの利用許可、Wi-Fi の設定、Microsoft Defender ウイルス対策の設定など、プラットフォームに応じてさまざまなポリシー設定が可能
- 各設定の適用の可能性、適合性、エラーの有無に関するレポートにより、デバイスの状況をすばやく把握

モバイル アプリ管理 (MAM)

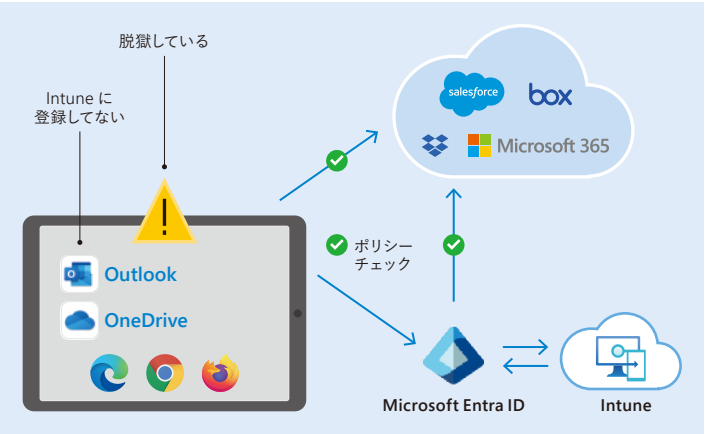
アプリケーション管理と組織データの保護

- Microsoft Entra ID との連携で、デバイス上の個人データと組織データを分離し、組織データにセキュリティ保護を追加して安全性を確保
- 管理対象アプリと非管理対象アプリ間でのコピー、切り取り、貼り付け、保存などの操作を制限して企業データの漏洩を防止
- 会社ポータルや管理コンソールからセルフサービスでセレクティブ ワイプを実行し、個人用アプリとデータを残したまま、管理対象アプリとデータを削除可能

デバイス コンプライアンス

許可された安全なデバイスのみで利用

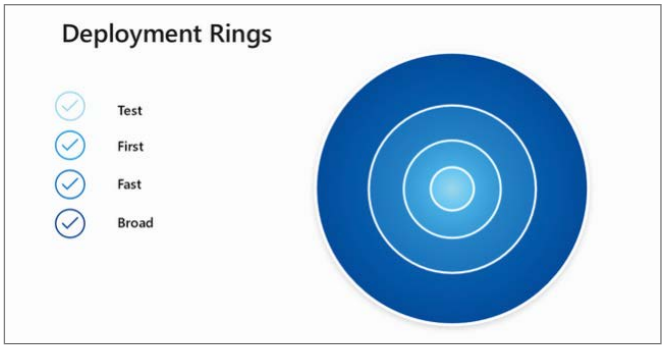
- クラウド サービスへ接続してくる PC やモバイル デバイスの管理状態を確認して、承認されたデバイスのみにアクセスを許可
- Intune に登録と管理されているか、Microsoft Entra ID のドメインに参加しているか、組織のコンプライアンス ポリシーに準拠しているかを自動的にチェック
- Microsoft Entra ID の条件付きアクセスや Microsoft Defender for Endpoint 脅威レベルと連携して、デバイスごとのアクセス許可を自動的に制御可能



更新プログラムを自動更新

Windows Autopatch による更新の自動化

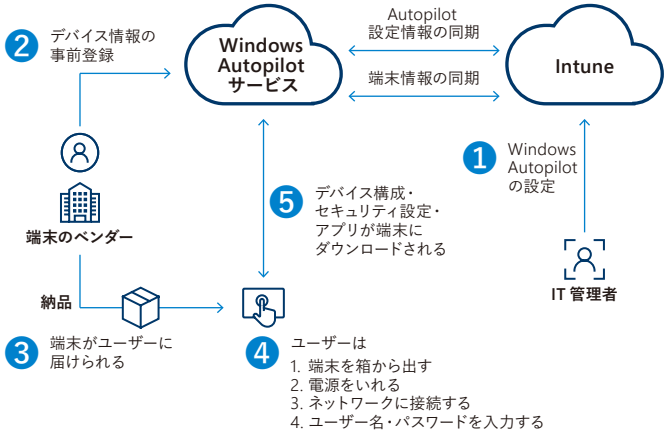
- Windows Enterprise E3 のライセンスを保有デバイスに対して、追加費用なしで Windows、Office アプリ、Edge を最新の状態に自動更新
- Windows Autopatch は、組織のエンドポイント間の変動を検出し、Test、first、Fast、Broad の 4 つに自動分類
- 更新は Test に分類されたデバイスにインストールされ、検証テスト期間を経過してから、次の Broad に進み、同様に他の分類へと順次処理を実行
- ユーザー エクスペリエンスに影響がある更新は分類ごとに 30 日の猶予期間があるため、問題の確認と報告、更新の停止が可能



Windows の初期展開を効率化

クラウドから Windows をすばやく展開

- Windows 端末の初期設定をクラウドベースで自動化、端末展開におけるユーザーと管理者の負担を大幅に軽減
- 端末の電源を入れ、ネットワークに接続し、ユーザー名とパスワードを入力するだけで、組織の設定やアプリのインストールを自動的に実行
- 特定のアプリを実行する Kiosk 端末にも対応
- 他ソリューションとの連携で、以前の Windows からのアップグレードと最新 Windows の設定をシームレスに実行可能



Microsoft Intune アドオン

アドオンを利用することで、アプリケーションとエンドポイントの管理機能をさらに統一し、ハイブリッド ワーカーのコンピューティング環境の保護とサポートにかかるコストと複雑さを軽減します。Intune Admin Center からプレミアム アドオンの試用版の利用や購入を行うことができます。

セキュアなリモート ヘルプの提供

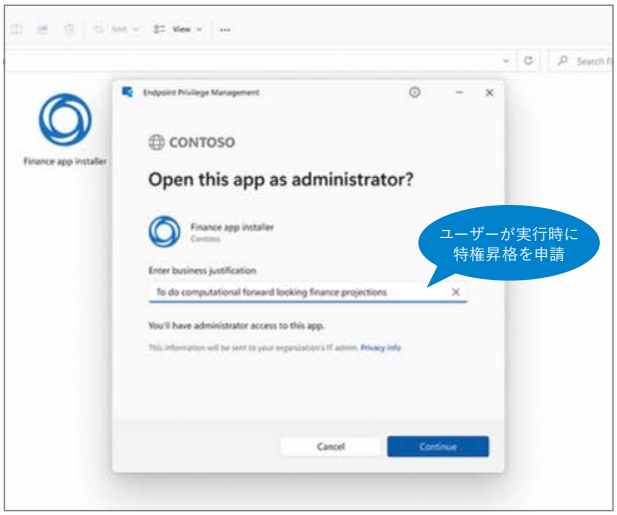
より安全で便利なリモート ヘルプ アドオン

- 多要素認証、セキュリティ更新プログラムのインストール、特定のリージョンまたは IP アドレスのリモート ヘルプへのアクセスのロックなど、条件付きアクセス機能を利用可能
- Intune に登録されていないデバイスにヘルプを許可可能 (既定では無効)
- ロールベースのアクセス制御でヘルパーがアクセスできる範囲を制御
- 特権の昇格により、ヘルパーは必要に応じて管理者の資格情報を使って管理アクセス許が必要な操作を提供可能

エンドポイント特権管理

管理者特権を必要とするタスクへの対応

- 標準ユーザーの昇格を制御し、特定の承認済みアプリを管理者権限で実行することを許可可能
- 必要な場合のみ特権昇格を許可、規則やルールの設定、自動承認などのオプションも提供



登録されていない デバイスのサポート プレビュー

モバイル アプリ管理用の Microsoft Tunnel

- Microsoft Tunnel の使用時、モバイル アプリ管理 (MAM) を追加することで、Microsoft Intune に登録されていないデバイスをサポートできるように拡張
- Microsoft Tunnel のデプロイ、Android Enterprise バージョン 10.0 以降、iOS バージョン 14.0 以降が必要

特殊なデバイスの管理 プレビュー

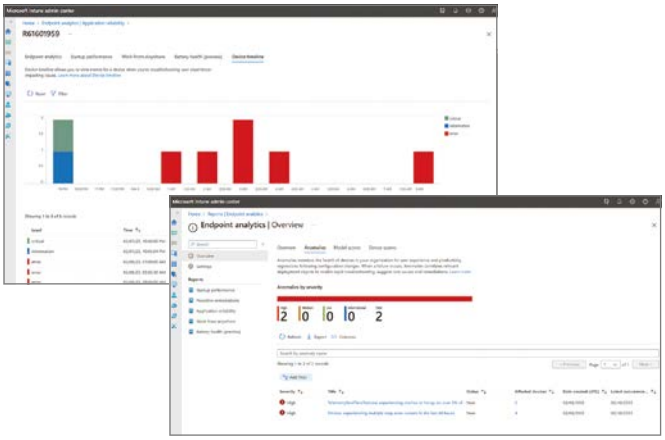
特殊なデバイスの管理、構成、保護機能

- サイズが 30 インチを超える大きなスマート スクリーン デバイス、AR/VR ヘッドセット、ウェアラブル ヘッドセット
- 電話会議、ワイヤレス画面共有、ビデオ会議に統合されたエクスペリエンスを提供するソフトウェア ベースの会議室システムである会議室会議デバイス

高度な エンドポイント分析 プレビュー

エンドポイント分析のさらに高度な機能を提供

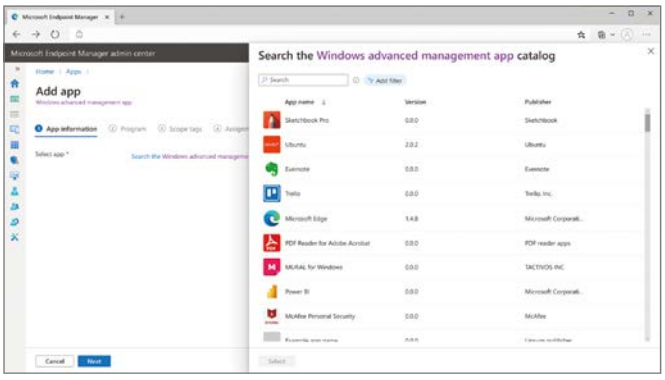
- スコープ タグを使用してエンドポイント分析レポートをデバイスのサブセットにスライス可能
- 構成変更後のユーザー エクスペリエンスと生産性の低下について、組織内のデバイスの正常性を監視
- 拡張されたデバイス タイムラインにより、特定のデバイスで発生したイベントの履歴を表示可能



高度なアプリ管理 プレビュー

組織で使用するアプリの管理負担を軽減

- エンタープライズ アプリのカタログを提供し、コントロールによるアプリの発見・展開・アップデート・脆弱性のパッチ適用を容易に行うことが可能



Microsoft 365 を高度な脅威から保護

Microsoft Defender for Office 365

統合型の脅威対策で Microsoft 365 全体を保護

Microsoft Defender for Office 365 は、スプーフィング対策やコンテンツ分析などが統合されたセキュリティによって高度な脅威から保護し、侵入した脅威を自動的に調査して対応することで、安全なコラボレーション基盤を実現します。

基本的対策

スプーフィング対策

- DMARK、DKIM、SPF
- ドメイン/ブランド偽装検出
- アンチウイルス/スパム対策
- メールボックス インテリジェンス

Exchange Online Protection (EOP)、ゼロアワー自動消去 (ZAP)

高度な脅威への対策

コンテンツ分析

- 添付ファイルの詳細解析
- 悪意のある URL の検査
- BEC/なりすましメール対策
- 不審なパスワード付 ZIP 対策

Safe Attachments、Safe Links、フィッシング対策、Safe Documents

調査の自動化

プレイブック

- 脅威の詳細調査
- 調査時間の短縮 (自動化)
- デバイス (MDE) とのシグナル共有

脅威エクスプローラー、自動調査と応答 (AIR)、キャンペーン ビュー

人的対策

ユーザー トレーニングとリテラシー向上

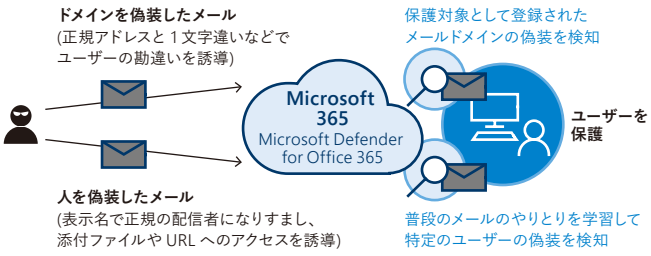
- 標的型メール攻撃訓練
- 訓練実施後のトレーニング ビデオ
- 受講状況の確認やトラック

攻撃シミュレーションのトレーニング

メールボックス インテリジェンス

偽装対策と高度なフィッシング対策

- 既知および不明な送信者を含むユーザーのコンタクト グラフに基づき、正常時とは違う異常を検出し、検疫およびユーザー ヒントを表示
- 連絡先や履歴メールのフロー パターンに応じて、ユーザーにメールを送る可能性が高いユーザー マップの作成が可能
- 日常的にメールの送受信がないユーザーからのメールを受信した際に、なりすましメールかを検出しやすくするインテリジェンス機能を提供



安全なドキュメント

不審な添付ファイルを検査

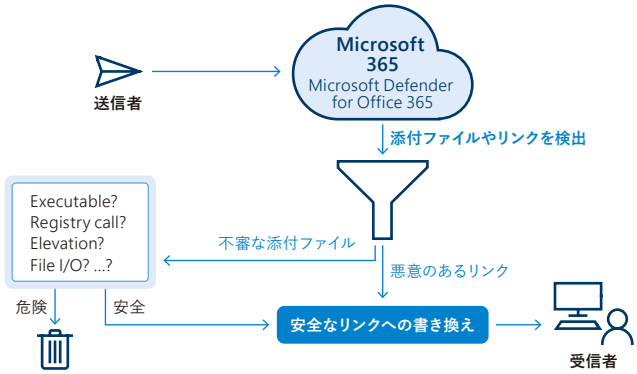
- Safe Documents により、パスワード付 ZIP などのメール フィルタリングで検出できなかった不審なファイルを開封時に詳細検査を実施

※ Microsoft 365 E5 Security もしくは Microsoft 365 A5 ライセンスが必要

安全な添付ファイル

Safe Attachments と Safe Links

- Safe Attachments により、メールが受信者に配信される前に、仮想環境上で添付ファイルを解析し、不正と判断された場合は検出と検疫を実施 (Teams などでファイルが共有された際も検出可能)
- Safe Links は、受信メールにある URL のスキャンと書き換え、URL リンクの検証機能を提供、Defender がリンクを先にスキャンすることでフィッシング攻撃サイトなどへのアクセスをブロック



Microsoft Defender for Office 365 Plan 2 と Microsoft Defender for Endpoint (MDE) の連携

たとえば、特定のエンドポイントで不審メールから脅威が検出された際に、同じ脅威を含んだメールが配信されたユーザーのメールボックスから一括削除して組織での感染拡大を防止可能

クラウドの保護、可視化、制御

Microsoft Defender for Cloud Apps

マイクロソフトおよびサード パーティ製のクラウド全体を保護

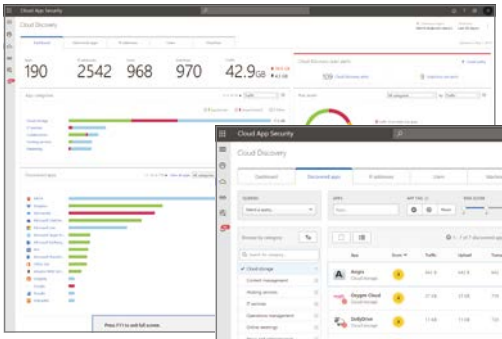
Microsoft Defender for Cloud Apps (MCAS) は、ログの収集、API コネクター、リバース プロキシなど、さまざまな展開モードをサポートするクラウド アクセス セキュリティ ブローカー (CASB) です。お客様が利用するクラウド サービス全体にわたるサイバー攻撃の脅威を特定および対処するために必要なセキュリティ機能を提供します。

シャドウ IT の検出

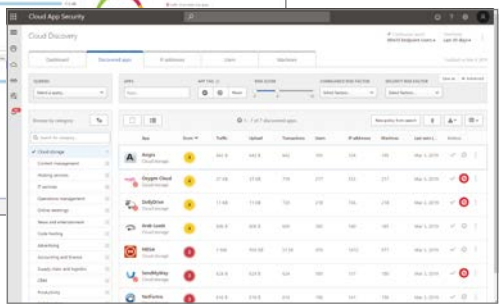
Microsoft Defender for Endpoint との統合

- Microsoft Defender for Endpoint との統合により、エンドポイントの通信履歴から組織の承認アプリおよび未承認アプリへのアクセス状況を可視化
- 未承認アプリに対するアクセス制御のポリシーをエンドポイントに直接配信して未承認アプリへのアクセスをブロック可能
- 16,000 以上のアプリ カタログを保有しており、検出した各アプリのリスク スコアの可視化や大量データのアップロードなどの異常行為の可視化が可能

Cloud Discovery ダッシュボード



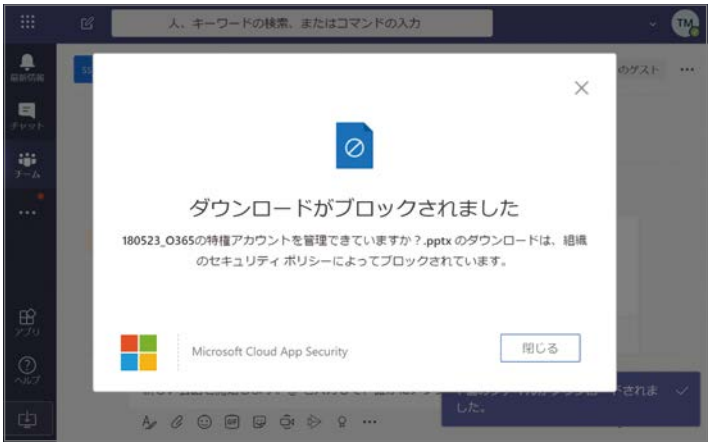
アプリケーション カタログ



セッション制御

安全なリモートワーク環境の実現

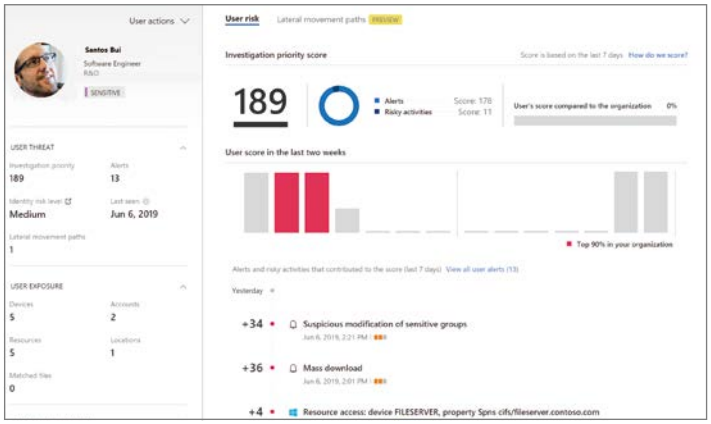
- Microsoft Entra ID の ID を連携する SaaS アプリや、Microsoft Entra ID App Proxy で公開されているオンプレミスの Web サービスに、Microsoft Entra ID 条件付きアクセス機能を拡張可能
- デバイスの管理形態 (BYOD など) や利用場所の条件に応じた制限付きのアクセスによって、セキュリティと業務継続性の両立を実現
- BYOD によるファイルのダウンロードの禁止、ファイル ダウンロード時の暗号化を強制、企業データの印刷やコピー & ペーストを禁止などのセッション制御が可能 (セッション制御はブラウザーのみ対象)



異常な行動の検知

ユーザー アクティビティの監視と制御

- API 接続されたクラウド サービス上のユーザーの行動を監視し、大量のファイルダウンロードや複数回のログイン試行の失敗など、通常とは異なる行動を検知した場合、管理者への通知や事前に定義された対処を自動的に実行
- オンプレミスの AD の資格情報に対する攻撃や不正アクセスを検知する Microsoft Defender for Identity と、Microsoft Entra ID 上の資格情報に対する攻撃や不正アクセスを検知する Microsoft Entra ID Identity Protection のアラートを MCAS に統合可能



ユーザーのリスクをスコアリングし、調査の優先度が高いユーザーを可視化

デバイスの脅威検出と対応

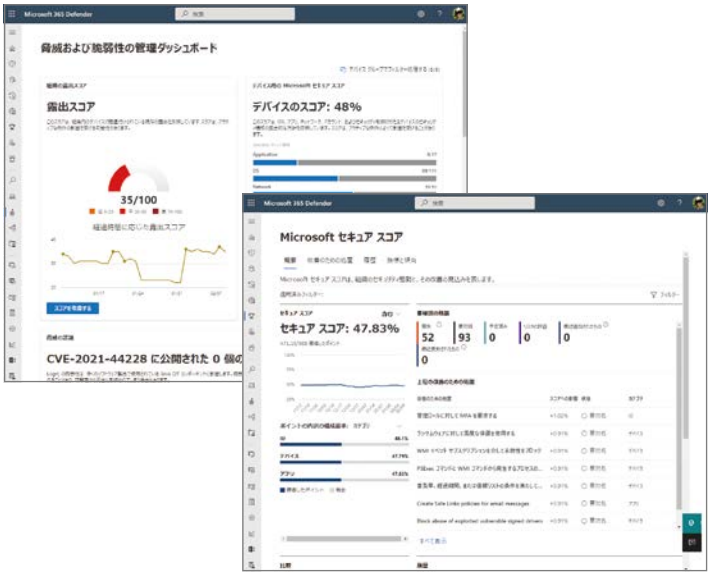
Microsoft Defender for Endpoint

進化した防御でセキュリティを強化、脅威を迅速に阻止

Microsoft Defender for Endpoint は、クラウドベースのエンドポイント セキュリティ ソリューションで、ランサムウェア、ファイルレス マルウェア、その他の高度な攻撃から多様なエンドポイントを保護します。Windows、macOS、Linux、Android、iOS デバイスとネットワーク デバイスに対応しており、これらを検出して巧妙な脅威から保護することが可能です。

脅威と脆弱性の管理

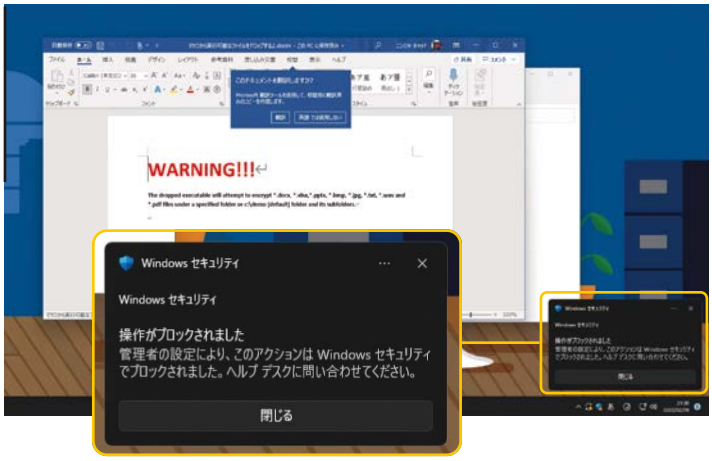
脅威と脆弱性の管理を使用して弱点を調査



- エージェントを追加することなく、脅威と脆弱性の管理に関する検出結果を自動的に取得
- Microsoft セキュリティ スコアにより、組織のセキュリティ状況をスコア化し、改善のための処置や構成方法を確認可能
- 脅威の分析により、世界で起こる最新の脅威情報確認組織内への影響と対策も確認可能
- 脆弱性の管理により、サード パーティ ソフトウェアを含む脆弱性への対応状況を確認可能
- Defender Vulnerability Management (現在パブリック プレビュー中)は、各種デバイス向けに、資産の可視性、インテリジェントな評価、組み込みの修復ツールを提供

攻撃面の減少

攻撃面の減少でマルウェアへの感染を防止



- Windows OS にルールを適用し、攻撃に悪用されるプログラムやソフトウェア動作をブロックすることで保護
- 攻撃面の減少ルールによって検出された侵害アクティビティや、前提条件を満たしていないあるいは誤まって構成されているデバイスなどの状況を Defender for Endpoint で把握可能
- Web コンテンツ フィルターにより、成人向けコンテンツ、チャット、ゲーム、P2P、画像共有などのカテゴリを指定して、各コンテンツへのアクセスを制限し、デバイスを Web の脅威から保護

次世代保護のエンジン

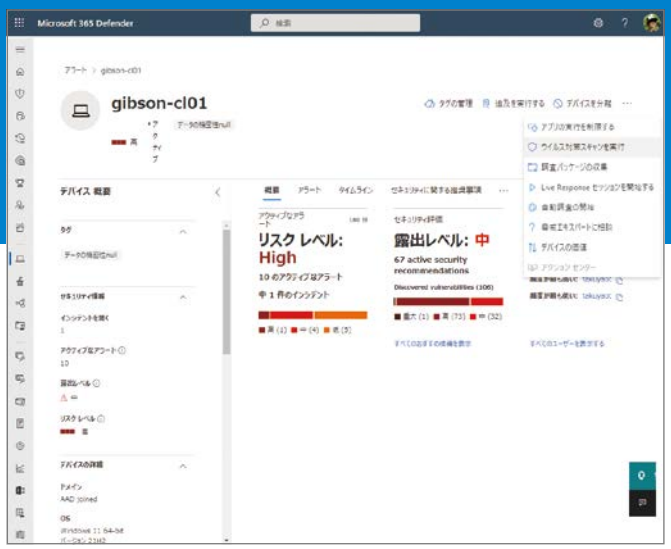
新たな脅威を補足するための次世代保護エンジン

- 挙動ベースおよびヒューリスティックのリアルタイム ウイルス対策保護は、ファイルとプロセスの動作監視、その他のヒューリスティックを使用したスキャンにより、安全ではないと見なされているがマルウェアとして検出されない可能性のあるアプリの検出とブロックを提供
- クラウドによる保護は、新たに出現する脅威のほぼ瞬時の検出とブロックを提供
- 専用の保護および製品の更新プログラムは、Microsoft Defender ウイルス対策を最新状態に維持することに関連する更新プログラムを提供

アラート検出と対処

ほぼリアルタイムで攻撃を検出

- 既知および未知の脅威に対応する高度な分析機能により、一見問題のない行為でも、一連の行動を関連付けて判断することで悪意のある行為かどうかの判定が可能
- 検出されたアラートと関連するエンティティがまとめられたインシデントにより、広範な攻撃ストーリーを把握し、複雑な脅威の範囲をすばやく確認可能
- インシデント発生時、デバイスの分離やアプリの実行制限、ウイルス対策のスキャンを実行など、特定のデバイスに対して的確なアクションを行えるため、感染などの被害を最小限に抑制可能

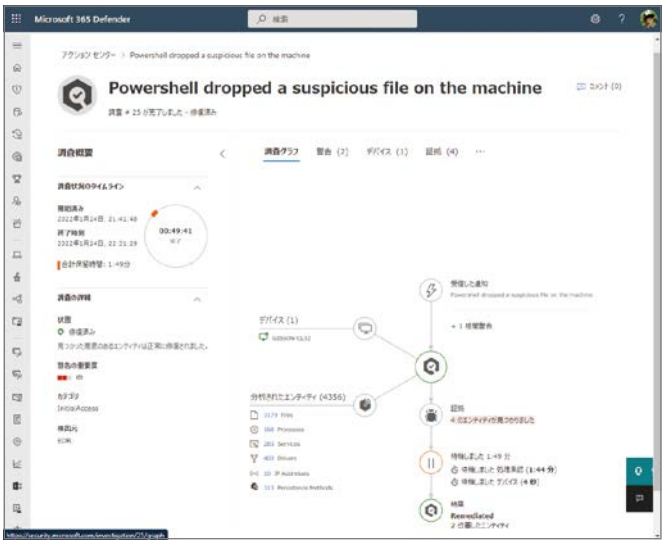


- 実行ファイルの停止や検疫、インジケーターの追加、ダウンロード、脅威エキスパートへの相談など、インシデントが発生した特定のファイルへのアクションが可能、感染の拡大防止やファイルの分析調査にも迅速に対応
- Live Response により、リモートシェル接続を使用して、特定のデバイスにアクセスし、詳細な調査作業や緊急時のアルタイム対応が可能

自動調査と応答

より効率的かつ効果的に脅威に対処

- Defender for Endpoint は、アラートを自動的に調査し、複雑な脅威を数分で自動修正
- セキュリティ専門家が実行するであろう脅威の調査と修復の最適な手順を仮想アナリストが模倣して実行
- 仮想アナリストは、無制限の容量で 24 時間 365 日稼働できるため、脅威への対応にかかる時間と管理者の負荷を大幅に削減可能
- すべての修復操作が自動的に実行されるフルオートから、一部のフォルダーへのアクションやすべての修復アクションに承認が必要になるセミオートが用意されており、多様なニーズに対応



Microsoft Security Experts

セキュリティ人材不足に悩む組織を支援

- マイクロソフトに所属する数千人の専門家による人的サービスと、先進テクノロジを組み合わせたマネージド セキュリティ ソリューション
- Microsoft Defender Experts for Hunting は、専門家が先回り型で脅威ハンティングを行い、検出したものを調査し、検証済みのアラート情報と修復手順を提供
- Microsoft Security Services for Enterprise は、専門家がオンボーディング、アドバイザリ サービス、マネージド型の検出と応答 (MXDR)、復旧の管理を支援
- Microsoft Defender Experts for XDR は、Microsoft 365 Defender 全体で検知と応答機能を提供し、自動化と専門知識でお客様と共にインシデントに対応するためのマネージド XDR (extended detection and response) サービス

クロスプラットフォーム対応

プラットフォームを超えたセキュリティを提供

- Windows をはじめ、Linux、macOS が動作するエンドポイントおよびサーバーをサポート
- Android と iOS を搭載するモバイル デバイスをサポート
- Windows 365 や Azure Virtual Desktop などの仮想デスクトップをサポート
- Cisco Juniper Networks や HP Enterprise Palo Alto Networks などのネットワーク デバイスをサポート

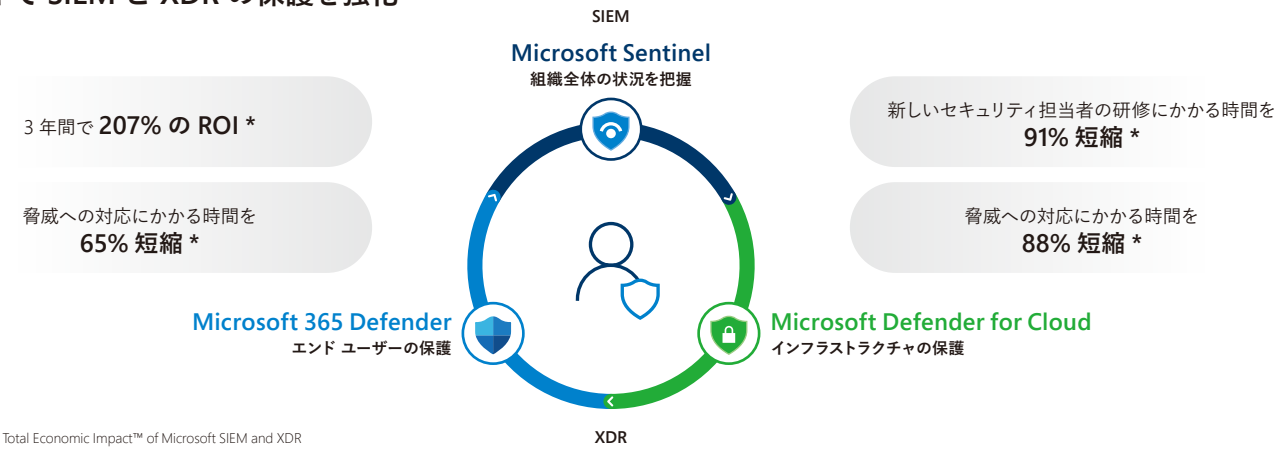
クラウド ネイティブの SIEM ソリューション

Microsoft Sentinel

クラウドと AI を活用した次世代型セキュリティ運用

Microsoft Sentinel は、スケーラブルでクラウド ネイティブのソリューションで、セキュリティ情報とイベント管理 (SIEM) とセキュリティ オーケストレーション、オートメーション、応答 (SOAR) によって、インテリジェントなセキュリティ分析と脅威インテリジェンスを組織全体に提供します。

低コストで SIEM と XDR の保護を強化



* The Total Economic Impact™ of Microsoft SIEM and XDR

Microsoft Sentinel の特長

デジタル資産全体を保護

ハイブリッド、マルチクラウド、マルチプラットフォームのビジネス向けのスケーラブルで統合型ソリューションにより、セキュリティを強化します。

- コネクタ、ダッシュボード、検出ルール、プレイブック、ハンティング クエリなどの広範なコンテンツをすべてソリューションとしてパッケージ化し、脅威に対する防御を迅速化
- すべてのセキュリティ ログやツールを統合
- 複数のクラウド、SaaS、CASB、エンドポイント、ネットワーク、OT/IoT からのデータの取り込み、エンリッチメント、配信を可能にする 225 種類以上の標準の統合により、初日から利用を開始
- SAP、Dynamics などのビジネス アプリケーションで脅威を検出、調査、対応

マイクロソフトのインテリジェンスを活用してレベルアップ

高度な AI、世界水準のセキュリティの専門知識、包括的な脅威インテリジェンスによって SecOps チームを支援します。

- 広範なトレーニングを行った AI によるスコアリングとチューニング、ノイズの削減、ガイド付きヘルプ、自社と似た顧客に関するインサイトに基づく推奨事項を活用
- 強化された UEBA、自動化、ハンティング機能、脅威インテリジェンス (TI) を日常業務のワークフローに統合し、調査と対応を迅速化
- Fusion と BYO ML (Build-your-own-Machine-learning) を活用し、進化する攻撃に先回りで対応

効率的に検出、対応

インシデントを監視、管理、対応する統合型ツールセットにより、進化する攻撃に先回りで対応できます。

- あらゆる種類のデータの脅威をクラウドのスピードで簡単にハンティング。機械学習により、アラートを優先度の高いインシデントに自動的に関連付け、ノイズを削減
- SOC チーム向けの組み込みのケース管理により、組織全体が協力して問題に迅速に対応することが可能
- 組み込みの UEBA により、ユーザーの異常な行動を迅速に特定し、業界最高レベルの脅威インテリジェンスにより、社内外の攻撃面を悪用する攻撃者を把握

セキュリティ運用の規模を拡張

ビジネス ニーズに対応するソリューションにより、セキュリティの需要の高まりに対応します。

- インフラストラクチャのセットアップやメンテナンスが不要
- コンピューティングまたはストレージ リソースの制限なしで自由に拡張
- SaaS ソリューションにより、組織全体からクラウド規模のデータを収集、分析
- 統合型 SecOps プラットフォームと Microsoft 365 Defender の標準の統合により、各種セキュリティ ツールの統合にかかる時間を短縮
- マイクロソフトのセキュリティ エキスパートのコミュニティの協力を得て、あらゆる規模、業界、MSSP、MDP の企業の現場で実証済み

サイバーセキュリティの脅威を軽減

Microsoft Defender Vulnerability Management

リスクベースの脆弱性管理

Defender Vulnerability Management には、資産の可視化とインテリジェントな評価と優先順位付けの機能に加えて組み込みの修復ツールが含まれており、Windows、macOS、Linux、Android、iOS のデバイスとネットワーク デバイスを対象として、組織全体で致命的な脆弱性や構成誤りを検出して対処できます。

セキュアな構成の維持

企業に必要な情報を 1 つの画面で提供

- Microsoft Defender for Endpoint との統合により、エンドポイントの通信履歴から組織の承認アプリおよび未承認アプリへのアクセス状況を可視化
- 未承認アプリに対するアクセス制御のポリシーをエンドポイントに直接配信して未承認アプリへのアクセスをブロック可能
- 16,000 以上のアプリ カタログを保有しており、検出した各アプリのリスク スコアの可視化や大量データのアップロードなどの異常行為の可視化が可能

デバイス情報


脅威の分析

セキュリティ ベースライン評価

対応の効率化

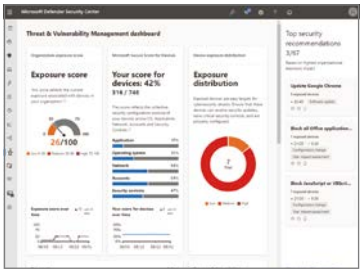
セキュリティ管理者と IT 管理者の共同作業を支援

- ユーザーが対応すべきアクションについて脆弱性の特性や脅威情報を元に優先順位付け
- Intune との連携で脆弱性に対する修復要求を依頼可能

リスクの把握

ハードウェアから OS までの幅広い脆弱性評価

- 自組織の全体的なスコア、セキュリティの推奨事項、脆弱性への対応状況、対応の指示と管理で脆弱性を管理
- ブラウザー拡張機能、インストールされている証明書、ノート PC・デスクトップ・サーバーなどのハードウェアとファームウェア、ネットワーク共有構成を評価
- 既知の脆弱なバージョンのアプリケーションの実行を防止、ネットワーク上の非管理デバイスの脆弱性をスキャン



Microsoft セキュリティ エキスパート

Security Experts は、企業がより良いセキュリティ成果を達成できるよう支援するための人的サービスと、専門家による訓練を受けたテクノロジを組み合わせたマネージド セキュリティ ソリューションです。

- **Microsoft Defender Experts for Hunting**
  エンドポイント、Office 365、クラウド アプリケーション、ID など Microsoft Defender データ全体の脅威をプロアクティブに調査したいとお客様向け
- **Microsoft Defender Experts for XDR**
  自社のセキュリティオペレーションセンターの能力を拡張する必要があるお客様向け
- **Microsoft Security Services for Enterprise**
  マイクロソフトの専門家による、より包括的で手厚いマネージドサービスを求める大企業のお客様向け
- **Microsoft Security Services for Incident Response**
  セキュリティ侵害の前、中、後においてお客様をサポート
- **Microsoft Security Services for Modernization**
  最新のセキュリティ機能を取り入れ、マイクロソフトのベストプラクティスとノウハウを活用したいお客様向け

データ資産のガバナンス、保護、管理

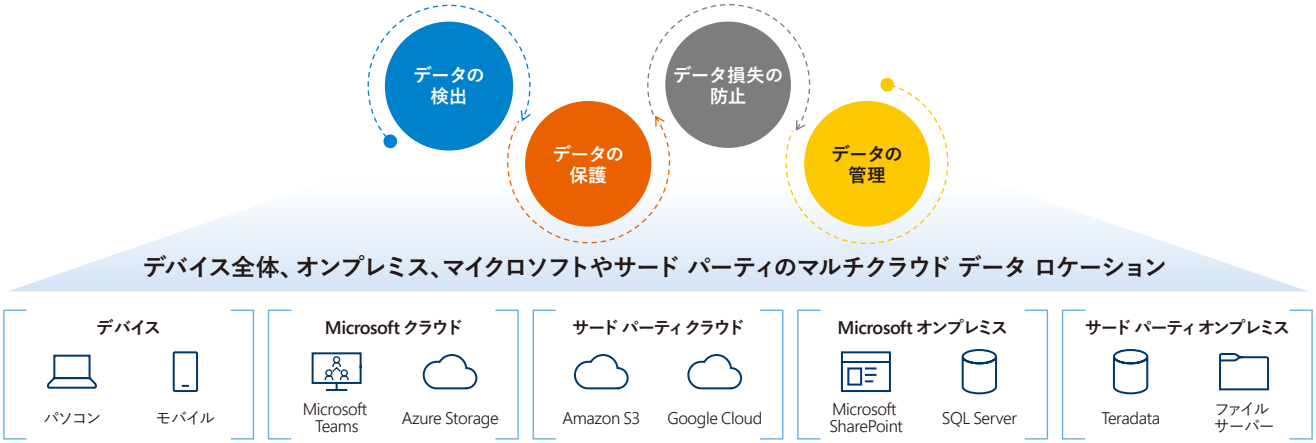
Microsoft Purview

重要なデータ資産を保護する包括的なソリューション

Microsoft Purview Information Protection は、プラットフォーム、アプリ、クラウドを横断してすべてのデータを安全に守るための情報保護、データ ガバナンス、リスク管理、コンプライアンスの機能を集めた、包括的なソリューションです。

場所に依存しないデータ保護

Microsoft Purview により、機密データがどこに保存されていても、どこに移動しても、それらの情報の検出、分類、保護を行えます。また、機密データのアクティビティを監視して、これらのデータが過度に共有されないように防止することも可能です。さらに、機密データの持ち出しやなどを検知できるため、組織内部で発生するさまざまなリスクへの準備と早期の対処を行うことが可能です。



データ資産を検出と保護 (Information Protection)

- 機密データを保護するためのインテリジェントなビルトインおよび拡張可能なソリューションを提供
- デバイス、アプリ、オンプレミスのファイル、クラウド サービス全体を横断して機密情報の保護が可能、大規模なデータの検知と分類を自動化
- 機械学習を使ったトレーニング可能な分類器により、データを自動的に分類
- 自動ラベリング、ユーザーによる手動ラベリング、推奨ラベリングを利用して柔軟にデータを分類可能、さまざまな業界の規制やルールにも対応
- Microsoft 365 に組み込まれた暗号化により、保存、転送中および使用中のデータを保護
- サード パーティ製のアプリやサービスに対応する SDK を用意しており、保護範囲を拡張可能

内部リスクへの準備 (Insider Risk Management)

- カスタマイズ可能なテンプレートとコンテンツに応じたインサイトにより、リスクのあるアクティビティや隠れたリスクを特定
- ユーザーの行動分析で異常なふるまいを検出するなど、コンプライアンス違反を人ベースで検知して内部不正に対処可能
- ユーザーのデータを匿名化するためのコントロール機能を内蔵し、プライバシーを保護可能
- 統合された調査のワークフローにより、情報セキュリティ、人事、法務などの各部門がコラボレーション可能

データの損失を防止 (Data Loss Prevention)

- 財務データ、所有権データ、クレジット カード番号などの機密データが故意、あるいは過失に関わらず共有されないように防止
- 150 種類上の機密情報のタイプとカスタムパターンを使用した横断的な機密情報の識別
- 機械学習アルゴリズムなどを使用して、DLP ポリシーに一致するコンテンツを検出
- レポート、ポリシー違反のアラート、不適切なデータの使用に対してアクションを実行
- Windows および Mac、オンプレミスのファイル共有、Edge および Chrome ブラウザー、サード パーティのクラウド サービスまで拡張して適用可能
- 柔軟なポリシー管理でデータを保護しながらユーザーの生産性も実現

リスクとコンプライアンス対応体制の改善

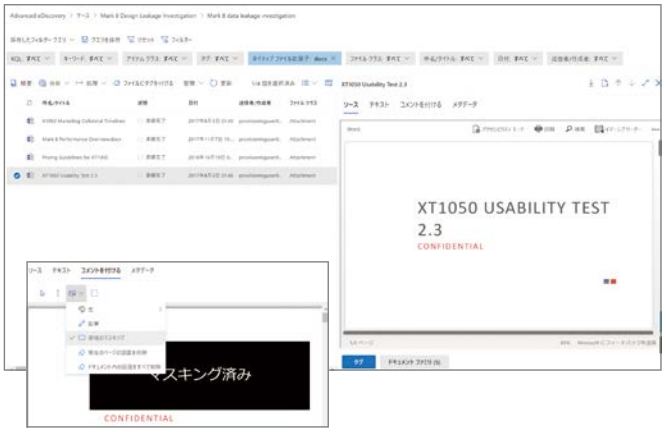
Microsoft Purview により、マルチクラウド環境においても、さまざまな国際、業種、または地域の規制と標準に対するコンプライアンス要件を満たすことができます。また、規制遵守義務を実現するとともに、組織の行動規範違反にすばやく対処することが可能です。

直感的なコンプライアンス管理 (Compliance Manager)

- コンプライアンス管理のオンボーディングから、ワークフロー管理、規制の実行までを直感的に実施可能
- すぐに使えてカスタマイズ可能な規制遵守評価テンプレートを 320 点以上を用意、マルチクラウドでのコンプライアンス要件にもすばやく対応
- コンプライアンス スコア、コントロール マッピング、バージョン管理、継続的コントロール評価など、リスクを縮小するための機能をビルトインで自動化
- 管理対象の環境を継続的にスキャンしてシステム設定を検出し、技術的コントロールの状態と自動信頼性判定の結果を通知

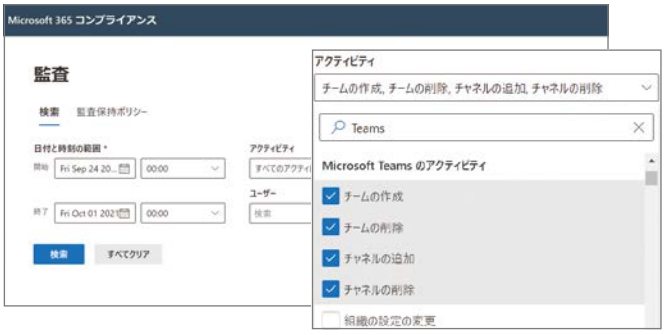
行動規範違反の迅速な特定と対応 (Communication Compliance)

- 事前定義したキーワードや条件、機械学習を活用してメールやチャットなどのメッセージにおける行動規範の違反を検知
- 業務上望ましくない不適切な画像を検知
- ハラスメント、違法な業務命令、カルテル等の談合、利益相反/競合する組織間のコミュニケーションを検知し、早急な対処を実現
- Exchange Online、Microsoft Teams、Yammer の通信の監視をサポート
- 多様なコネクターにより、サード パーティ製品の通信監視にも対応



データの検出、保持、収集、処理、選別、分析 (eDiscovery Premium)

- カストディアンごとのコンテンツの保持、ホールド通知の送信、確認応答の追跡
- 独立して検索、分析、共有、対処することができるケース内の静的なドキュメント セットのレビューと管理
- 重複検出、メール スレッド、テーマ、ML モデルにより、価値の高いコンテンツの候補を特定し、レビュー プロセスを効率化
- 検索結果で見つかった Teams や Outlook におけるクラウド添付ファイルのコンテンツの収集が可能



フォレンジックとコンプライアンス調査を強化 (Audit Premium)

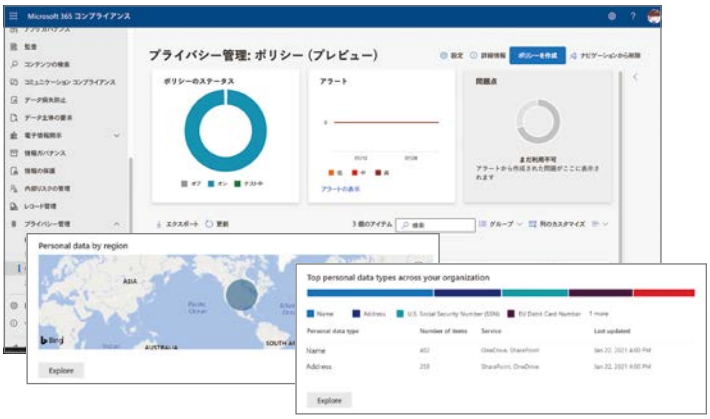
- アクセスしたメール アイテム、メール送信、ユーザー検索など、フォレンジック調査において重要な追加イベントを利用することが可能
- Exchange や SharePoint などの監監査ログを最大 1 年間保存、オプションで 10 年間保存のアドオンも提供
- ベースラインの 2 倍以上の広帯域データ アクセス

プライバシー管理

Microsoft Priva

Microsoft 365 に統合されたプライバシー管理ソリューション

Microsoft Priva は、先回りでプライバシーのリスクを特定し、それに対する防御を支援するプライバシー管理ソリューションです。組織に存在する個人情報の検索や視覚化、エンド ユーザーからのデータ主体権利の要求に対応する機能を提供します。



- 個人データの状況、好ましくないデータの転送、データの過度な公開、溜め込みから生じるプライバシーのリスクの傾向など、組織のプライバシー態勢を可視化
- 重大なプライバシー リスクを先回りで防ぐためのカスタマイズ可能なビルトイン ポリシーを用意
- プライバシー リスクを軽減するための自動修復アクションを Microsoft Outlook や Microsoft Teams などのアプリ内に表示し、従業員の行動変容を推進
- プライバシー関連の規制に係るデータの可視化、管理、追跡、主体の権利要求などに対する運用負担やコスト軽減を実現

プライバシー リスク管理

必要に応じたアクションを促すメールでリスクを低減

- プライバシーのリスクを効果的に軽減するために、自動化ポリシー、組み込みのリスク検出と修復、コラボレーション ワークフローを提供

プライバシー リスク管理の 3 つのポリシー

✓ データ転送

組織内の部署間、または国や地域の境界を越えて共有されている個人データを検出した場合、リスクを軽減するための推奨アクションを提示

✓ データの過度な公開

過度に公開されている個人データを検出した場合、適切な対応を行うように促すメールを送信

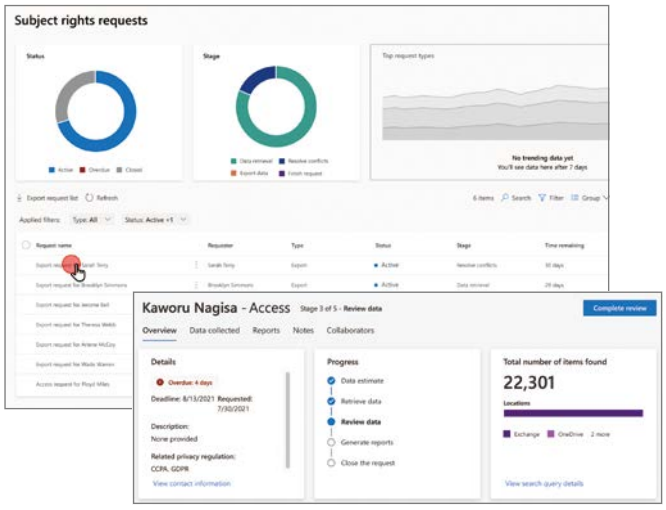
✓ データの最小限化

保持する必要のない個人データを検出した個人データを検出した場合、不要な個人情報の最小化を促すメールを送信

主体の権利要求に対応

Subject Rights Requests (SRR)

- 顧客のデータ主体権利要求である Data Subject Access Right (DSAR) に対応
- テナント環境内の個人データ検索、検索結果のレポート作成とエクスポート、レビュー、データ主体要求などの一元管理を実現
- Exchange Online、SharePoint Online、OneDrive for Business (Teamsや Groups 含む)、パブリック フォルダーを横断した検索に対応
- 最大 10,000 件の個別アイテムの検索、管理者協議のための Teams チャネルの自動作成、データ マッチングによる正確な検出、Power Automate による自動化などの機能も提供

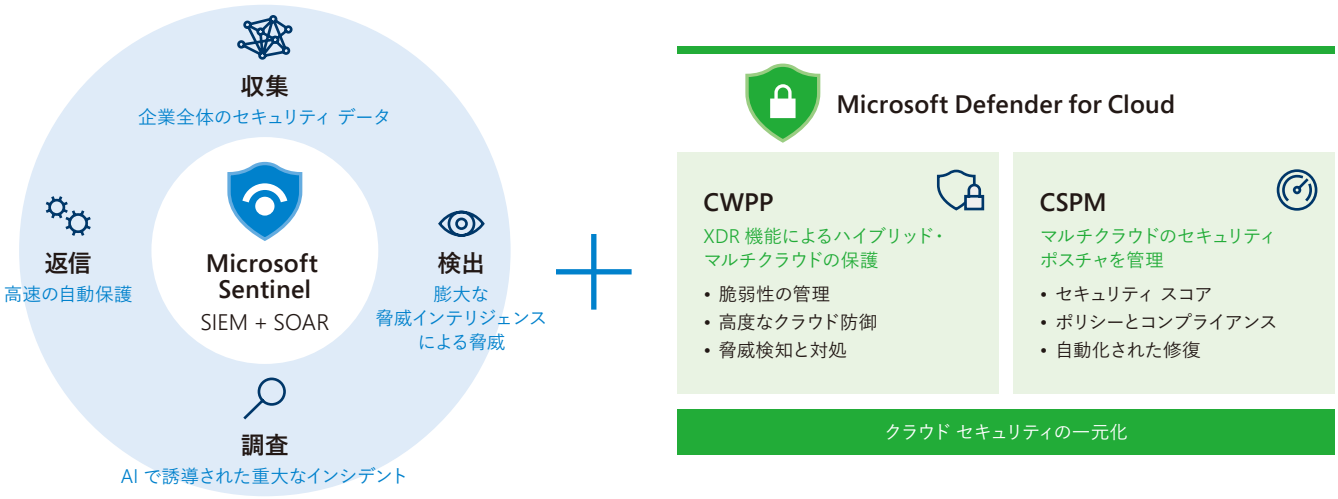


クラウドの保護、可視化、制御

Microsoft Defender for Cloud

ハイブリットおよびマルチクラウドのセキュリティ管理を強化

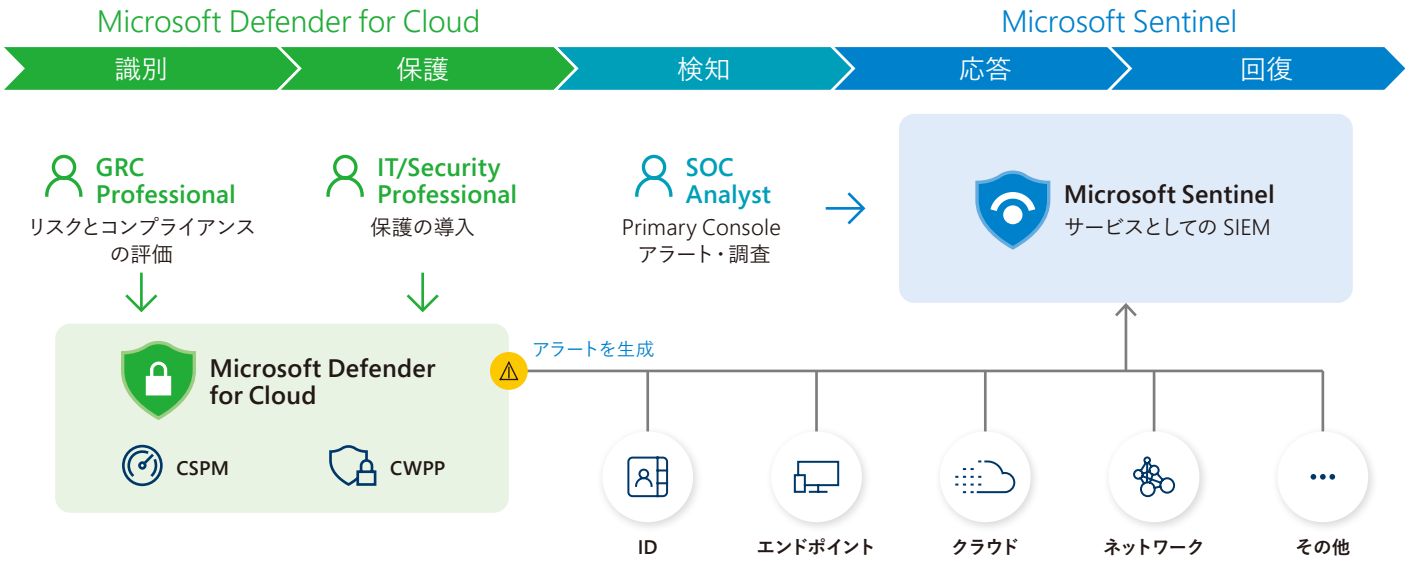
Microsoft Sentinel は、クラウド ネイティブのセキュリティ情報イベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAR) ソリューションです。Microsoft Defender for Cloud は、Azure、オンプレミス、マルチクラウドのすべてのリソース用のクラウド セキュリティ態勢管理 (CSPM) とクラウド ワークロード保護プラットフォーム (CWPP) を提供します。



連携によるアラート同期

コネクターでアラートを双方向に同期

- Defender for Cloud からアラートを Sentinel にストリーミングできるので、アラートと生成されるインシデントをより広範な組織の脅威コンテキストで表示、分析、対応可能
- インシデントの統合管理をはじめ、他の製品のアラートと関連付けして攻撃の全体像を把握、Sentinel の持つ AI エンジンによる脅威の検知が可能
- アラートを Sentinel に送る場合、サブスクリプションごとにログの保管を分けたい場合に便利
- セキュリティ ログを Sentinel と共有する場合、セキュリティ運用チームがすべての情報を一元管理可能



Microsoft 365 E3/E5 セキュリティ & コンプライアンス機能対応表

Microsoft 365 E5

	E5 Security	E5 Compliance		
		Information Protection & Governance	Insider Risk Management	eDiscovery & Audit
Office 365 E5	Microsoft Defender for Office 365 P1/P2	Data Lifecycle Management	Communication Compliance	eDiscovery (Premium)
		Records Management	Information Barriers	
		Advanced Message Encryption	Communication Compliance	Audit (Premium)
		DLP for Teams chat	Information Barriers	
EMS E5	Microsoft Defender for Cloud Apps			
	Microsoft Entra ID Premium P2	Microsoft Information Protection		
	Microsoft Defender for Identity			
Windows Enterprise E5	Microsoft Defender for Endpoint P2			
	Safe Documents	Endpoint DLP	Insider Risk Management	

Microsoft 365 E3

Office 365 E3	DLP for emails & files	eDiscovery (Standard)	Audit (Standard)	Microsoft Defender for Endpoint P1
	Azure Information Protection for Office 365	Compliance Manager		
EMS E3	Microsoft Entra ID Premium P1	Azure Information Protection P1		
	Microsoft Intune	Microsoft Configuration Manager		
Windows Enterprise E3	Microsoft Defender Application Control	Microsoft Defender Credential Guard	Microsoft Defender Application Guard	

追加サービス

セキュリティ & コンプライアンス機能

- Microsoft Priva Privacy Risk Management
- Microsoft Priva Subject Rights Request
- 10 年間の監査ログ保持

その他のセキュリティ サービス

- Microsoft Defender for Servers
- Microsoft Defender for Cloud
- Microsoft Sentinel
- Microsoft Security Experts

機能一覧はこちらをご覧ください。https://go.microsoft.com/fwlink/p/?LinkID=2139145

Microsoft 365 Enterprise に関する最新情報は、https://www.microsoft.com/ja-jp/microsoft-365 をご覧ください。

Microsoft

日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー

6660-NOC1