



セキュリティのステップアップ販売ガイド

Microsoft 365 Business Premium から E5 Security へ

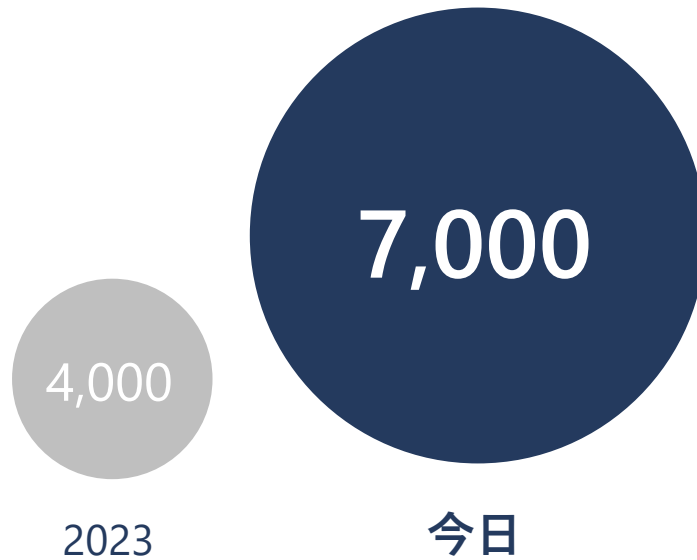
FY 26

サイバー脅威は 5 倍に増加

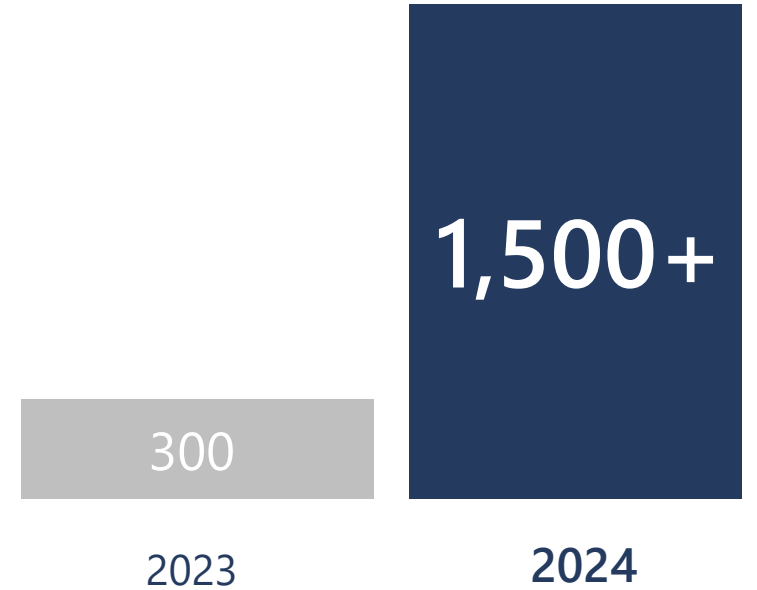
攻撃者がフィッシングの個人データにアクセスする時間の中央値



パスワード攻撃数 / 秒



Microsoft が追跡する脅威アクター



速度

規模

高度化・巧妙化

サイバー犯罪の現状

ランサムウェア

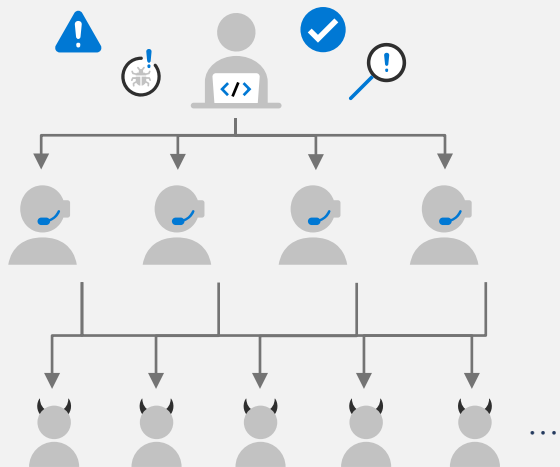
ランダムな攻撃 - 標的が広範でボリューム依存

- マルウェア開発者が自身のマルウェアを販売
- 攻撃の専門知識がなくとも容易に攻撃可能
- 高額報酬にてリクルート
- **費用対効果が高く**、世界中で増加傾向

マルウェア開発者

脆弱性偵察部隊

マルウェアのデプロイ



標的型攻撃 - ターゲットを絞り、成功率を向上

典型的な human-operated 攻撃

ランサムウェアの展開フェーズに到達する前に攻撃者を阻止することが重要

Pre-Ransomware

数日~数週間、数か月に及ぶこともあったが、過去 2 年の間に短縮

展開!

Ransomware

わずか数分で完了

組織の
マインドセット
の転換が必要

- ✓ 攻撃のレベルを下げることを目標
- ✓ セキュリティレベルの一貫性のために統合的にポリシーを適用
- ✓ 攻撃発生時にアラートを 1 つにグルーピングし、傾向や全体像を把握することで SOC の負荷を軽減

数値で見るサイバー犯罪の現状



88%

機密性の高い特権アカウントに対して、MFA が実装されていない割合

84%

ジャストインタイムの特権 ID 制御を実装していない組織の割合



68%

脆弱性 / 修正プログラム管理プロセスがなく、手動プロセス依存でセキュリティホールがある組織

60%

EDR, SIEM 未導入組織

60%

複数のクラウド環境をセキュリティ運用ツールに統合していなかった組織



7 億 1,000 通

1 週間にブロックしているフィッシングメール数

1 時間 12 分

フィッシングメールの被害に遭ってから、攻撃者が個人情報にアクセスするのにかかる時間の中央値

531,000

Defender for Office 365 によってブロックされた URL に加え、マイクロソフトの Digital Crimes Unit の指示により、削除したフィッシング URL

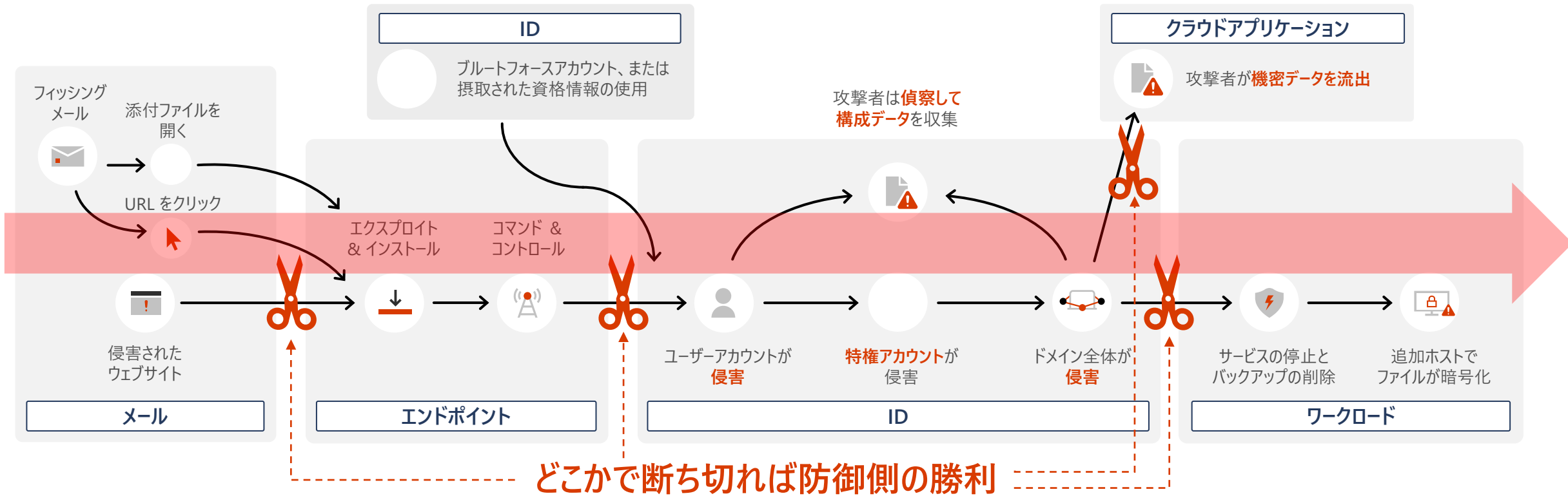


92%

リスクを軽減する効果的なデータ損失防止制御を実装していなかったために、データを損失した組織

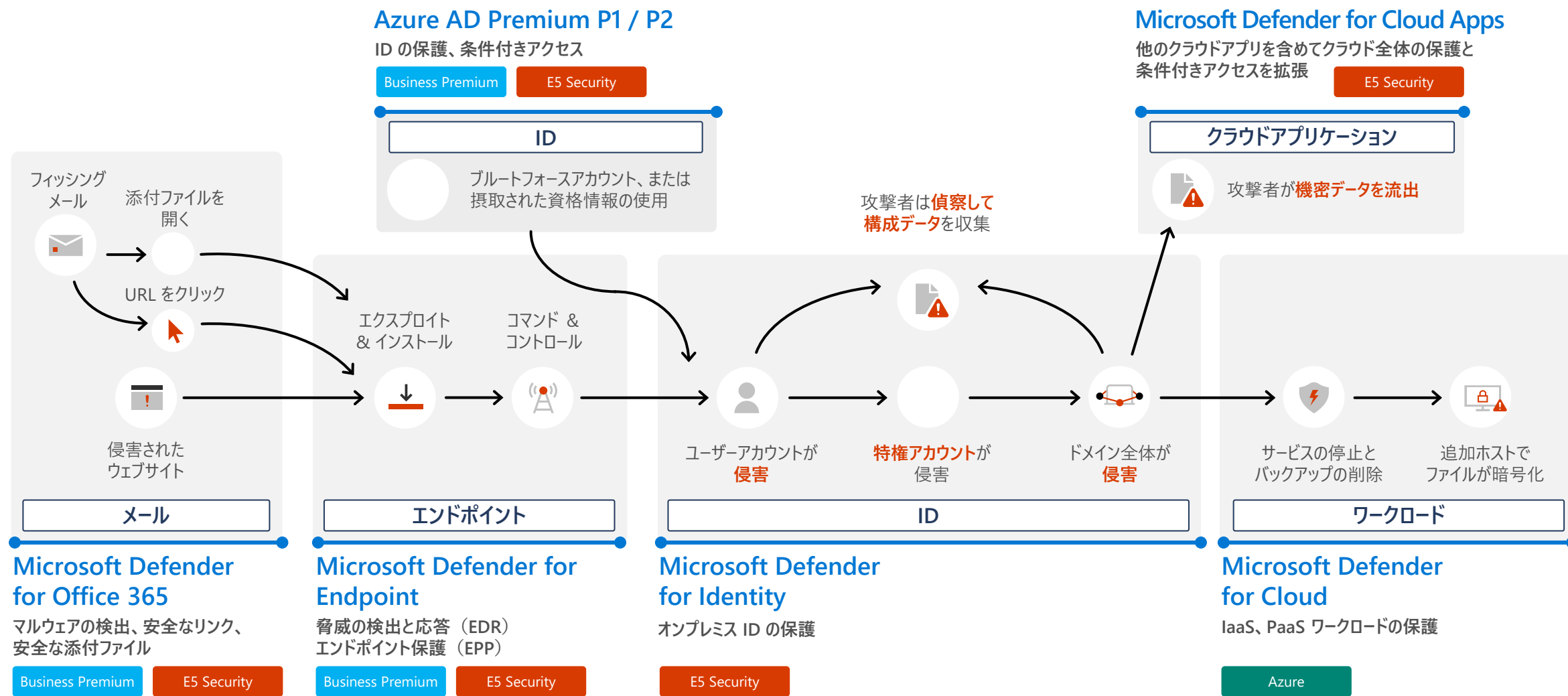
Cyber Kill Chain の攻撃フロー

典型的な人手によるランサムウェアキャンペーン



このモデルは線形であり、攻撃者が各ステージを順番に辿ることを予想し、どこかで攻撃を断ち切ることでその後のステージにおける攻撃を成功させないという防御方法

Microsoft ソリューションによる攻撃からの保護

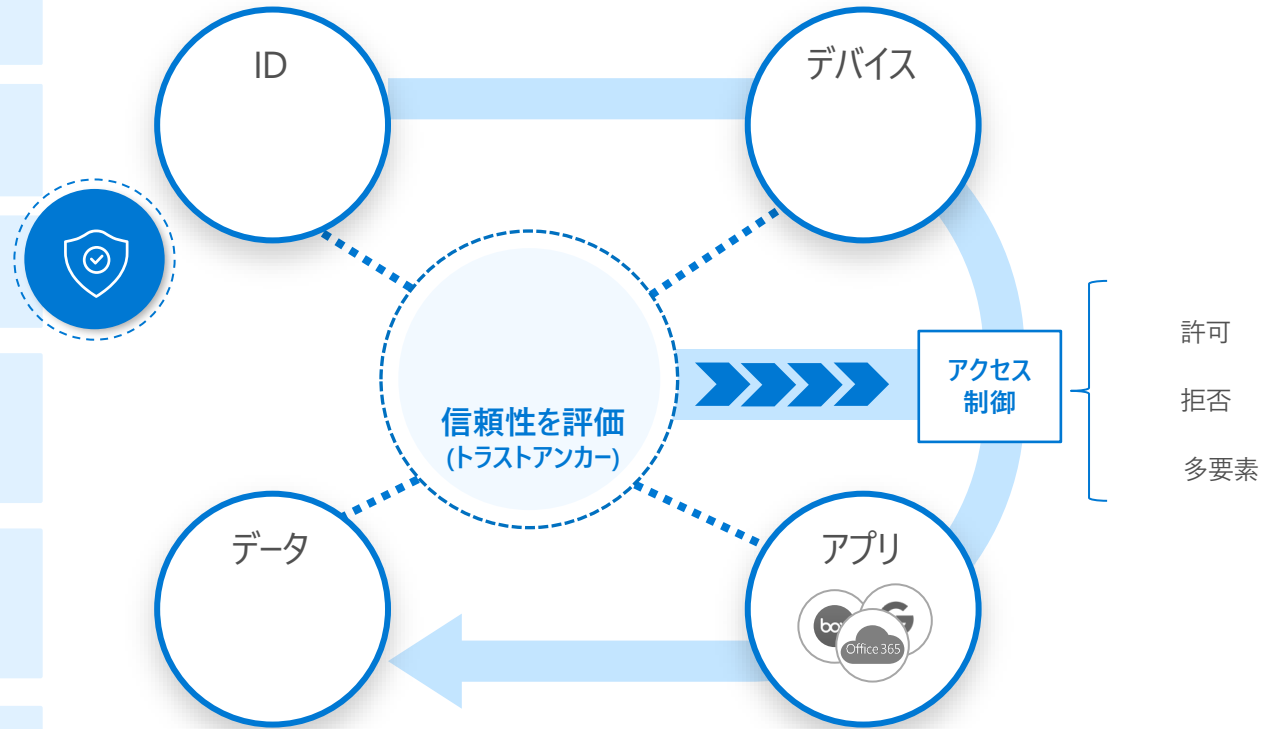


NIST：ゼロトラスト アーキテクチャの 6 原則

参考情報：NIST Zero Trust Architecture: "2. Zero Trust Architecture"

Microsoft Security の大原則

1. すべてのデータソースとサービスを識別する
2. “**暗黙的な信頼**”は排除する
3. 要求元の信頼は、アクセスが許可される前に評価する
4. リソースへのアクセスは、**ユーザー ID / デバイス**の評価と **リソース / データの重要度**によってポリシーで決定する
5. 組織が所有するシステムを監視して、**安全な状態のまま**であることを確認する
6. ユーザー認証は**動的**であり、アクセスが許可される前に厳密に実施する



Microsoft Entra ID を中心にインターネットおよびプライベートネットワークに拡張



Microsoft Entra ID によって管理される ID と Microsoft Intune によって管理されるエンドポイントに対するゼロトラストポリシーの適用として、Microsoft Entra 条件付きアクセスを使用します。ID、エンドポイント、ネットワーク全体で:適応型IDおよびネットワークアクセス制御 / 一貫したセキュリティポリシーの実装/継続的なアクセス評価を実行して、潜在的な侵害をリアルタイムで修正します。

Microsoft ならではの エンドポイント防御ソリューションの優位性として、Windows OS にビルトインしているためエージェントのインストールが不要という大きなメリットがある

攻撃への耐性

Windows OS に組み込み込まれた挙動センサーを使用するため、プロセスやサービス停止などによる攻撃を受けない。

メンテナンスフリー

エージェントの展開不要、アップデートの管理不要。
Windows OS の毎月の更新プログラムを適用するのみ。
アップデートに伴う検証も不要

高パフォーマンス

OS 標準のセンサーを利用するため負荷が非常に低い。
また通信データも最適化され、1 台あたり 1 日 5MB 程度。

Microsoft 365 セキュリティ製品連携

Windows セキュリティ製品はもちろん、Entra ID や Intune, Defender for CloudApps や Office 365 といった様々な製品と連携



Microsoft 365 Business Premium で
実装する

サイバー攻撃への 対応と防御



Microsoft 365 Business Premium

レイヤーセキュリティ：リスクレベルに応じたセキュリティ対策

Microsoft 365 Business Premium

Identity and access controls

Microsoft Entra ID Plan 1

パスワードの紛失を防ぐ多要素認証
パスワードレス認証
セルフサービスパスワードリセット
業務データへのアクセス制御を提供する条件付きアクセス
シャドー IT を発見

Device management

Microsoft Intune

モバイル、デスクトップ、Mac デバイスの一元管理
許可されたアプリからのみ業務データにアクセスできるようにする
紛失・盗難デバイスのデータをリモートワイプ BitLocker 暗号化

Device security

Microsoft Defender for Business

EDR によるランサムウェア対策
Android、iOS、Mac、Windows、Linuxにまたがる保護脅威と脆弱性の管理
月次サマリーレポート

Email and app security

Microsoft Defender for Office 365

電子メール全体にわたるフィッシングとマルウェアの防御
Microsoft Teams、OneDrive、および SharePoint
クリックした時点で URL フィルタリングを行う SafeLinks
サンドボックスでリアルタイムに添付ファイルをスキャンする Safe Attachments

Data security

Microsoft Purview

クレジットカード番号や社会保障番号などの機密データを保護するデータ紛失防止機能
機密データの分類とラベル付け転送禁止や電子メールの暗号化などの保護の適用

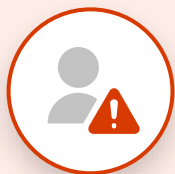
攻撃

ランサムウェア

一年で最も忙しい時期に、Northwind Trader のミッション クリティカルなファイルが使用できなくなりました。

ハッカーはランサムウェアを使用して Northwind のファイルを暗号化し、暗号化「キー」の支払いを要求しました。

Northwind は、暗号化の「キー」の料金を支払う必要があり、そうしないとデータが失われ、ビジネスが閉鎖される可能性があります。



攻撃者

社内ファイルの
暗号化

身代金を要求

身代金を受け取り
暗号化を解除

80%

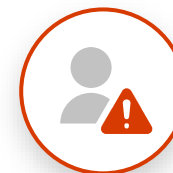
の中小企業がランサムウェアを最大の懸念事項として挙げています

*Source: Microsoft Internal Research of SMBs (2-299 employees)

防御

ランサムウェア防御

Microsoft 365 Business Premium では、従業員のデバイスは Microsoft Defender for Business で保護され、多層的なランサムウェア保護を提供して、業界初の攻撃を阻止し、手動攻撃や標的型攻撃から防御し、ネットワーク内を移動するのを阻止します。



攻撃者



Microsoft Defender
for Business は
ランサムウェア攻撃から
会社のファイルを保護します

94%

2020 年のランサムウェア攻撃に関連するダウンタイムの平均コストの増加

Microsoft Defender for Business

エンタープライズグレードの保護。従業員数が 300 人以下の企業向けに特別に設計されており、スタンドアロンソリューションとして、または Microsoft 365 Business Premium の一部としてご利用いただけます。



エンタープライズグレードの保護

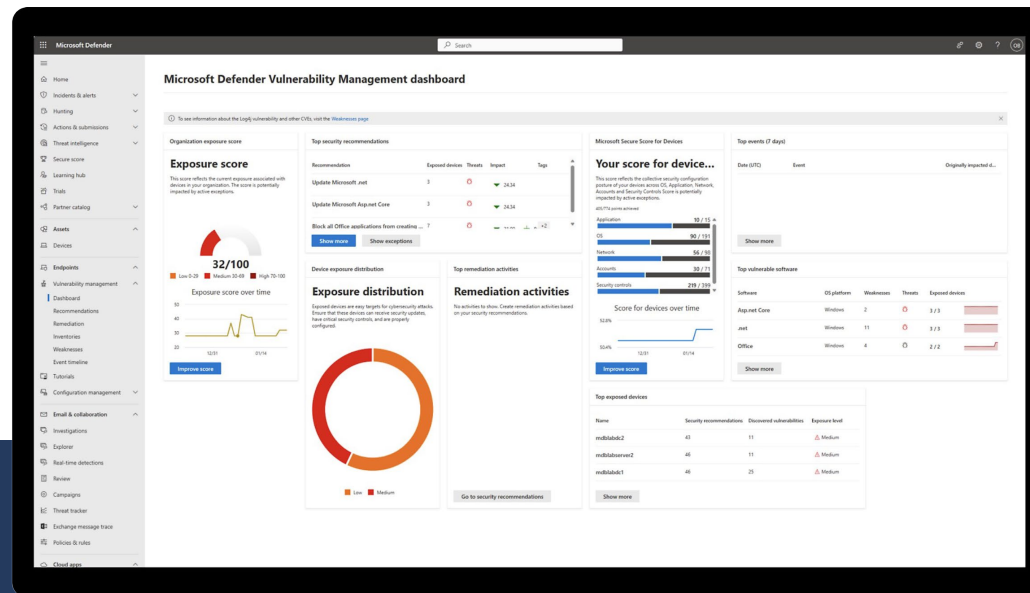
簡単なセットアップ、使いやすい



コスト効率



クロスプラットフォーム



EDR* と呼ばれるジャンルのセキュリティ

現在はセキュリティ統合プラットフォームとして発展
EDR は多くの機能の一つに

*EDR : Endpoint Detection and Response 以下の 4 機能を備えたソリューション

- ① セキュリティ インシデントの検出
- ② セキュリティ インシデントの調査
- ③ インシデントを封じ込め
- ④ エンドポイントを修復

ウイルス対策ソフトが侵入防御が前提であるのに対し、EDR は侵入されたときの対処を前提に考えられています。EDR はウイルス対策ソフトと組み合わせて使用します。

攻撃

フィッシング攻撃

表向きは有名な組織からのセキュリティで保護されたドキュメントへのリンクが記載された電子メールを受け取ります。資格情報を入力して表示しますが、読み込みに失敗します。彼らは他の仕事に移り、不具合を忘れてしまいます。これはフィッシング攻撃でした。



1 in 4 SMB がセキュリティ侵害を経験

防御

高度なフィッシング防御

Northwind Traders の従業員は、ドキュメントへの悪意のあるリンクが記載された電子メールを受信します。Microsoft 365 Business Premium には、Defender for Office 365 が含まれており、「セキュリティサンドボックス」内のリンクを確認し、ユーザーに脅威を警告し、攻撃から保護します。また、添付ファイルにマルウェアやその他の脅威がないかリアルタイムでチェックします。



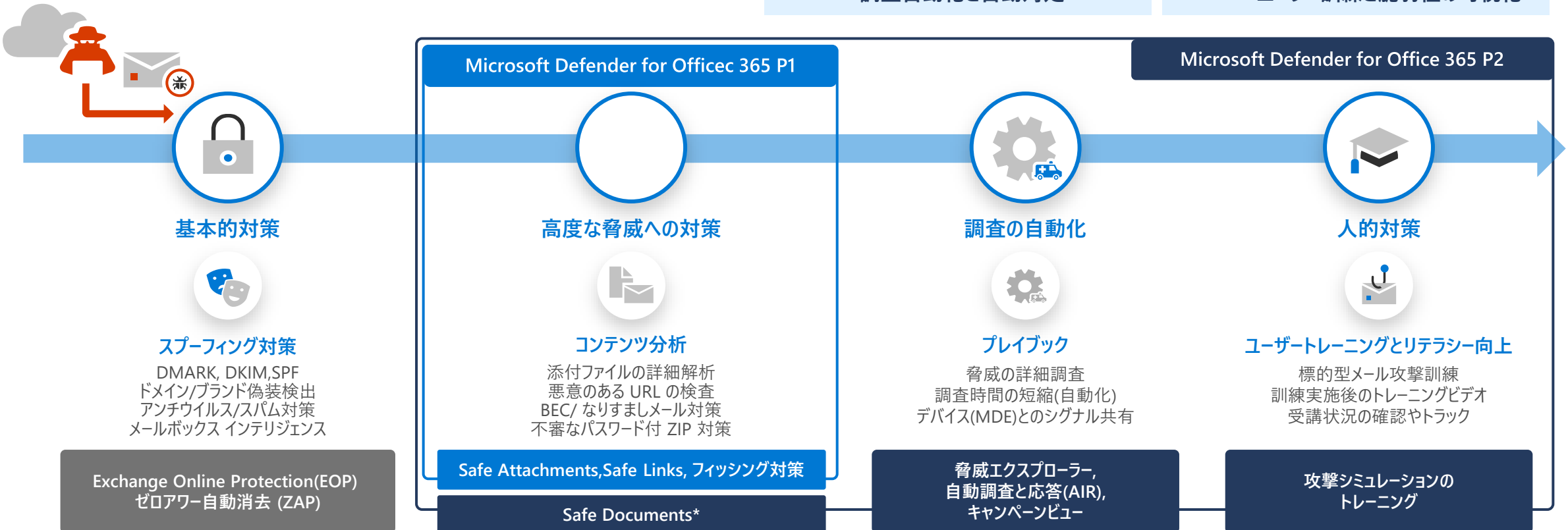
3.5 倍 メールボックスに到達するフィッシング戦術の数

Microsoft Defender for Office 365

メールを介したゼロデイ攻撃や未知のマルウェアからの保護

導入により期待される効果

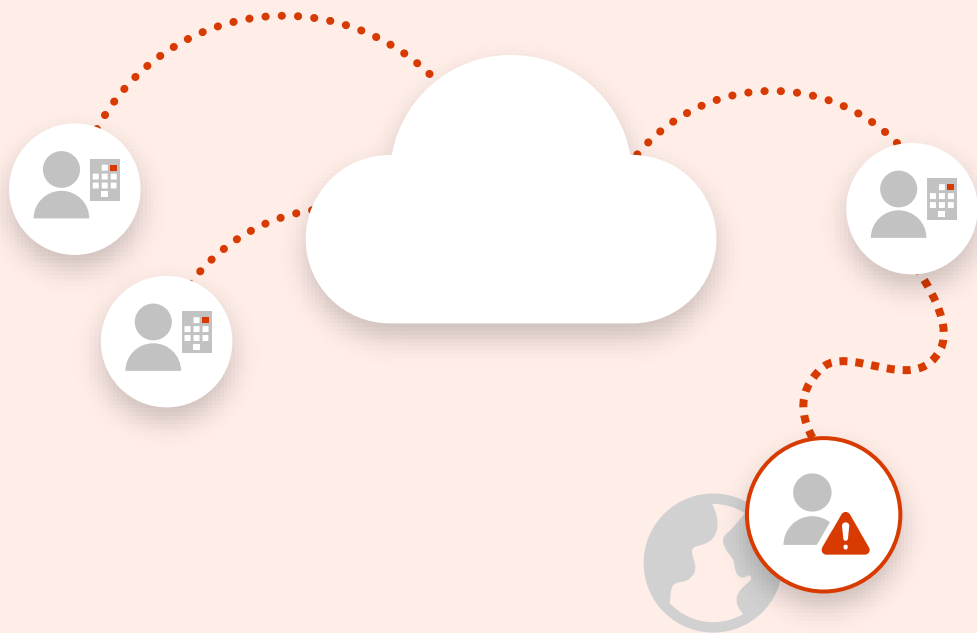
 未知のマルウェア・ウイルスに対する保護	悪意のある URL に対するクリック時のリアルタイム保護
偽装を利用したビジネスメール詐欺(BEC)からの保護	 組織への脅威/侵入状況の可視化と対処
 インシデント発生時の調査自動化と自動対処	 攻撃シミュレータによるユーザー訓練と脆弱性の可視化



不正アクセス

仕事用データへの不正アクセス

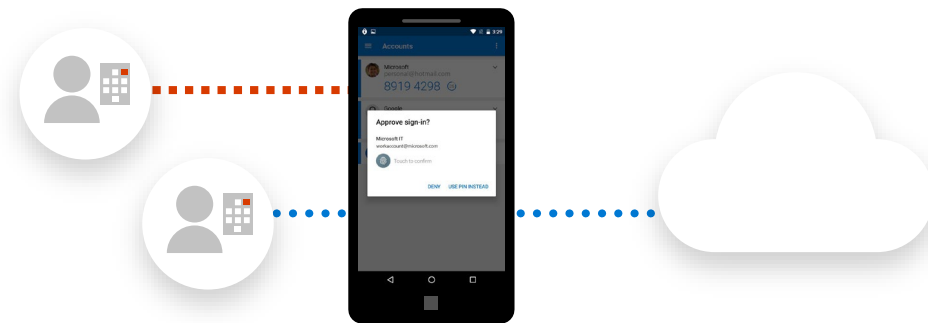
Northwind Traders の従業員は、自宅や外出先で仕事をするときに、作業データにアクセスする必要があります。ただし、悪意のある人物は、パスワードを盗んだり、他の国の仕事データにアクセスしたりしようとするので、仕事情報にアクセスしようとする可能性があります。



防御

仕事用データへの安全なアクセスを実現

Microsoft 365 Business Premium では、高度な多要素認証 (MFA) と条件付きアクセス ポリシーを適用して、いつでもどこでも、適切なユーザーのみが作業データに適切にアクセスできるようにすることができます。ビジネスを行っていない国からのログインが試みられた場合に、アクセスをブロックしたり、追加の認証を要求したりするポリシーを設定できます。



Microsoft Entra ID P1 :

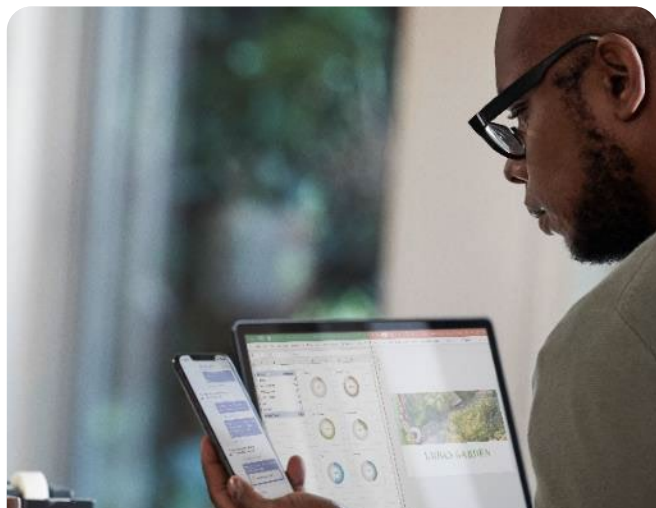
- ✓ 多要素認証
- ✓ 条件付きアクセス ポリシー
- ✓ セルフサービスパスワードリセット

99% の ID 攻撃が多要素認証によって阻止されている

多要素認証でパスワードの紛失や盗難から保護

強力な認証によるユーザー ID の検証

Entra ID の条件付きアクセス機能を使用すると、特定の条件に基づいて環境内のアプリケーションへのアクセスに制御を中央の場所から適用できます。



幅広い多要素認証オプション
をサポートしています

パスワードレス技術を含む



Microsoft
Authenticator



Windows
Hello



FIDO2
security key



Biometrics



Push
notification



Soft
Tokens OTP



Hard
Tokens OTP



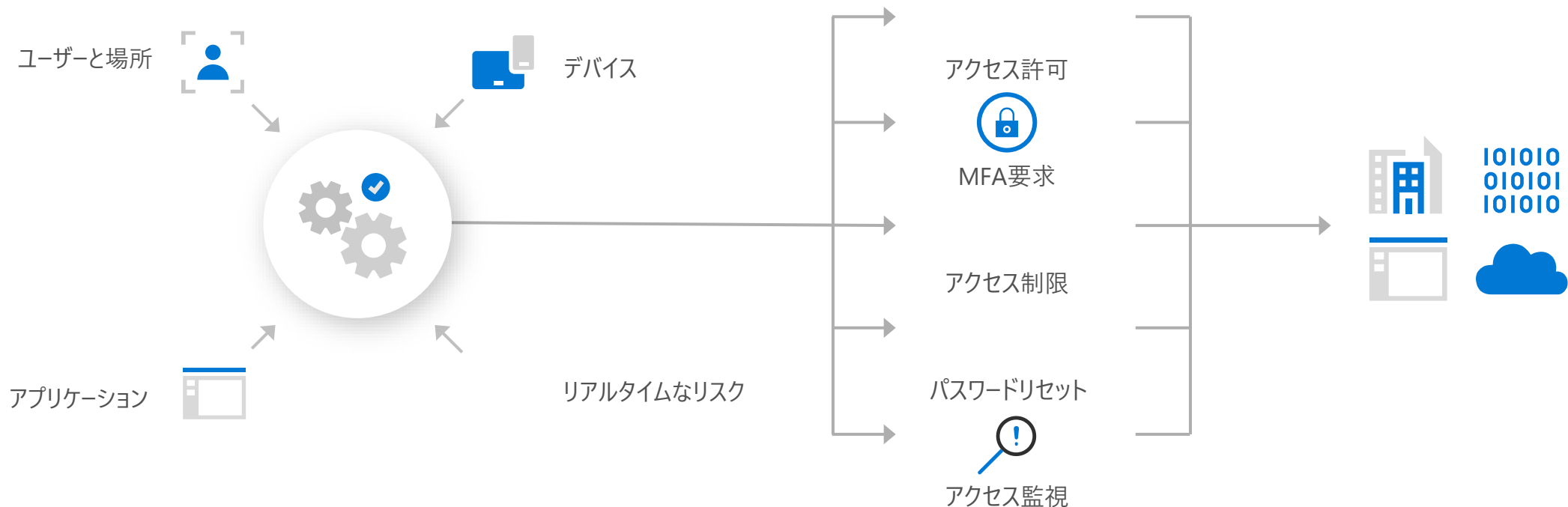
SMS,
voice

多要素認証により

99%

の ID 攻撃を防止

Entra ID 条件付きアクセスと多要素認証で ID とリソースを保護



どこからでも、どんなデバイスでも、セキュアにアプリケーションへアクセス

情報漏洩

不慮のデータ損失やデータ漏洩

Northwind Traders は、会社の機密情報を保護するために、Excel スプレッドシートをパスワードで保護することがあります。しかし、このセキュリティ対策は一貫性がなく、多くの機密文書が保護なしで電子メールで送受信されたり、USBキーに保存されたりしています。



その結果、従業員が退職した場合、機密文書が流出し、ビジネスリスクとなる。

80% の中小企業が PII データを扱っています

データ保護

機密データの保護

Microsoft Business Premium には、Microsoft Purview のラベル付けと情報保護が含まれています。これにより、機密性の高いドキュメントに「極秘」などのラベルを付け、暗号化や転送不可などの保護を適用できます。Copilot for Microsoft 365 を使用している営業担当者がファイルを開こうとします。秘密度ラベルを自動的に継承して尊重し、ファイルの暗号化を解除する前にアクセス許可を確認します。従業員が会社を辞めてドキュメントを USB に保存しても、仕事の資格情報に関連付けられているため、アクセスできません。



55% の中小企業は、従業員が個人デバイスに保存されているデータを持って会社を去ることを懸念している

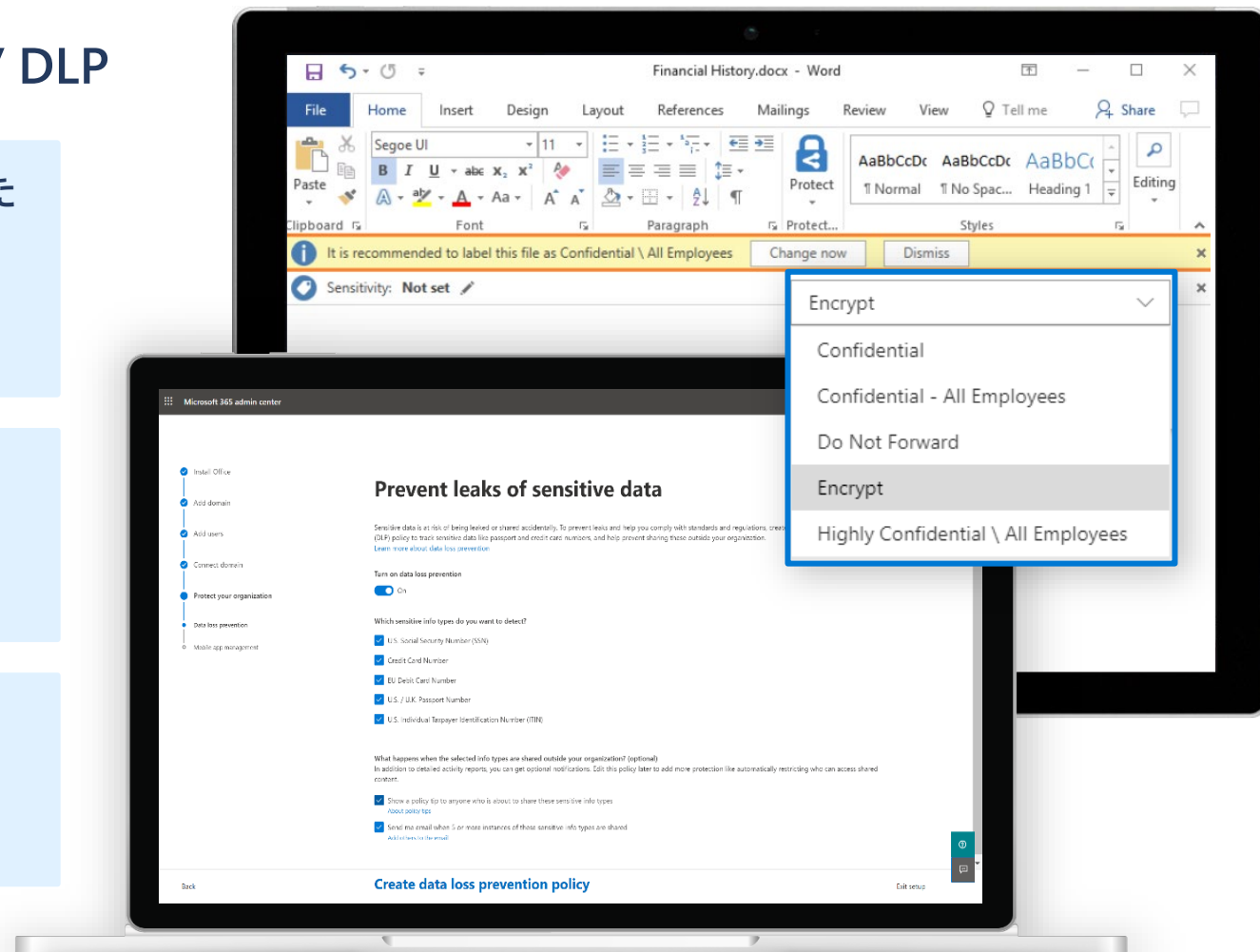
ビジネスデータの保護

Microsoft Purview Information Protection / DLP

HIPAA、PCI_DSS、SSN などの事前設定された DLP ポリシーテンプレートを使用して、クレジットカード番号などの機密情報の共有を防止します。

従業員以外がメールを転送、印刷、閲覧できるかどうかをコントロールできます。

従業員以外が文書を編集、印刷、閲覧できるかどうかを制御できます。また、アクセスを取り消すこともできます。



参考価格

Microsoft 365 Business Premium

サードパーティ ソリューション

8,000円以上/月

セキュリティ、ID、デバイスの管理

リモート アクセス ソリューション	5 ドル
高度なメール保護	5 ドル
シングル サインオン	2 ドル
条件付きアクセスと多要素認証	6 ドル
エンドポイント ウイルス対策	約 3 ドル
エンドポイントでの検出と対応	約 5 ドル
デバイス管理	4 ドル

コラボレーションと生産性

生産性アプリとファイル ストレージ	12 ドル
チャット ベースのコラボレーション	6.67 ドル

インテリジェントな生産性向上



Microsoft 365 Business Premium

3,463円/月

1つのソリューションで
どこからでも安全にビジネスを運営
さらにコストダウンも実現

Microsoft 365 Business Premium +
Microsoft 365 E5 Security

E5 Security へ ステップアップ



Microsoft 365 Business Premium から Security を拡張

Microsoft 365 Business Premium

デバイスのコンプライアンス、位置情報、アプリの感度など事前に定義された条件に基づく標準的な**条件付きアクセス**

会社所有のデバイスと従業員デバイスの**業務データを管理**
紛失または盗難にあったデバイスから業務データを削除

AI を活用した Windows、macOS、Linux、Android、iOS の
エンドポイントセキュリティを実現

マルウェア対策、安全なリンク/添付ファイルによる脅威からの保護を含めた
電子メールとコラボレーションのセキュリティ

電子メールを暗号化し、機密データを検出、分類、手動でラベル付け
および自動拡張アーカイブの有効化有効化



Microsoft 365 E5 Security

アイデンティティエンドポイント、アプリ、電子メールにわたる**包括的な XDR 機能**を提供し、高度な攻撃を検出してアラートを発し対応策を提案

Identity Protection は、AI によるリスク検知と、**漏洩したアカウント、危険なサインイン、ユーザーの行動異常**への自動対応を追加

IoT デバイスと脅威に対するエンドポイントセキュリティの追加ハンティング機能

自動応答機能、侵害後の調査、サイバー攻撃シミュレーション、トレーニング、詳細レポートなどの高度なセキュリティ機能を含む電子メールとコラボレーションのセキュリティ

リスクレベル、異常なユーザー活動、データ共有行動に基づいて
アプリを自動的にブロック

Microsoft 365 E5 Security

セキュリティ強化

Microsoft 365 E5 Security



Identity and access controls

Microsoft Entra ID Plan 2

リスクベースの条件付きアクセス、リアルタイムの動的ユーザーおよびサインイン評価

高度な機械学習を使用したアイデンティティ保護により、危険なサインイン、漏洩したアカウント、インサイダーの脅威を特定

自動化された昇格とアクセス・レビューによる特権アカウントのきめ細かな管理

ユーザーのリスクに応じてリアルタイムにアクセスポリシーを調整



Identity protection

Microsoft Defender for Identity

アイデンティティとインフラストラクチャ全体にわたる脅威と不審なユーザー活動の検出

組み込みのレスポンスと自動化されたプレイブックによる迅速な脅威対策

インシデント調査中に、最近の出来事、アクティビティ、リスクスコアリングなど、コンテキストに富んだアイデンティティに関する洞察を提供

構成に合わせた脆弱性と攻撃経路のモデリング



Device security

Microsoft Defender for Endpoint Plan 2

業界をリードするマルウェア対策

サイバー攻撃サーフェスの削減削減、デバイスベースの条件付きアクセス

包括的なエンドポイント検出と応答 (EDR)

カスタム検出をサポートする高度なハンティング

Secure Score による攻撃対象領域の削減機能



Collaboration security

Microsoft Defender for Office 365 Plan 2

フィッシングやマルウェアなどの高度な攻撃からの保護
ビジネスメールの漏洩やスパムからの保護

電子メール以外のMicrosoft Teams、OneDrive、SharePointへの保護

AI と自動化による 調査、分析、対応

電子メールの脅威に対応

サイバー攻撃シミュレーショントレーニングと詳細レポート



SaaS security

Microsoft Defender for Cloud Apps

完全な SaaS セキュリティ機能
使用中のアプリを検出することで「シャドール IT」を可視化

設定のギャップを発見し、推奨事項を提供する SaaS アプリのセキュリティ姿勢

Oauth に対応したビジネスアプリの監視、

ガバナンス、保護

含まれる機能一覧 Microsoft 365 Business Premium + Microsoft 365 E5 Security

	セキュリティ能力	Business Premium	Microsoft 365 E5 Security
アイデンティティ およびアクセス制御	基本的なアイデンティティとアクセス管理（シングルサインオン（SSO）、多要素認証（MFA）、セルフサービスによるパスワードリセット）	✓	✓
	リスクベースの MFA：ユーザーが認識できないデバイスや見知らぬ場所からリソースにアクセスしている場合、MFA を要求する。		✓
	ログイン行動が異常な場合にのみ MFA を要求するなど、リスク評価に基づいて認証要件を調整する。		✓
	強化されたポリシーによるセルフサービスパスワードリセット。(例)ユーザがセキュリティ質問をパスした場合のみパスワードのリセットを許可する または検証ステップを追加するなど		✓
	AI によるリスク検知は、ユーザーの行動を分析し、危険なアカウントや危険なサインインを検知します。		✓
アイデンティティ・セキュリティ	AI を活用したリスク検知は、ユーザーの行動を分析し、アカウントの漏洩や疑わしい行動（例：不可能な旅行や異常なログイン）を検出します。		✓
	ID ベースの脅威に関する詳細なアラートを提供		✓
	オンプレミスの Active Directory を攻撃から守る		✓
デバイス管理	会社所有および従業員所有のデバイスと業務データを管理	✓	
	紛失または盗難にあったデバイスから業務データを削除	✓	
デバイスのセキュリティ	アンチウイルスやファイアウォールなどの基本機能を備えたエンドポイントプロテクション	✓	✓
	新しい脅威や出現しつつある脅威をほぼ瞬時に検知しブロックする、クラウド配信の保護機能	✓	✓
	異常なシステムアクティビティを検出し、疑わしいプロセスにフラグを立て、攻撃のタイムラインを提供することで、データが盗まれたり暗号化されたりする前に、セキュリティチームが脅威を阻止できるようにします。	✓	✓
	AIR（Automated Investigation and Response）は、ID、電子メール、およびエンドポイントのアクティビティ全体のデータを即座に関連付けます； 漏洩したアカウントを検出した場合、自動的にアクセスを無効化し、デバイスを隔離してインシデント・レポートを作成します。		✓
電子メールと アプリのセキュリティ	シンプルなフィルタリングによるフィッシングやマルウェアからの基本的なメール保護	✓	✓
	電子メール、Microsoft Teams、SharePoint、OneDrive 内のファイルやリンクを、開いたり共有したりする前に自動的にスキャンします； ファイルやリンクが安全でない場合、被害を防ぐためにブロックされます。	✓	✓
	高度なフィッシング詐欺、なりすまし攻撃、電子メール詐欺を検知して阻止するAI主導のフィッシング対策	✓	✓
	誰が標的になっているのか、どの攻撃がブロックされたのか、組織の潜在的弱点に関する詳細なレポート		✓
クラウド・アクセス・セキュリティ	従業員が使用しているアプリを表示	✓	✓
	従業員がどのようなアプリを使用しているかを示し、その安全性を評価する。		✓
	危険なアプリを自動的にブロックまたは制限する		✓
	奇妙なファイルアクセスパターンや異常なダウンロードなど、クラウドアプリの不審な動作を検出します。		✓
データ・セキュリティ	機密メールの暗号化	✓	
	機密データの発見、分類、手動ラベル付け	✓	

Microsoft Entra ID によるリスクの検出

アカウントの侵害や攻撃者の侵入を検出

サインインリスク

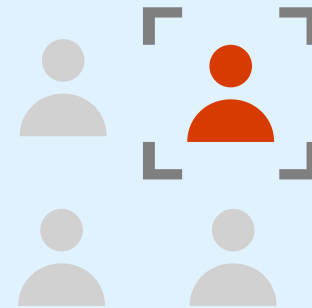
ユーザーの普段と異なる怪しいサインインを自動検出

🔥 コントソ株式会社



ユーザーリスク

侵害されたアカウントを自動検出



Microsoft Entra ID による脅威保護

ライセンス	Microsoft Entra ID P1			Microsoft Entra ID P2		
機能	サイン画面のカスタマイズ	多要素認証	アクセス制御	なりすまし検出	侵害状況の可視化	特権IDの管理
イメージ						
攻撃者	ID を不正に入手		なりすまして侵入		不正な侵害	

Challenge

ランサムウェア

一年で最も忙しい時期に、ノースウインド・トレーダーのミッション・クリティカルなファイルが使用不能になった。ハッカーはランサムウェアを使ってノースウインドのファイルを暗号化し、暗号化「キー」の代金を要求した。ノースウインド社は暗号化「キー」の代金を支払わなければデータを失う、その結果、廃業に追い込まれた。



275%

2022年から2024年にかけてのランサムウェア攻撃の増加*

*Source: Microsoft Digital Defense Report, 2024

Solution

ランサムウェア対策

Microsoft 365 E5 Securityでは、従業員デバイスはMicrosoft Defender for Endpoint P2で保護され、多層的なランサムウェア対策により攻撃を未然に防ぐことができます。AIによる自動攻撃阻止機能を備えたエンドポイント検知レスポンスは、手動攻撃や標的型攻撃を防御し、ネットワーク経由での攻撃を阻止します。



3x

暗号化段階に達した身代金攻撃は、過去2年間で3倍に減少している*

Microsoft Defender for Endpoint

OS 組み込み型 クラウドベースエンドポイントセキュリティ

導入により期待される効果

アンチウイルスでは検知できなかったデバイス上での脅威を可視化

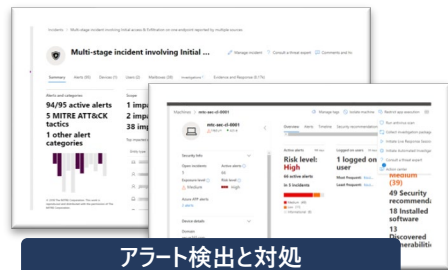
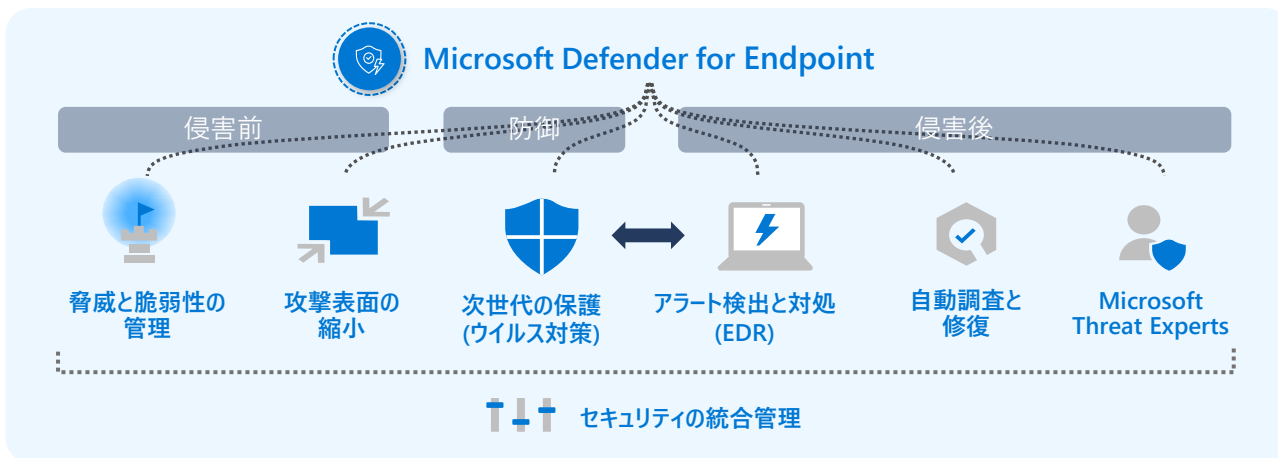
自動的にアラートを調査し、複雑な脅威の修復を数分で完了



Microsoft の脅威インテリジェンスを活用した脅威検出の実現

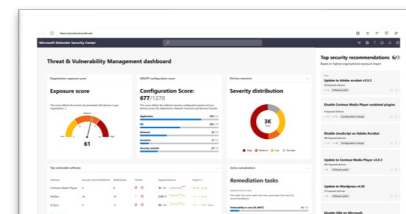
脆弱性や構成誤りを検出し、優先度を決定して修復

Microsoft Defender for Endpoint



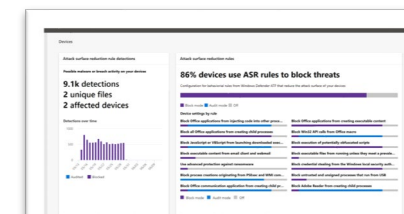
アラート検出と対処

- デバイス上のプロセスの挙動を時系列的に解析し脅威判定
- IoC に加え IoA を用いた未知の攻撃検出にも対応
- 侵害活動により発生した複数のアラートをインシデントとして一元化
- 脅威判定に利用した情報は証拠として一元的に参照可能
- インシデントやアラートのログから、脅威にさらされたデバイスやファイルを確認し、必要に応じて様々なアクション(特定のプログラムの実行をブロック、デバイスをネットワークから分離、調査パッケージの収集など)を実行可能
- Live Response 機能により、リモートからデバイスにアクセスし詳細な調査作業をすることが可能



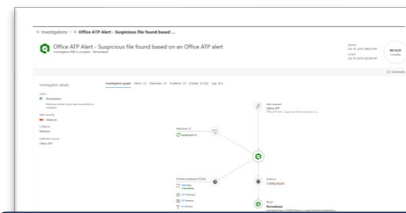
脅威と脆弱性の管理

端末の構成や 3rd Party ソフトウェア含む既知の脆弱性情報を元に企業内のリスクを定量的に可視化し、優先順位を付けた対策を示唆



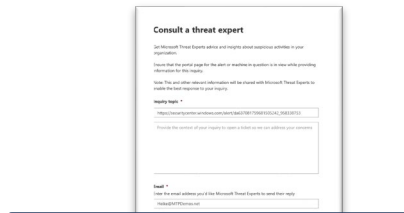
攻撃表面の縮小

攻撃者によって悪用されることが多いソフトウェア動作を 15 のルールを基にブロックすることが可能



自動調査と修復

Automated Investigation 機能により検出したアラートを自動的に調査し、複雑な脅威による影響を数分で修正



専門家による調査

専門家の深い知識による、SOC への脅威分析のアドバイスを実施 (追加のサービス契約が必要)

Challenge

アイデンティティは 新しいセキュリティの境界線

ID は最も一般的な攻撃ベクターの 1 つである。
ID ベースの攻撃の速度、巧妙さ、規模は飛躍的に増大している。
指数関数的に増加している。

7,000

パスワード攻撃は
2023 年の 4,000 件から
2024 年には毎秒 2,000 件に
増加する。

+111%

トークン盗難攻撃
を受けた。

60 秒

攻撃者がフィッシングから
個人データにアクセスする
までの時間の中央値。

攻撃者が組織内で貴重な足がかりを得るには、
たった 1 つの設定ミスや保護のギャップが必要なだけであり、
今日の複雑な ID 環境は十分な機会を提供している。

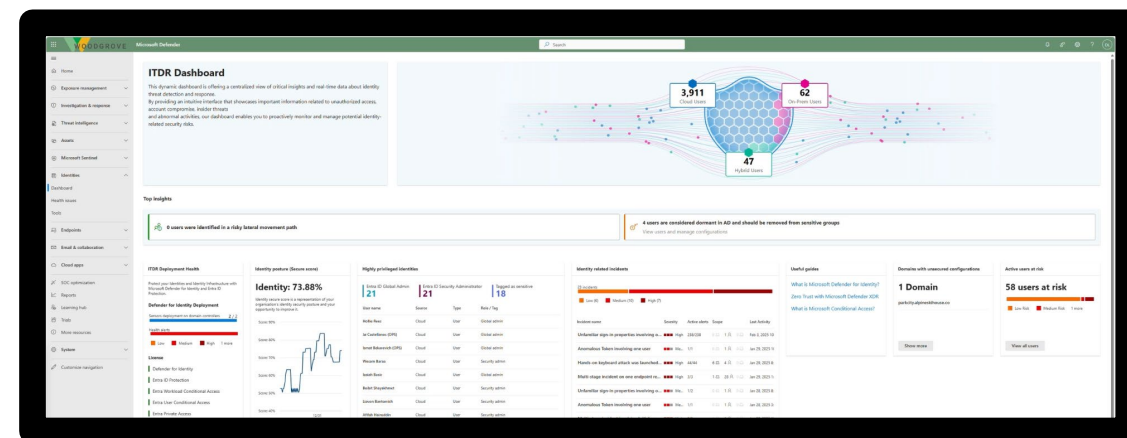
1 危険にさらされたアイデンティティは、
最も強固なセキュリティ慣行でさえも構成する。

Solution

Microsoft Defender for Identity

Microsoft Defender for Identity は、Microsoft Defender XDR の統合部分として、
ID 特有のセキュリティ機能を提供します。

オンプレミスアイデンティティ専用センサー EntralID のためのネイティブ統合と、
他の一般的なソリューションのための双方向コネクタを組み合わせることで、
Defender for Identity は、独自のアイデンティティ環境を包括的に保護します。
強力な ID 特異的検出が自動的に強化されるし、
他のドメインからのデータと相関させることで、比類のない洞察力と
洞察力とインシデントレベルの可視性を提供します。



Microsoft Defender for Identity

オンプレミス Active Directory の資格情報に対する不審な挙動検出

導入により期待される効果

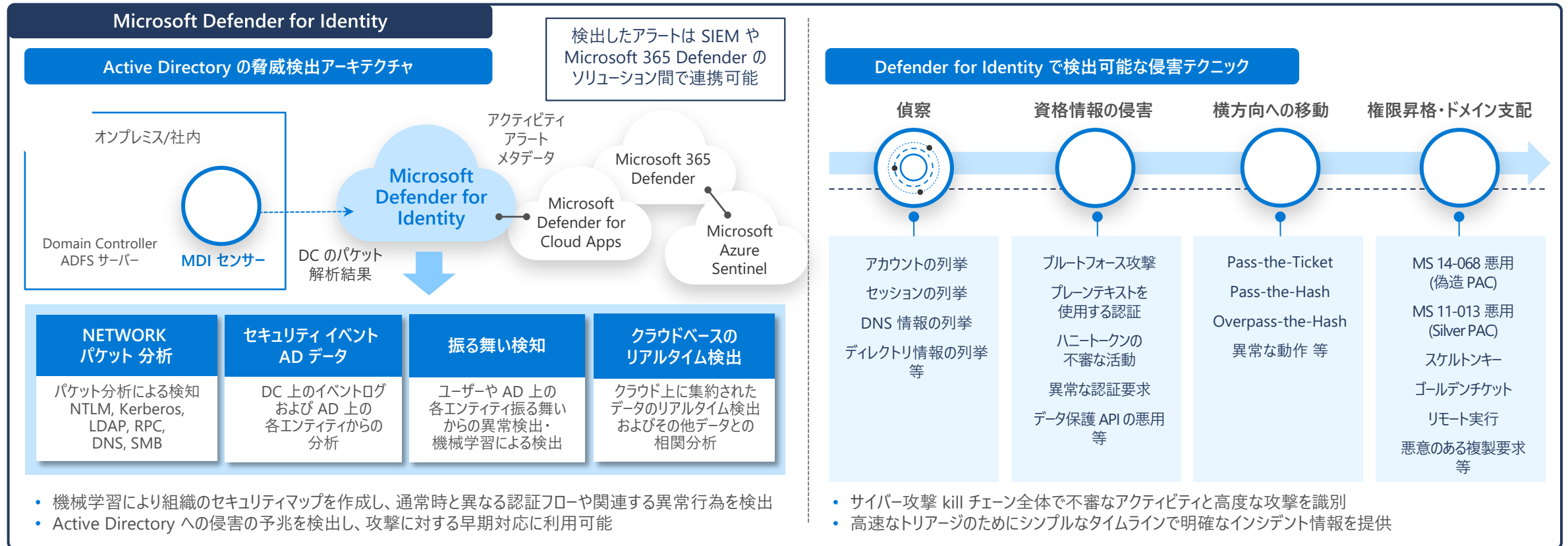
Active Directory / ADFS での資格情報の不正利用を検知

機微なユーザーの利用や機微なグループの変更などを可視化



サイバーキルチェーン全体で高度な脅威を識別可能に

ユーザー ID を保護して攻撃対象領域を削減するための分析情報を得る



Microsoft Defender for Cloud Apps

Office 365 とその他のクラウドサービスの監視とポリシーの適用

導入により期待される効果

組織のシャドウ IT 利用状況の検出とアクセス制御が可能

SaaS 上でのサイバー攻撃の脅威と異常なアクティビティからの保護

迅速にセキュアなテレワーク環境を実現

Microsoft Defender for Cloud Apps

シャドウ IT の検出と評価

- Defender for Endpoint のセンサーや、Proxy/Firewall のログから SaaS アプリの利用状況を検出
- 検出された SaaS アプリのリスクスコアの可視化
- Defender for Endpoint と連携して、企業が未承認のアプリへのアクセスをブロック

Threat Protection 脅威からの保護

SaaS アプリのセッションに対する脅威

オンプレミスの ID に対する脅威

クラウド上の ID に対する脅威

アクティビティ ポリシーの例

- 大量のファイルダウンロード
- 疑わしい受信トレイの転送
- 悪意のある OAuth アプリの同意
- 複数回のログイン試行の失敗 など

セッション制御 - Entra ID 条件付きアクセスの拡張

※ セッション制御の対象は Web ブラウザーからのアクセスのみに限定

管理されていないデバイス

データの閲覧は許可

データのダウンロードは禁止

- Entra ID 条件付きアクセスの機能を拡張し、条件に応じたセッションの制御を実現
- 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アクセス制御を実施可能
- セキュリティと業務継続性の両立を実現

- 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脅威判定
- 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
- Entra ID Identity Protection や Microsoft Defender for Identity と統合

参考価格

Microsoft 365 E5 Security

個別ライセンス

4,230円/月

Microsoft Defender

Defender for Endpoint P2	¥780
Defender for Office 365 P2	¥750
Defender for Identity	¥825
Defender for Cloud Apps	¥525

Microsoft Entra

Entra ID Plan 2	¥1,350
-----------------	--------



Microsoft 365 E5 Security

1,800円/月

Save ~57% per license
エンド・ツー・エンドのセキュリティを実現

Microsoft Defender for Cloud

Azure プラットフォーム のセキュリティ対策



Microsoft Defender for Cloud

Azure ネイティブな CSPM / CWPP

- コンプライアンスの評価やリスク・脆弱性の発見を行い、ポリシーの強制を行うことで誤設定や管理ミスリスク軽減をサポート
- サーバー EDR 機能や PaaS サービスへの脅威保護を行う
- Azure だけでなくオンプレミスや AWS / GCP といったハイブリット環境にも対応

導入により期待される効果

構成管理・ミスによるセキュリティインシデントを防ぐ	脆弱性対策などの自動化
PaaS 領域に関するセキュリティ向上	ハイブリット環境における一元管理

Microsoft Defender for Cloud

クラウドセキュリティ態勢管理 : CSPM (Cloud Security Posture Management)

各種クラウドサービス



API やエージェントからリアルタイムで情報収集

コンプライアンスの評価

リスク・脆弱性の発見

構成ミスの発見

ポリシーの強制

新たなクラウドセキュリティソリューションの考え方

- クラウドサービスでの構成ミスや管理の不備を検知

インベントリ管理



全ての監視対象リソースをシングルビューで表示
推奨事項や脆弱性の確認もここで一元管理

セキュアスコア



組織全体のセキュリティ状態を指標に基づいて可視化

- 重要度やベストプラクティスの提示のほか、設定したポリシーに基づいた改善点も表示
- 規制コンプライアンスの対応なども対応
- セキュリティポリシーの管理・割り当ての実行

推奨事項への対処の自動化



Logic Apps の Playbook を利用して
特定の推奨事項に対するワークフローの自動化が可能

クラウドワークロード保護プラットフォーム : CWPP (Cloud Workload Protection Platform)



SQL



VMs



Containers

IaaS、PaaS、コンテナなど
各ワークロードの種類に合わせた保護や脅威検知を提供

- ファイル改ざん検知やアプリケーション制御、適応型ネットワーク強化などサーバーのハードニングに必要な機能群を提供
- EDR によるサーバーの振る舞い検知
- SQL や Storage、Kubernetes などの PaaS サービスに対して不正アクセスや不正操作などの脅威を検知



Apps



IoT



Network

マルチクラウド環境への対応



Azure Arc

Azure Arc を利用し、ハイブリットクラウド環境に対して
AWS、GCP、オンプレミス製品の構成管理や規制コンプライアンス対応などが可能



#digitaltrust

- 本書に記載した情報は、本書各項目に関する発行日現在の Microsoft の見解を表明するものですMicrosoftは絶えず変化する市場に対応しなければならないため、ここに記載した情報に対していかなる責務を負うものではなく、提示された情報の信憑性については保証できません
 - 本書は情報提供のみを目的としています Microsoft は、明示的または暗示的を問わず、本書にいかなる保証も与えるものではありません
 - すべての当該著作権法を遵守することはお客様の責務ですMicrosoftの書面による明確な許可なく、本書の如何なる部分についても、転載や検索システムへの格納または挿入を行うことは、どのような形式または手段（電子的、機械的、複写、レコーディング、その他）、および目的であっても禁じられていますこれらは著作権保護された権利を制限するものではありません
 - Microsoftは、本書の内容を保護する特許、特許出願書、商標、著作権、またはその他の知的財産権を保有する場合がありますMicrosoftから書面によるライセンス契約が明確に供給される場合を除いて、本書の提供はこれらの特許、商標、著作権、またはその他の知的財産へのライセンスを与えるものではありません
- © 2025 Microsoft Corporation. All rights reserved.
Microsoft, Windows, その他本文中に登場した各製品名は、Microsoft Corporation の米国およびその他の国における登録商標または商標です
その他、記載されている会社名および製品名は、一般に各社の商標です