Microsoft

Microsoft Security で実現する
マルチクラウド セキュリティ

Microsoft Azure Security

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

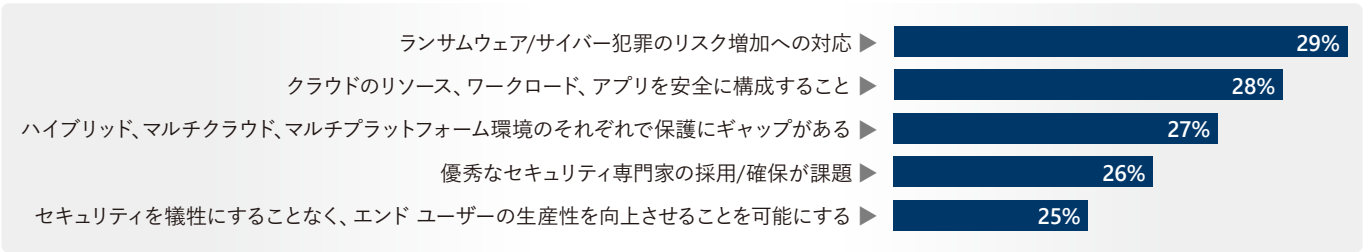
企業を狙うサイバー攻撃はその数だけでなく、巧妙さも上昇しています。急速にテクノロジ導入が進み、ハイブリッド ワークが増加していますが、予算の制約やセキュリティ専門の人材不足という悩みを持つ組織にとってはリスクが増大します。また、マルチクラウドの利用増加や多様な規制環境への対応が求められており、組織はこれまで以上に厳しいセキュリティの課題に直面しています。

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

CISO の最優先事項 御社における最優先事項は何ですか?

世界のセキュリティ リーダーが考えていること

https://www.microsoft.com/en-us/security/blog/2022/01/25/how-cisos-are-preparing-to-tackle-2022/



マルチクラウド環境をセキュアにするために直面する課題 Top-of-mind

クラウド上での セキュアなアプリの開発・運用

>54%

DevOps パイプラインに セキュリティが統合されていない エンタープライズ環境 *3

セキュリティ・コンプライアンスの 可視性

86%

自社のサイバーセキュリティ戦略が マルチクラウド環境に追いついていないと 考えている意思決定者の割合 *4

攻撃手法の高度化と 攻撃頻度の増加

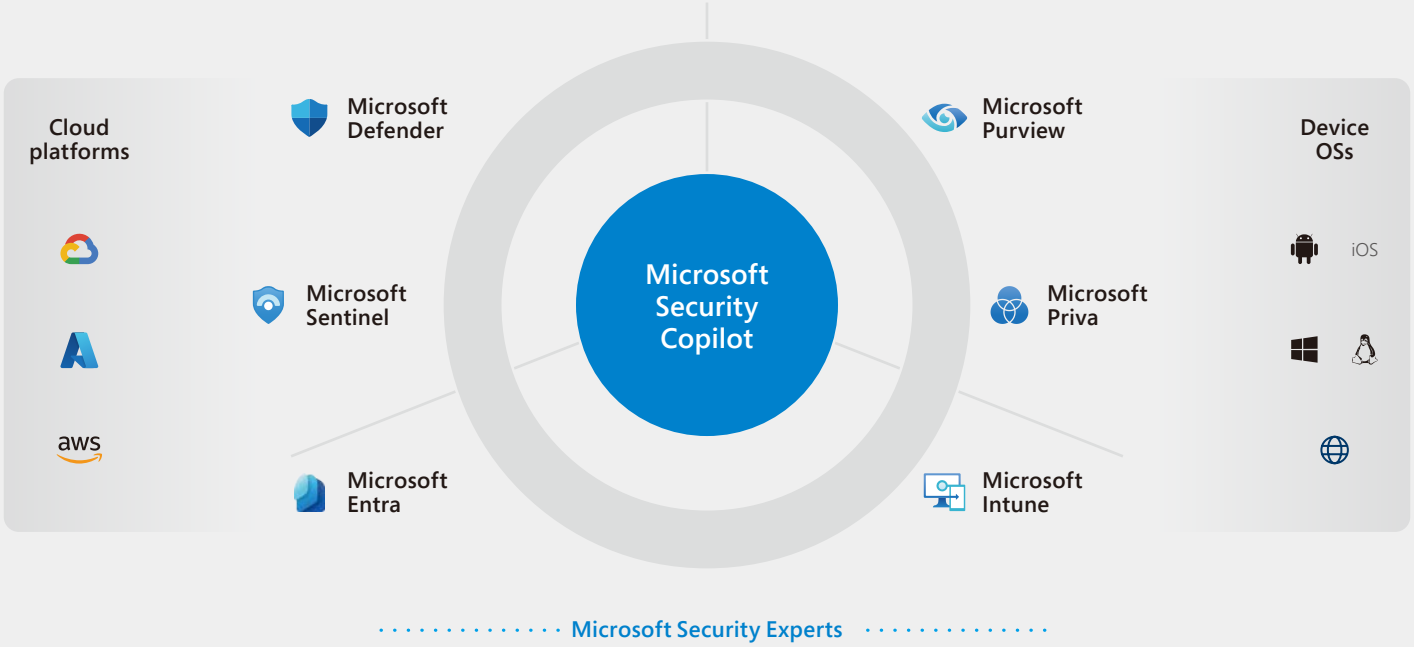
$4.24M

2021 年の侵害に関する 平均的なコスト *5

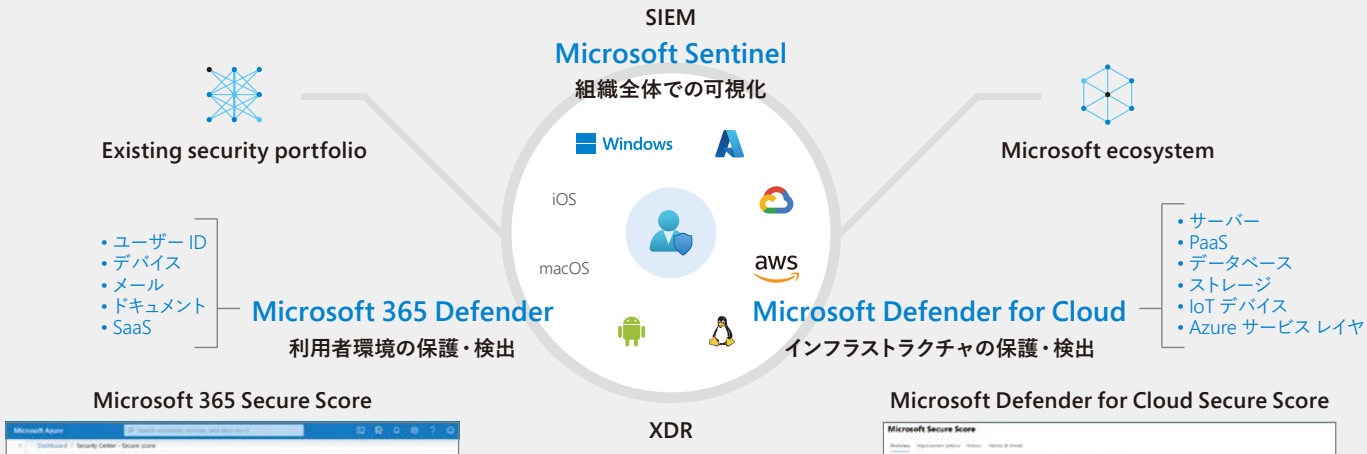
*3 Microsoft Enterprise DevOps Report *4 Microsoft Cloud Security Priorities and Practices Research *5 Ponemon Institute, Cost of a Breach Report

Microsoft Security ポートフォリオ

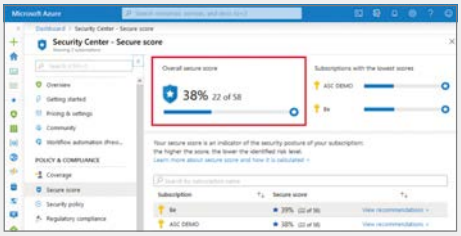
Security Copilot では、お客様のデータは常にお客様のデータとなります。ユーザーの境界内にとどまり、基礎となる AI モデルの学習には使用されません。実際、最も包括的なエンタープライズのセキュリティ & コンプライアンス制御によって保護されています。これらはすべて、Microsoft Security 製品ポートフォリオの中心にある Security Copilot と連携しています。



マイクロソフトは、セキュリティ情報イベント管理 (SIEM) を提供する Microsoft Sentinel、インフラストラクチャの保護と検出を行う Microsoft Defender for Cloud、利用者環境の保護と検出を行う Microsoft 365 Defender が連携したソリューションにより、お客様のマルチクラウド環境を全包囲で保護します。また、2 つの Microsoft Secure Score による脆弱性と成熟度の管理により、組織のセキュリティの状態をすばやく把握し、マルチクラウドにおけるセキュリティ目標を達成することが可能になります。



Microsoft 365 Secure Score

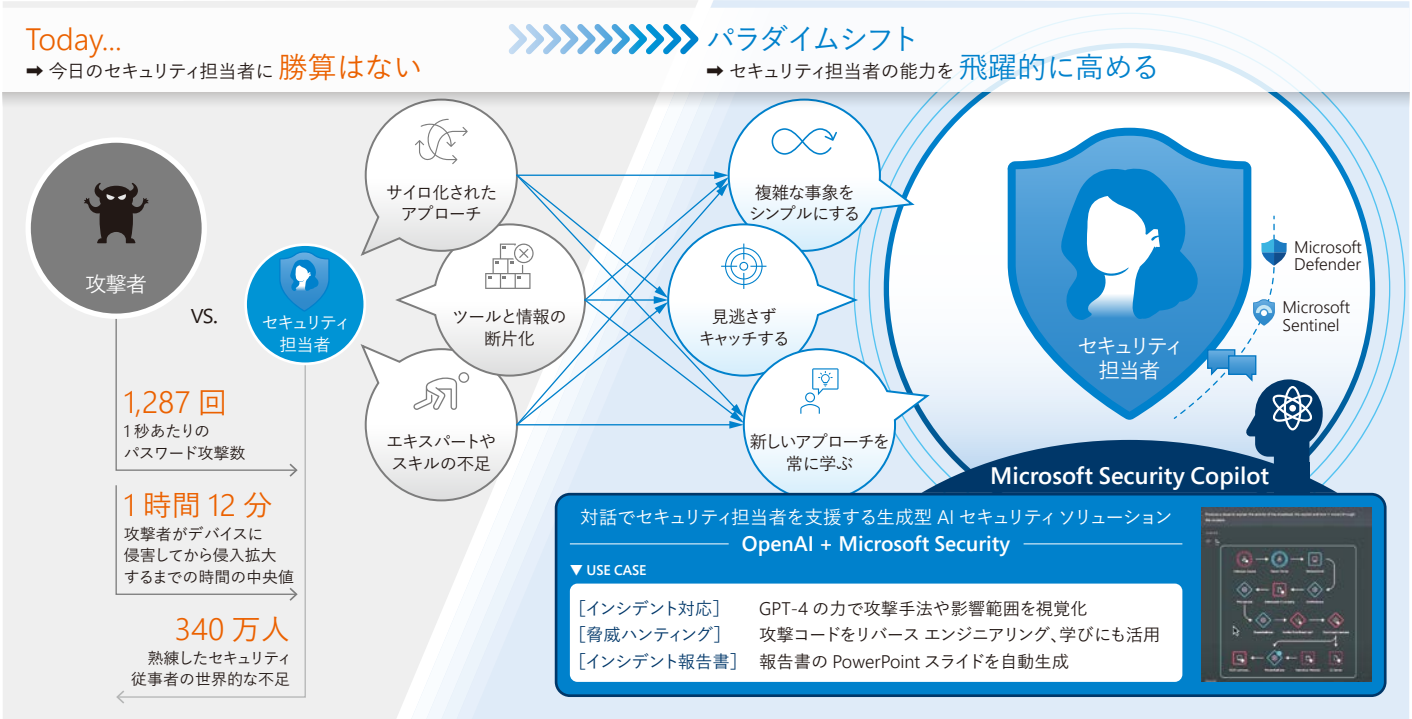


Microsoft Defender for Cloud Secure Score

クラウドの可視化と制御

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。



Microsoft Sentinel

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。 Microsoft Sentinel を使用すると、攻撃の検出、脅威の可視化、予防的ハンティング、脅威への対応のための単一ソリューションをすばやく導入できます。

デジタル資産全体を保護

- 広範なコンテンツをパッケージ化、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
- 225 種類以上の標準の統合により、即日利用を開始
- SAP、Dynamics などで脅威を検出、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

- 広範なトレーニングを行った AI とインサイトによる推奨事項を活用
- UEBA、自動化、ハンティング機能などの統合で調査と対応を迅速化

効率的に検出、対応

- あらゆる種類のデータの脅威を高速にハンティング
- 機械学習により、アラートをインシデントに自動関連付け
- ユーザーの異常な行動を特定し、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

- インフラのセットアップやメンテナンスが不要、拡張も自由
- 組織全体からクラウド規模のデータを収集、分析
- 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が協力

Microsoft Sentinel

クラウドと AI を活用した最新のセキュリティ運用

クラウドにより無制限の速度とスケールを実現

進化する脅威を検出

インシデント対応を迅速化

攻撃者の先をいく

Microsoft よる SIEM と XDR 統合は、最先端のエンドツーエンドの包括的な脅威保護ソリューションを提供します

包括的な機能

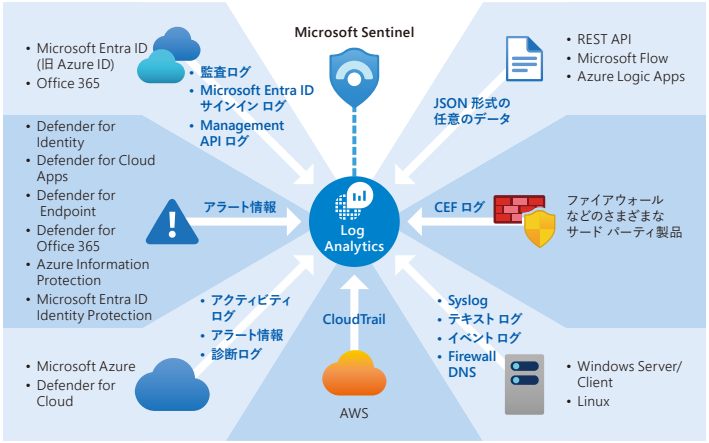
- クラウド スケールの保護
- 組み込みの UEBA と ML による分析
- Microsoft のセキュリティ エキスパート
- 自動検出、調査、修復
- プロアクティブな脅威ハンティング
- エコシステム統合

Microsoft Defender と Microsoft Sentinel の連携

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。各 Defender との連携により、クラウドと AI を使用した次世代セキュリティ運用基盤を構築できます。

幅広いデータ ソースからデータを収集

- 容易にログを取り込むためのコネクタを提供し、さまざまなデータ ソースからデータを収集可能



Defender との連携、独自クエリや AI による検知

- Microsoft XDR で検出された脅威を自動登録
- セキュリティ専門家による組み込みのアラート ルール
- クエリによる脅威検出や組み込みの機械学習モデルを利用可能

インシデント管理による調査

- 各インシデントのオーナー、重要度、ステータス、コメントを統一的に管理可能
- アラートやインシデント間の相関分析機能を提供
- インシデント管理もオートメーション (SOAR) 機能に統合し、対処の自動化が可能

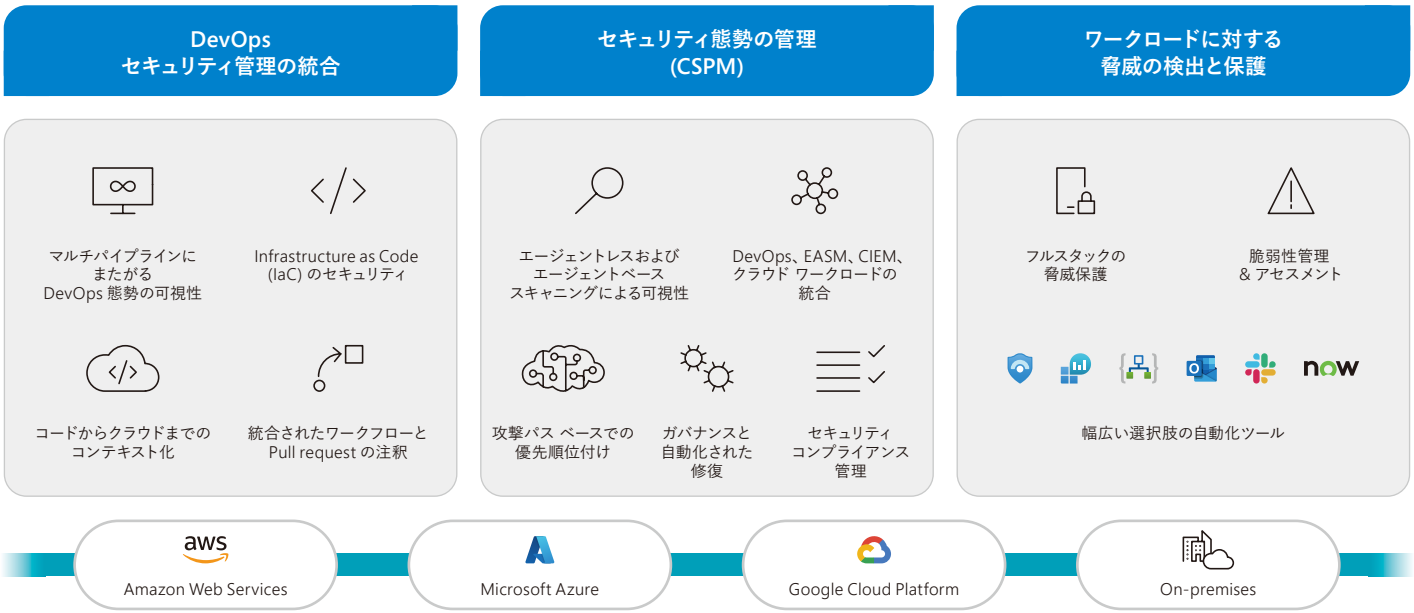
脅威への対応を自動化

- Microsoft Sentinel の Security Playbook では、250 種類以上のコネクタを利用し、アラートに対する対処手順を予め定義することで発行時にワークフローを自動実行可能

クラウドの可視化と制御

Microsoft Defender for Cloud

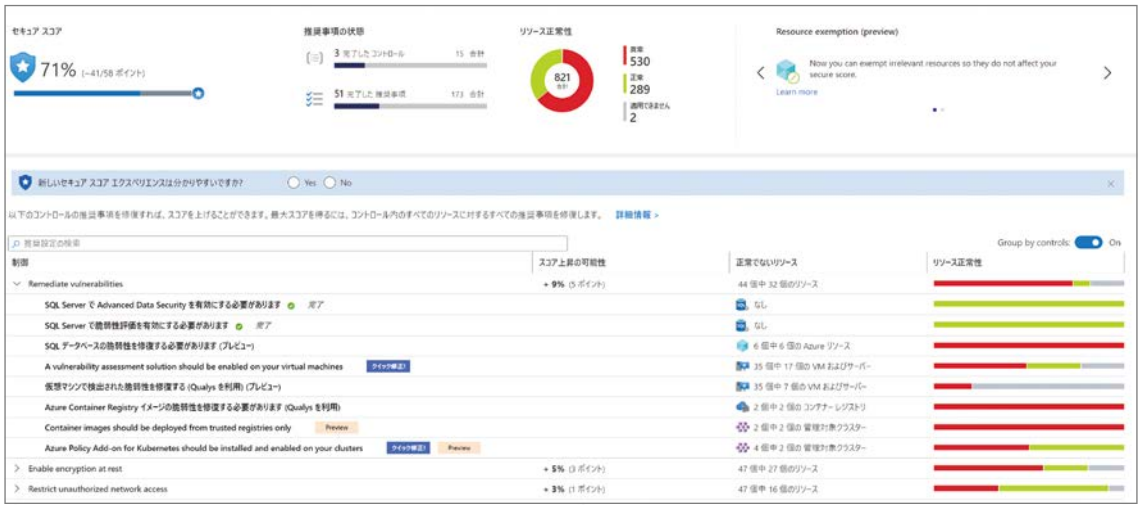
Microsoft Defender for Cloud は、クラウドとオンプレミス環境に渡って
クラウド ネイティブなアプリケーションを保護します。



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。

クラウド セキュリティ態勢管理 (CSPM)

- コンプライアンスの評価、リスクや脆弱性の検出、ポリシーの強制によって、誤設定や管理ミスによるリスクを軽減
- 組織のセキュリティ状態を可視化し、重要度やベスト プラクティスも提示、規制やコンプライアンスにも迅速に対応
- 全ての監視対象リソースを表示し、推奨事項や脆弱性も一元管理可能、また 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

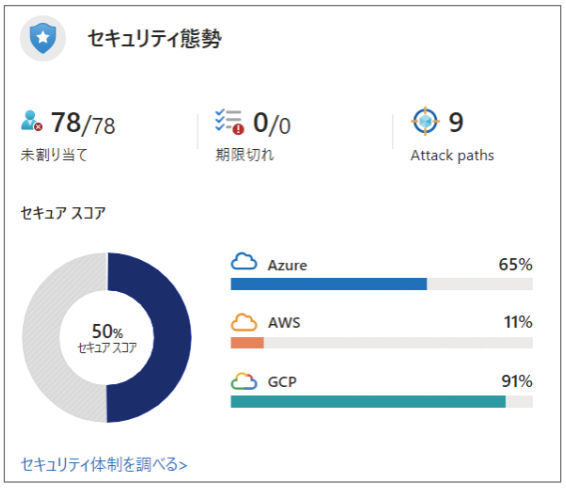


Microsoft Defender for Cloud のプラン一覧 (2022 年 7 月現在)

- Microsoft Defender for Servers
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Containers
- Microsoft Defender for App Service
- Microsoft Defender for Key Vault
- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS
- Microsoft Defender for open-source relational database
- Microsoft Defender for Azure Cosmos DB

クラウドワークロード保護プラットフォーム (CWPP)

- IaaS、PaaS、コンテナーなどのワークロードの種類に合わせた保護や脅威検知が可能
- ファイル改ざん検知やアプリ制御、適応型ネットワーク強化などのサーバーのハーデニングに必要な機能群を提供
- EDR (検出と応答) 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



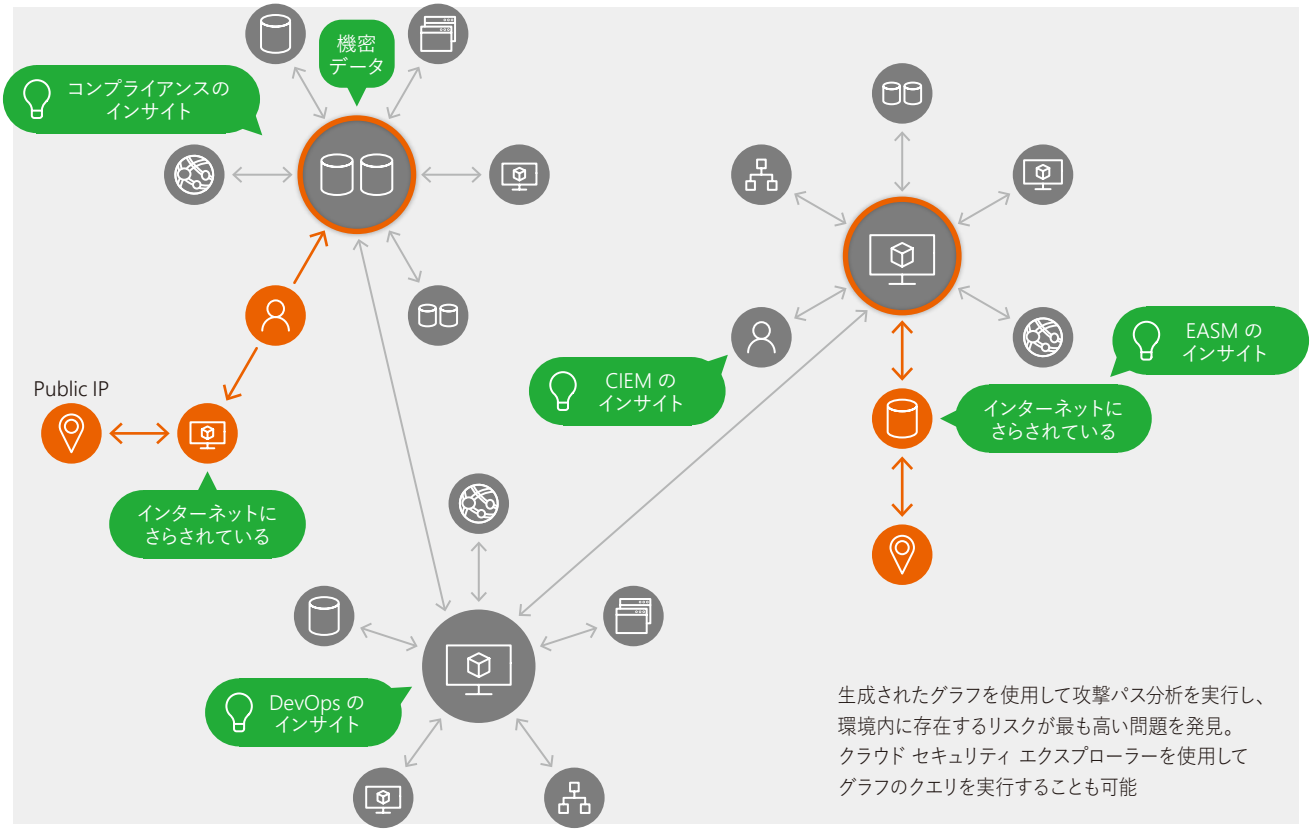
マルチクラウド環境への対応

- ハイブリッド 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、規制やコンプライアンスへの対応が可能

攻撃影響範囲を分析するクラウド セキュリティ グラフ

- Defender for Cloud 内に存在するグラフ ベースのコンテキスト エンジン
- 状況に応じたセキュリティ インサイトを使用して、横方向への移動経路を特定し、優先順位付け
- DevOps、EASM、CIEM、コンプライアンス、Data を意識した態勢管理を統合して、コンテキスト データを使用

リスクを評価し、最も早期に解決する必要がある最もリスクの高い問題を特定する



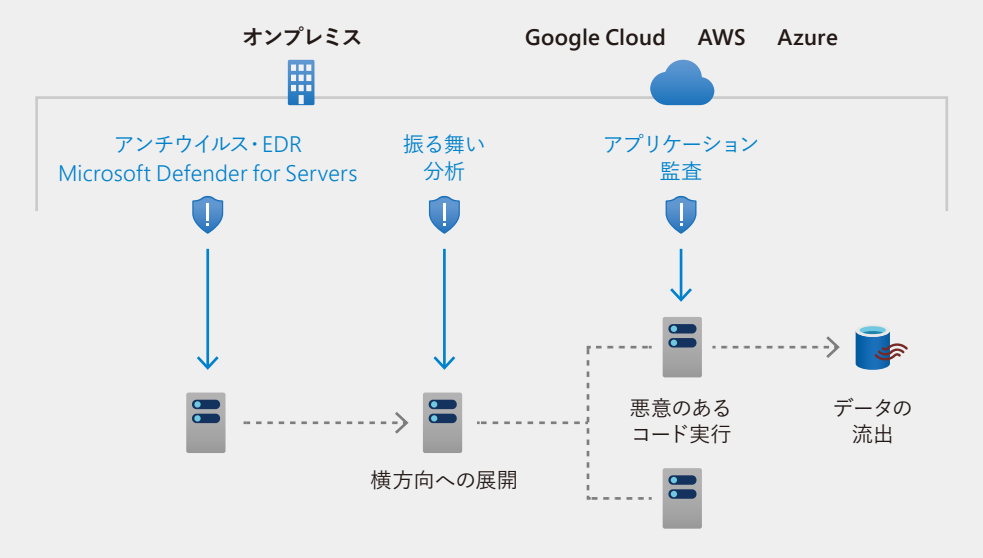
クラウドの可視化と制御

Microsoft Defender for Servers

Microsoft Defender for Servers は、Azure、AWS、GCP、オンプレミス環境で実行されている Windows マシンや Linux マシンの脅威検出と高度な防御を提供します。

Windows や Linux のサーバーを脅威から保護

- Azure Arc を経由することで、オンプレミスやマルチクラウド環境にも対応可能

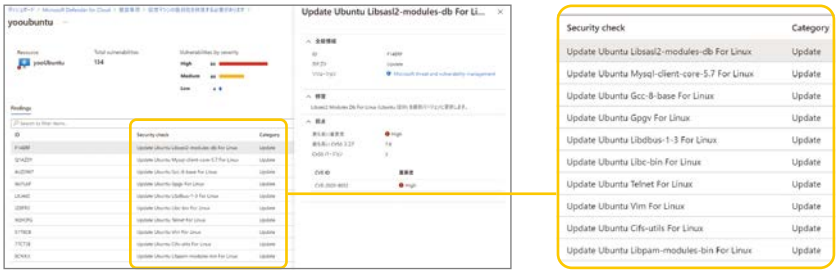


Microsoft Defender for Endpoint との統合

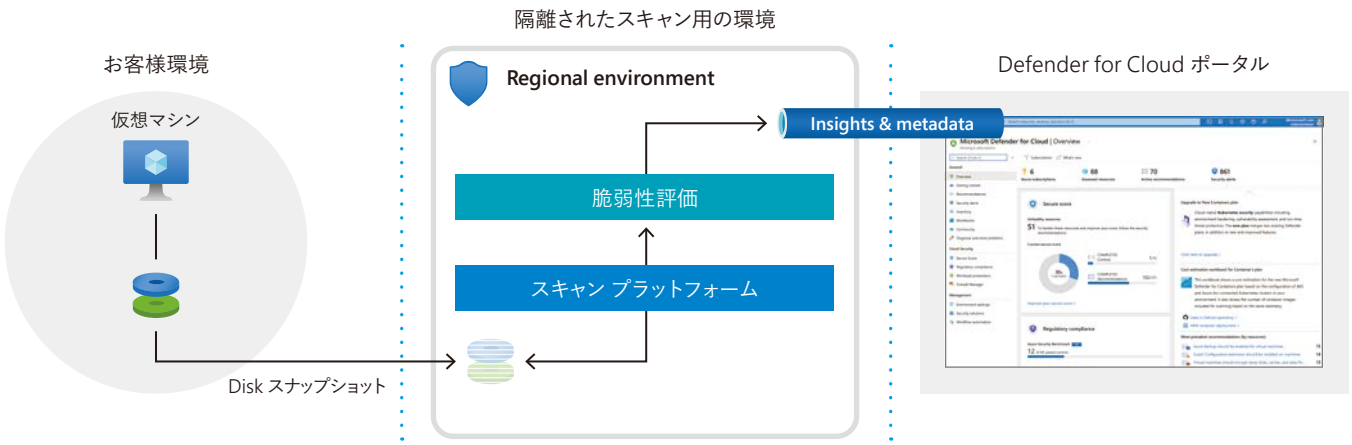
- Microsoft Defender for Endpoint との統合により、クライアント デバイスを含めたセキュリティ オペレーションを一元化
- Microsoft Defender for Cloud に追加された Windows や Linux サーバーは、Microsoft Defender for Servers にも自動的に追加

サーバー環境の脆弱性評価

- クラウド上の IaaS 環境、あるいはオンプレミスの Windows や Linux のサーバーに対して、Defender for Endpoint のエージェントと TVM による脆弱性管理の仕組みを提供
- 脅威と脆弱性について継続的な評価を行い常に適切な構成でサーバーを運用可能



エージェントレス スキャンのプラットフォーム

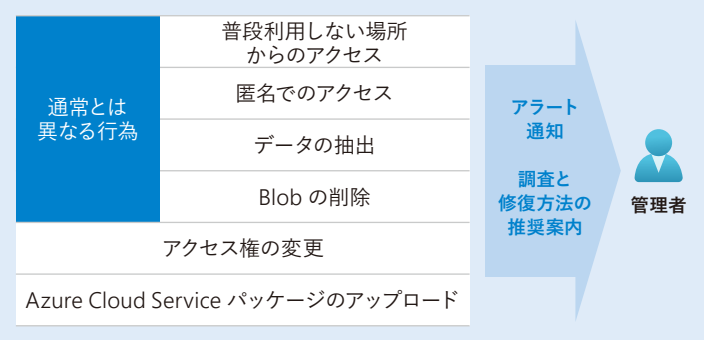


Microsoft Defender for Storage

Microsoft Defender for Storage は、Azure Storage (Blob、Files、Data Lake Storage) を対象としたクラウド ストレージの脅威検出と保護機能を提供します。

有害な可能性のあるアクティビティを検出

- セキュリティ AI の高度な機能と Microsoft の脅威インテリジェンスを利用して、コンテキストに応じたセキュリティ アラートと推奨事項を提供
- 匿名アクセス、資格情報の漏洩、ソーシャル エンジニアリング、特権の乱用、悪意のあるコンテンツなど、ストレージに関する代表的な脅威をカバー



クラウド ストレージ上のファイルのスキャン

- アップロードされたファイルは、Microsoft 脅威インテリジェンスでサポートされているハッシュ評価分析によって評価
- ストレージ ログから対象のファイルのハッシュと、既知のウイルス、トロイの木馬、スパイウェア、ランサムウェアのハッシュを比較
- ファイルにマルウェアが含まれている疑いがある場合、Defender for Cloud でアラートを表示し、ファイル削除の承認を要求

包括的な対応

- Azure で管理されるすべてのデータ資産に一元的なセキュリティを提供し、Microsoft Sentinel など他の Azure セキュリティ サービスと連携
- 特定された脅威は、Defender for Cloud のオートメーション ツールによって簡単に防止、対応が可能

Microsoft Defender for SQL

Microsoft Defender for SQL は、データベースの潜在的な脆弱性を検出して軽減するとともに、データベースに対する脅威を示す可能性のある異常なアクティビティを検出できます。

SQL サーバーを継続的に監視する検出サービス

- Azure SQL Database や SQL Server (Azure IaaS、Azure Arc マシン) へのアクセス、データベースを悪用しようとするなど、有害な可能性がある不自然なアクティビティを検出
- SQL インジェクションの脆弱性、通常とは異なる場所や通常とは異なる Azure データセンターからのアクセス、通常とは異なるプリンシパルからのアクセス、潜在的に有害なアプリケーションからのアクセスなどを検知
- 不審なアクティビティの詳細、脅威を軽減する方法のガイダンスを提供、Defender for Cloud でアクション指向のセキュリティ アラートを通知し、Microsoft Sentinel で調査の続行と対処を実施

環境に合わせた 2 つのプランを提供

- Microsoft Defender for Azure SQL database servers は、Azure SQL データベース、Azure SQL Managed Instance、Azure Synapse の専用 SQL プール向け
- Microsoft Defender for SQL servers on machines は、仮想マシンやオンプレミスの SQL サーバー、Azure Arc が有効な SQL サーバーなど向け

潜在的な脆弱性とセキュリティ状態を評価

- データベースの潜在的な脆弱性を検出、追跡、修復を実施し、セキュリティ状態の概要と結果を提示
- データベースの誤設定、過剰なアクセス許可、保護されていない機密データなど、ベスト プラクティスからの逸脱を特定

クラウドの可視化と制御

Microsoft Defender for App Service

Microsoft Defender for App Service は、Web アプリと API に対する脅威の監視と検出を行うための機能を提供します。

Web アプリと API の構成を評価

- App Service のリソースを評価、評価結果から推奨事項を生成
- 推奨事項の手順で App Service リソースのセキュリティを強化

アプリに対するさまざまな脅威の検出

- MITRE ATT&CK (実際のサイバー攻撃をフェーズや技術、手法で分類したナレッジベース) に基づく攻撃手法のカバー
- App Service Web サイトが使用停止されたときに、未解決 DNS エントリを特定し、サブドメインの乗っ取りなどの攻撃から保護

Microsoft Defender for Containers

Microsoft Defender for Containers は、コンテナーをセキュリティで保護するためのクラウド ネイティブ ソリューションです。

イメージの脆弱性をスキャン

- Defender for Cloud に統合された ACR (Azure Container Registry) にプッシュされたコンテナ イメージをスキャンし、脆弱性を検出、詳細な情報と対処法を提示
- 過去 30 日以内にプルされたイメージを毎週スキャン

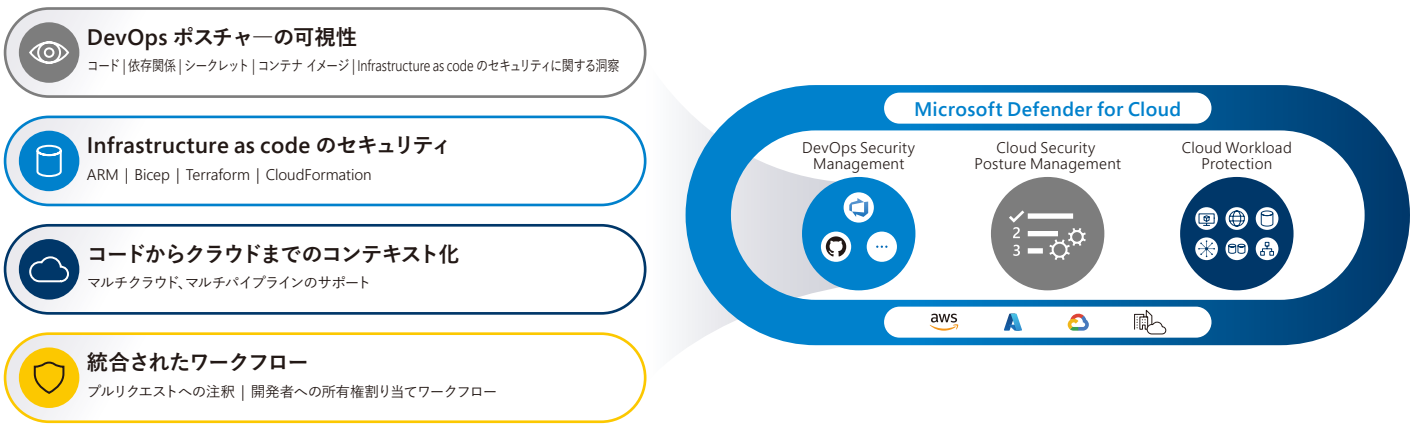
AKS クラスターの保護

- AKS (Azure Kubernetes Service) のログを収集して分析し、Kubernetes API や DNS、ダッシュボードのインシデントを検知
- AKS クラスターの各ノード上のポッドからセキュリティ情報を収集 (コンテナ内での悪質なファイルのダウンロードやコマンド実行などを検知)

Microsoft Defender for DevOps (CNAPP)

Defender for Cloud で利用できるサービスである Defender for DevOps によって、セキュリティ チームはマルチパイプライン環境全体で DevOps のセキュリティを管理できるようになります。

Defender for DevOps のカバー領域



Microsoft Defender for IoT

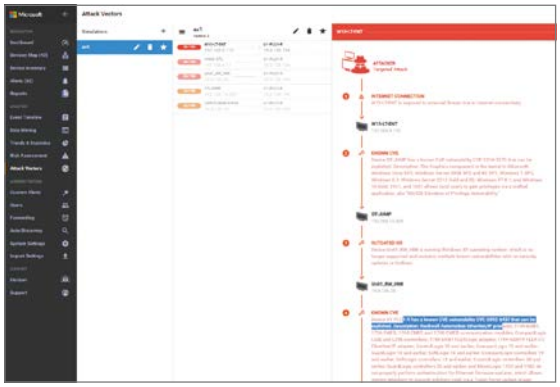
Microsoft Defender for IoT は、IoT/OT デバイスの脆弱性と脅威を特定し、中央インターフェイスを使用して管理するための統合セキュリティを提供します。

すべての IoT/OT デバイスを検出

- 管理されている IoT/OT 資産、脆弱性、脅威を特定可能、管理されていない IoT/OTデバイスはエージェントレスでネットワーク層を監視可能
- 特許取得済みの OT 特化型ふるまい検知のためのディープ パケット インスペクション (DPI) を提供
- IoT/OT ネットワーク トポロジ全体を視覚化し、デバイスの通信パスの把握や問題の迅速な原因特定を支援
- エージェントレスのセンサーから収集された情報を分析しデバイスの詳細情報を特定 (製造元、種類、シリアル番号、ファームウェア レベル、IP または MAC アドレス)
- デバイス イベントリ、デバイス マップを自動的に作成

脅威検知と各種レポート機能

- OT 環境の通信を 5 つのエンジンと機械学習で分析、検出したアラートは時系列で表示
- センサーにより収集された情報から OT 環境のリスク アセスメント レポートを作成
- デバイスの脆弱性情報から攻撃ベクトルをリアルタイムで計算し、特定のターゲットへの攻撃の実現可否を分析



Microsoft Defender Threat Intelligence

動的な脅威インテリジェンスで、最新の脅威とそのインフラストラクチャを排除することを支援します。

敵対者の正体を暴く

- 世界規模での攻撃者と攻撃に利用される悪意のあるインフラを特定、エンドポイントからインターネットまで広範囲に渡る脆弱性を検出
- 脅威インテリジェンスを利用してインシデント対応を迅速化、攻撃者を完全に排除し、二重の恐喝のリスクを低減するために露出を明確化
- 既存のセキュリティ インフラと統合、予防を強化し、セキュリティ ポスチャを向上

Microsoft Defender External Attack Surface Management

急速に変化するグローバルな外部からの攻撃対象領域をリアルタイムで確認できます。

脆弱性を発見

- 旧 RiskIQ の独自技術により、インターネット上で公開されている未把握の資産やリソースを検出
- 発見されたデバイスを継続的に監視し、エージェントや認証情報を必要とせず、新しい脆弱性を検索
- 露出したアセットの対応の優先順位を決め、露出したリソースを保護下に置くことで、クラウド セキュリティを強化し、セキュリティを向上

ネットワークのセキュリティ保護

Azure DDoS Protection

Azure DDoS Protection は、レイヤー 3/レイヤー 7 の DDoS 攻撃を常時監視し、DDoS 攻撃を自動減策機能を Azure がネイティブに提供するソリューションです。IP 保護とネットワーク保護の 2 種類があります。

ユーザーによる詳細設定が不要な自動軽減策

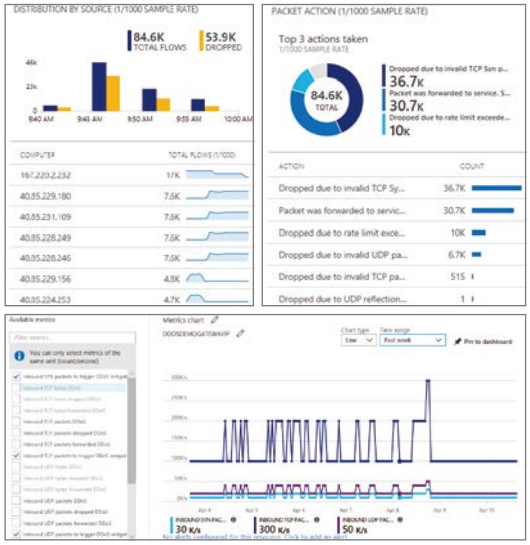
- パブリック IP トラフィックを継続的にプロファイル
- 独自の機械学習アルゴリズムにより、保護された各 IP の通常のトラフィック パターンを学習し、DDoS 軽減ポリシーを設定
- 開始後 1 分あたりの PPS 値の予測を開始し、学習したトラフィック パターン/ポリシーを 15 分ごとに適用

グローバルなネットワーク規模に対応

- 大規模な DDoS 攻撃にも対応、45+ Tbps グローバル規模の緩和能力
- 継続的な監視、学習、保護シグネチャの改善
- お客様アプリのために特別に調整された保護
- アクティブ トラフィック モニタリングにより、新たな脅威や攻撃ベクトルを積極的に検出

3 層の Web アプリ階層で多層防御を実現

- DDoS Protection で仮想ネットワークで有効化し、パブリック IP に L3/L4 の DDoS 保護適用
- L7 を保護するためには、Application Gateway を利用
- 仮想マシン スケール セットにより、VM の数を手動でスケールインまたはスケールアウト

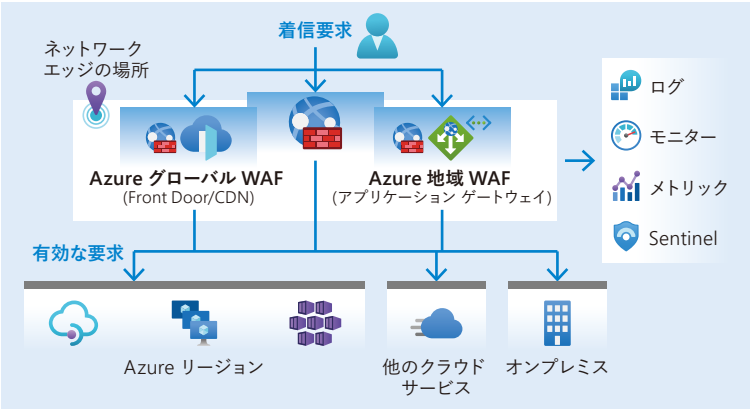


Azure Monitor との統合による分析と洞察

- Azure Monitor と統合し、DDoS 攻撃の軽減策レポートを生成
- 発信元 IP、宛先 IP、発信元ポート、宛先ポート、プロトコルの種類など、Azure analytics ダッシュボードでフロー ログ データのモニタリング

Azure Web Application Firewall

Azure Web Application Firewall は、強力なカスタム ルール エンジン (国や地域ごとのフィルタリング、IP 制御など) を提供し、一般的な脆弱性やその悪用から Web アプリケーションを保護します。



Azure サービスとの統合

- Azure Application Gateway/Front Door/CDN (プレビュー中) に統合されたセキュリティ
- 最新のマネージドおよび事前構成済みのルール セットにより Web アプリを保護
- SIEM との統合によるリソース セキュリティ情報イベントの管理、分析が可能

Web アプリケーションのセキュリティを強化

- SQL インジェクション攻撃、クロスサイト スクリプティング攻撃、その他の一般的な攻撃 (コマンド インジェクション、HTTP 要求スマグリング、HTTP レスポンス スプリッティングなど) から保護
- HTTP プロトコル違反/HTTP プロトコル異常 (ホスト ユーザー エージェントと承認ヘッダーが見つからないなど)、一般的なアプリケーション構成ミス (Apache や IIS など) の脆弱性から保護

Azure Front Door

Azure Front Door は、CDN と WAF の機能を兼ね備えた、エッジ上で動作する L7 ロードバランサーであり、高速で信頼性が高く、セキュリティで保護されたアクセスを実現します。

コンテンツへのアクセス時間を安全に最適化

- 通信元の一番近いエッジで通信処理
- バックエンド コンテンツへのアクセスをファイアウォールでセキュリティ保護しながらアクセスを最適化
- 高可用性のために最大限のパフォーマンスと即時グローバル フェイルオーバーを最適化
- Web トラフィックのグローバル ルーティングを定義、管理、監視が可能
- マイクロソフトのグローバル エッジ ネットワーク内のアプリへのエントリポイントをワンクリックで有効化
- エッジから、ホストされているアプリに対するユーザー管理を実施

Azure Front Door Premium の機能

- Web Application Firewall 全体の広範なセキュリティ機能
- ボット保護
- Private Link のサポート
- 脅威インテリジェンスとセキュリティ分析の統合

Azure Front Door Standard の機能

- コンテンツ配信の最適化
- 静的及び動的なコンテンツのアクセラレーション
- グローバルな負荷分散
- SSL のオフロード
- ドメインの証明書の管理
- 強化されたトラフィック分析
- 基本的なセキュリティ機能

Azure Network Watcher

Azure Network Watcher は、Azure 仮想ネットワーク内のリソースの監視、診断、メトリックの表示、ログの有効化または無効化を行うツールを提供します。

仮想マシンとエンドポイントの間の通信を監視

- Virtual Machines、Virtual Networks、アプリケーション ゲートウェイ、ロード バランサーなどの IaaS 製品のネットワーク正常性を監視および修復
- 通信を定期的に監視し、VM とエンドポイントの間の到達可能性、待ち時間、ネットワーク トポロジの変更などを通知

関係図の作成や問題の診断

- トポロジ機能により、仮想ネットワーク内のリソースとリソース間の関係図を生成可能
- ネットワーク トラフィック フィルター、ネットワーク ルーティング、Azure 仮想ネットワーク ゲートウェイと接続などを診断可能

Azure Bastion

Azure Bastion は、Azure portal から直接、仮想マシンに安全かつシームレスに接続できるサービスです。

仮想マシンへのセキュアなアクセス

- Azure portal から Web クライアントを介して RDP および SSH で仮想マシンに接続
- 仮想マシンに公開用 IP アドレスの付与や Firewall の公開設定が不要
- 専用の接続ツールや仮想マシンに各種エージェントなどの展開は不要

ゼロデイ攻撃から保護

- ポート スキャンや VM を標的とする脅威から保護
- 仮想ネットワークの境界にホストを配置、各 VM のセキュリティ負担を軽減
- フル プラットフォームマネージド PaaS サービスとして提供
- サービスは常に最新の状態に維持されゼロデイ攻撃から保護

Azure Bastion の利用状況を収集、可視化

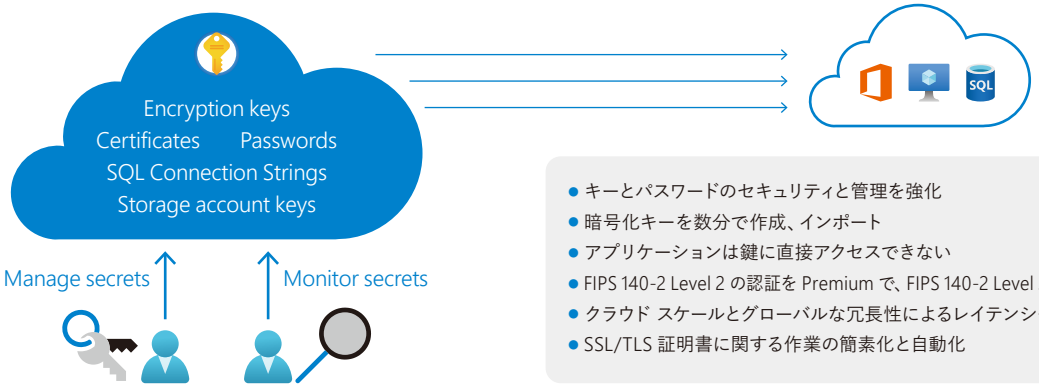
- Azure Bastion を使用してユーザーがワークロードに接続すると、リモートセッションの診断ログを記録
- 診断ログを利用して、だれがどのワークロードに、いつ、どこから接続したかなどのログ情報を確認可能

注: 別途 Log Analytics もしくは Azure Blob Storage との連携が必要

キー、シークレット、証明書の管理/データの保護

Azure Key Vault

Azure Key Vault は、クラウド アプリやクラウド サービスで利用される、暗号鍵やシークレットを一元的に保護します。ソフトウェア キーを使用して暗号化する Standard、ハードウェア セキュリティ モジュール (HSM) で保護されたキーを含む Premium、シングルテナントで、HSM で保護されたキーのみに対応する Managed HSM があります。



- キーとパスワードのセキュリティと管理を強化
- 暗号化キーを数分で作成、インポート
- アプリケーションは鍵に直接アクセスできない
- FIPS 140-2 Level 2 の認証を Premium で、FIPS 140-2 Level 3 認証をManaged HSM で提供
- クラウド スケールとグローバルな冗長性によるレイテンシーの低減
- SSL/TLS 証明書に関する作業の簡素化と自動化

Azure Key Vault のアクセス管理

- 接続文字列などのシークレットは HSM で高度に暗号化し、Microsoft Entra ID のユーザーやサービス プリンシパル、マネージド ID のみがアクセス可能
- Key Vault はキーとシークレットを一元管理し、アプリケーションのリソースへのアクセス ポリシーをコントロール
- Microsoft Entra ID は アプリ (サービス プリンシパル、マネージド ID) の Key Vault へのアクセスをコントロール

Azure Key Vault の証明書

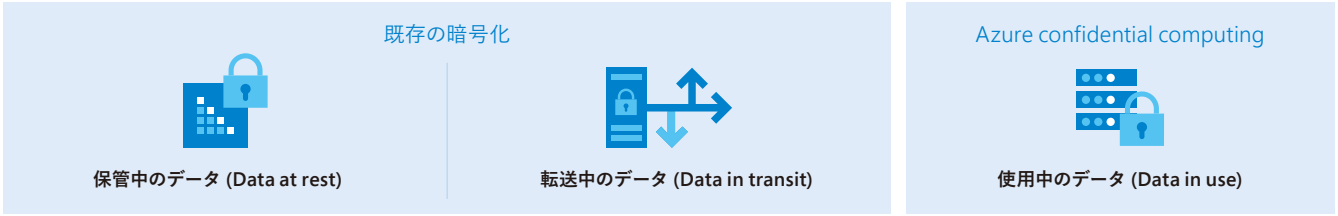
- Key Vault 作成プロセスまたは既存の証明書をインポートして、証明書を作成可能
- 秘密キー マテリアルを操作せずに、X509 証明書のセキュリティ保護されたストレージと管理を実装可能
- 証明書のライフサイクル管理のポリシー作成や証明書の失効、更新を通知するための連絡先情報の指定が可能
- 選択した発行者 (Key Vault パートナー X509 証明書プロバイダーまたは証明機関) による自動更新をサポート

Azure Confidential Computing

Azure Confidential Computing では、財務データや患者の情報などの機密データが処理されている間、そのデータを隔離することができます。

使用中のデータを保護

- ハードウェア ベースの高信頼実行環境 (TEE) を使用してアプリとデータに対する未承認のアクセスや変更から保護
- データ整合性、データ機密性、コード整合性を一定レベルで保証
- Intel Software Guard Extensions (Intel SGX) や AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) などがコンフィデンシャル コンピューティングの実装をサポート



Sentinel と Defender for Cloud を採用、クラウドサービスのセキュリティ強化を目指す 商船三井システムズ

会社全体の方針として、ランサムウェアを中心としたサイバー攻撃への対策の強化があり、Sentinel や Microsoft Entra ID PIM 導入はその一環として取り組んだものでした。一方で、以前から懸念していたアプリ開発におけるクラウド セキュリティをどう担保していくかという課題を解決してくれたのが、Defender for Cloud でした。これらは本来、セキュリティ対策としては別々の取り組みだったのですが、結果的にクラウド セキュリティを統合的に管理できる仕組みにつながりました。マイクロソフトの製品として親和性が高く、連携しやすいことが大きなポイントだったと思っています。

商船三井システムズ株式会社
技術統括部
アーキテクチャチーム 兼 クラウドチーム
チーフエンタープライズシステムアーキテクト
安宅 恭子 氏

■ 課題

- 内製化していたアプリ開発や運用に関する業務について、セキュリティリスクを把握できるようにし、その知見やノウハウを蓄積して全社的に共有するための仕組みをつくる必要があった

■ 選定ポイント

- Microsoft Sentinel の PoC を行って Microsoft Entra ID (旧Azure AD) などのログを分析してみると、Microsoft 365 にサインインを試みる不正アクセスなどが多く発生するなど危険な兆候が見られた。こうした兆候を捉えておけば、ユーザーや管理者の権限を奪うランサムウェア対策としても有効だと考えた
- Microsoft Defender for Cloud が提供する、セキュリティ態勢をスコア化する機能や脅威を防ぐための推奨策を提案する機能に興味を持っていた

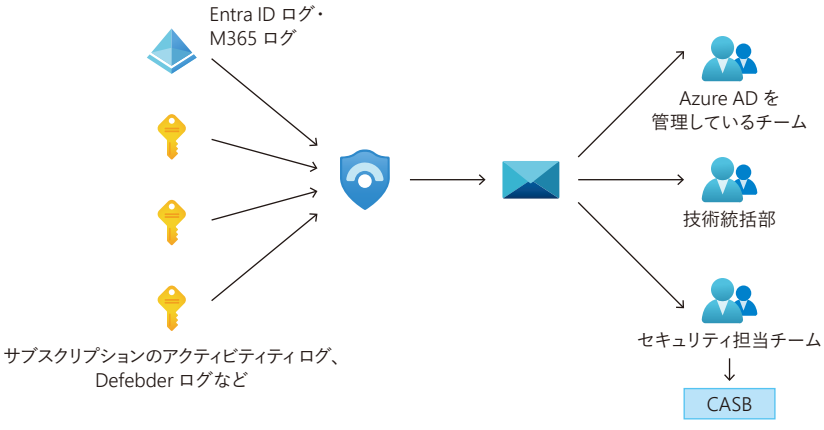
■ 効果

- ランサムウェア対策の一環として不正ログインの予兆を検知するための SIEM 環境を素早く手軽に構築できた
- 従量課金で利用できるので、一般的な SIEM 製品のようにシステム構築に多大なコストがかかることがない
- 自分たちで見逃してしまうリスクを的確に見つけることができ、開発するサービスの安全性や信頼性を高めることができる
- Defender for Cloud は、ポータル画面上で、セキュリティスコアをわかりやすく可視化してくれるため、セキュリティ態勢の見直しと高度化につながっている

■ 今後の展望

- Defender for Cloud が提案する推奨事項の設定のうち、業務やシステム、タイミングの関係で実施できてなかったものに取り組み、100%に近づけていきたい

■ Microsoft Sentinel のシステム構成図



導入・運用
- 外部ベンダーに依頼せずに構築 (日本マイクロソフトより支援)
- インシデントも社内で確認 (専用の Teams チャネル)

効果
- CASB で発見できていなかった攻撃予兆を確認、対応ができた

課題
- インシデントの抑制、調査対応

上記事例は、2023 年 3 月 27 日時点の内容です。

Azure で利用できるセキュリティ サービスとテクノロジ

Azure の全般的なセキュリティ

- Microsoft Sentinel
- Microsoft Defender for Cloud
  - Microsoft Defender for Servers
  - Microsoft Defender for Storage
  - Microsoft Defender for SQL
  - Microsoft Defender for Containers
  - Microsoft Defender for App Service
  - Microsoft Defender for Key Vault
  - Microsoft Defender for Resource Manager
  - Microsoft Defender for DNS
  - Microsoft Defender for open-source relational database
  - Microsoft Defender for Azure Cosmos DB
- Microsoft Defender for IoT
- Azure Key Vault
- Azure Monitor logs
- Azure Policy
- Azure DevTest Labs
- Azure Confidential Computing

ストレージのセキュリティ

- Azure Storage Service Encryption
- Azure Client-Side Encryption
- Azure Storage Shared Access Signature
- Azure Storage Account Keys
- Azure File shares with SMB 3.0 Encryption
- Azure Storage Analytics

データベースのセキュリティ

- Azure SQL Firewall
- Azure SQL Cell Level Encryption
- Azure SQL Connection Encryption
- Azure SQL Always Encryption
- Azure SQL Transparent Data Encryption
- Azure SQL Database Auditing
- Microsoft Purview Governance Portal

ID 管理とアクセス管理

- Azure role-based access control
- Microsoft Entra ID
- Microsoft Entra ID B2C
- Microsoft Entra ID Domain Services
- Microsoft Entra ID Multi-Factor Authentication
- Microsoft Entra Permissions Management

バックアップと障害復旧

- Azure Backup
- Azure Site Recovery

ネットワーク

- Network Security Groups
- Azure VPN Gateway
- Azure Application Gateway
- Azure Web Application Firewall (WAF)
- Azure Load Balancer
- Azure ExpressRoute
- Azure Traffic Manager
- Azure Application Proxy
- Azure Firewall
- Azure Front Door
- Azure DDoS protection
- Azure Network Watcher
- Azure Bastion
- Azure Private Link
- Virtual Network service endpoints

Cloud Security に関する最新情報は、https://azure.microsoft.com/ja-jp/ 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

6580-NOC2