



Microsoft Defender for Cloud で実現する ハイブリッド環境の保護

日本マイクロソフト株式会社
コーポレートソリューション 事業本部
インテリジェントクラウド技術本部
Digital Technical Specialist
津郷 晶也

目次

1. クラウド時代のセキュリティリスク
2. Defender for Cloud 概要
 1. MS Defender / Defender for Cloud
 2. CSPM , CWPP
3. CSPM
4. CWPP
 1. Defender for Server
 2. Defender for SQL

クラウド時代のセキュリティリスク

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

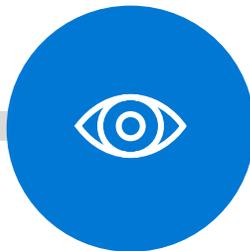
クラウド上での
セキュアなアプリの開発・
運用



>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¹

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。²

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³

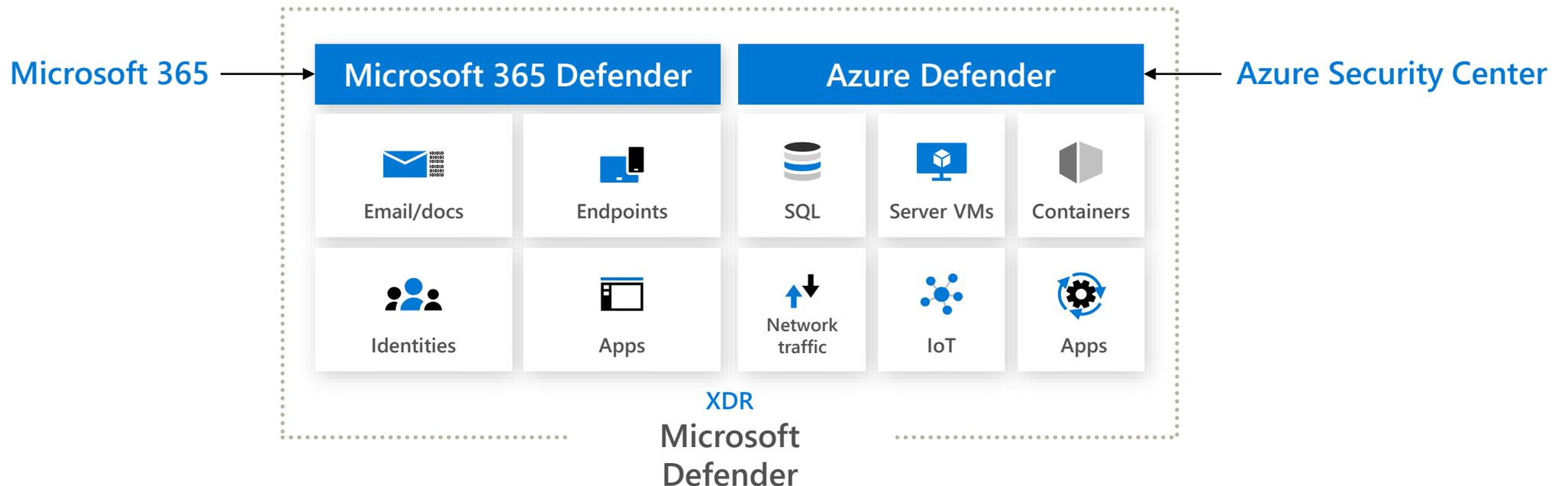
1. Microsoft Enterprise DevOps Report

2. Microsoft Cloud Security Priorities and Practices Research

3. Ponemon Institute, Cost of a Breach Report

Microsoft Defender

- Microsoft の持つ、Extended Detection & Response (XDR) の機能を統合
Microsoft Defender = Microsoft 365 Defender + Azure Defender ブランド
- エンドポイント (EDR) やネットワーク (NDR) だけでなく、ID, クラウドアプリ、Email とドキュメント、インフラ、クラウドプラットフォーム、IoT まで、脅威検知と対処の機能を統合的に提供



Microsoft Defender for Cloudの役割



Leveraging
Azure Arc



CSPM

(Cloud Security Posture Management)

マルチクラウドの
セキュリティポスチャを管理

セキュリティ
スコア

ポリシーと
コンプライア
ンス

自動化された
修復



Leveraging
Azure Arc



CWPP

(Cloud Workload Protection Platform)

XDR 機能による
ハイブリッド・マルチクラウドの保護

脆弱性の
管理

高度な
クラウド防御

脅威検知
と対処



クラウドセキュリティの一元化

Microsoft Defender for Cloudの特徴

マイクロソフトセキュリティの優位性



Azure にビルトイン

- 展開作業の必要なし、有効化作業のみ
- Azure リソース展開プロセスに保護機能を組み込み
- 最も広い保護範囲を提供
- ワンクリックで修復



マルチクラウドとハイブリッドのサポート

- AWS と GCP のポスチャーマンをエージェントレスでオンボード
- 新規リソースの自動プロビジョニング
- Azure Arc でオンプレミスのリソースをオンボード



セキュアスコア

- すべてのクラウドのセキュリティ状態を俯瞰的に把握可能
- セキュリティに関する推奨事項の優先順位付け
- セキュリティポスチャーの状態を時系列で追跡・管理

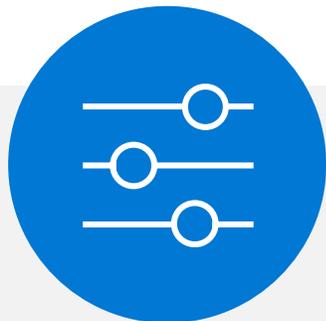


高度な脅威からの保護

- ワークロードに応じたシグナルと脅威のアラート
- 決定論的検知、AI、アノマリベースの検知メカニズム
- 毎日65兆件のシグナルを収集するMicrosoft脅威インテリジェンスのパワーを活用

セキュリティ態勢管理 (CSPM)

クラウドにおけるセキュリティ態勢の全体的な管理



リソースの可視化

クラウドリソースの
一覧と管理



セキュアスコア

セキュリティ態勢の
基準となるベースラインを
理解し、推奨事項を実行
継続的な監視



コンプライアンス

キーとなるコンプライアンス標準
に沿った構成となっていることを
確実にし、
組織のポリシーを強化する



データセキュリティ

機密データの特定と
重要なリソースの
優先順位付け

クラウドセキュリティ ポスチャ管理

基本的な CSPM (無料)



アセット インベントリとセキュア スコア分析

スムーズなオンボーディング | +450 のビルトイン アセスメント | カスタム機能 | ポリシー管理



高度な修復

応急処置による修復 | Logic Apps を使用した自動修復 | エンフォースメント ポリシー



データ エクスポートと Out-of-The-Box レポート作成

ビルドインの Azure ワークブック | 大規模なデータ ストリーミングとエクスポート | SIEM/SOAR ソリューションとの統合



統合されたワークフローと自動化

セキュリティ イベントによってトリガーされる、Out-of-The-Box なカスタム自動化

Defender CSPM

※Azure, AWSがGA
GCPはPublic Preview



エージェントレス脆弱性スキャン

ソフトウェアと CVE の可視性 | ディスク スナップショット | 安全でないシークレットと鍵



統合されたデータとインサイト

Defender for DevOps | Defender External Attack Surface Management |
Entra Permissions Management



コンテキストに応じたクラウド セキュリティとリスクの優先順位付け

攻撃パス分析 | Intelligent Cloud Security Graph | Cloud Security Explorer のカスタム パス クエリ |
リスクベースの優先順位付け



規制コンプライアンスと業界ベンチマーク

50以上の規格 | マルチクラウドの Microsoft セキュリティ ベンチマーク |
コンプライアンス ダッシュボードとレポート作成 | Microsoft Purview コンプライアンス マネージャとの統合



ガバナンス管理

所有者の自動割り当て | 組織におけるアカウントビリティの推進 | 猶予期間 | 修正にかかる時間を短縮



データを意識したセキュリティ ポスチャ

マルチクラウドのデータ資産検出 | 機密データやシャドー データを含むデータ フローおよびリソースの特定 |
潜在的な機密データの露出やデータ漏洩の検出

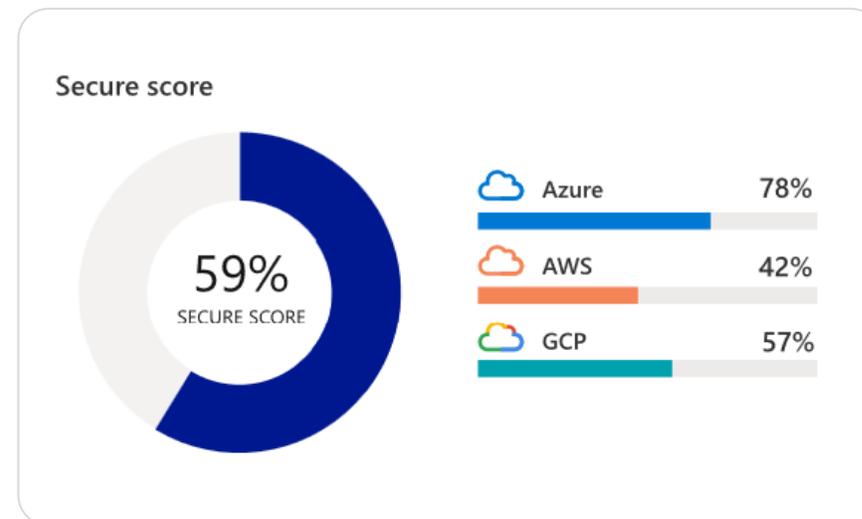
基本的なCSPM機能

セキュアスコア

- » セキュリティとコンプライアンスに関するベストプラクティスの評価と実装
- » ネットワーク、コンピューターリソース、データベース、サービスレイヤーなど重要なクラウドリソースを全てカバー
- » すぐに利用できる450以上の推奨事項
- » 組織の要件に合わせたカスタム推奨事項の作成
- » インベントリ一覧や条件指定によるフィルタリング
- » 1クリックで修正できる「Quick Fix」の利用や、望ましくない構成を回避する強制ポリシーの適用

マルチクラウドセキュリティベンチマーク

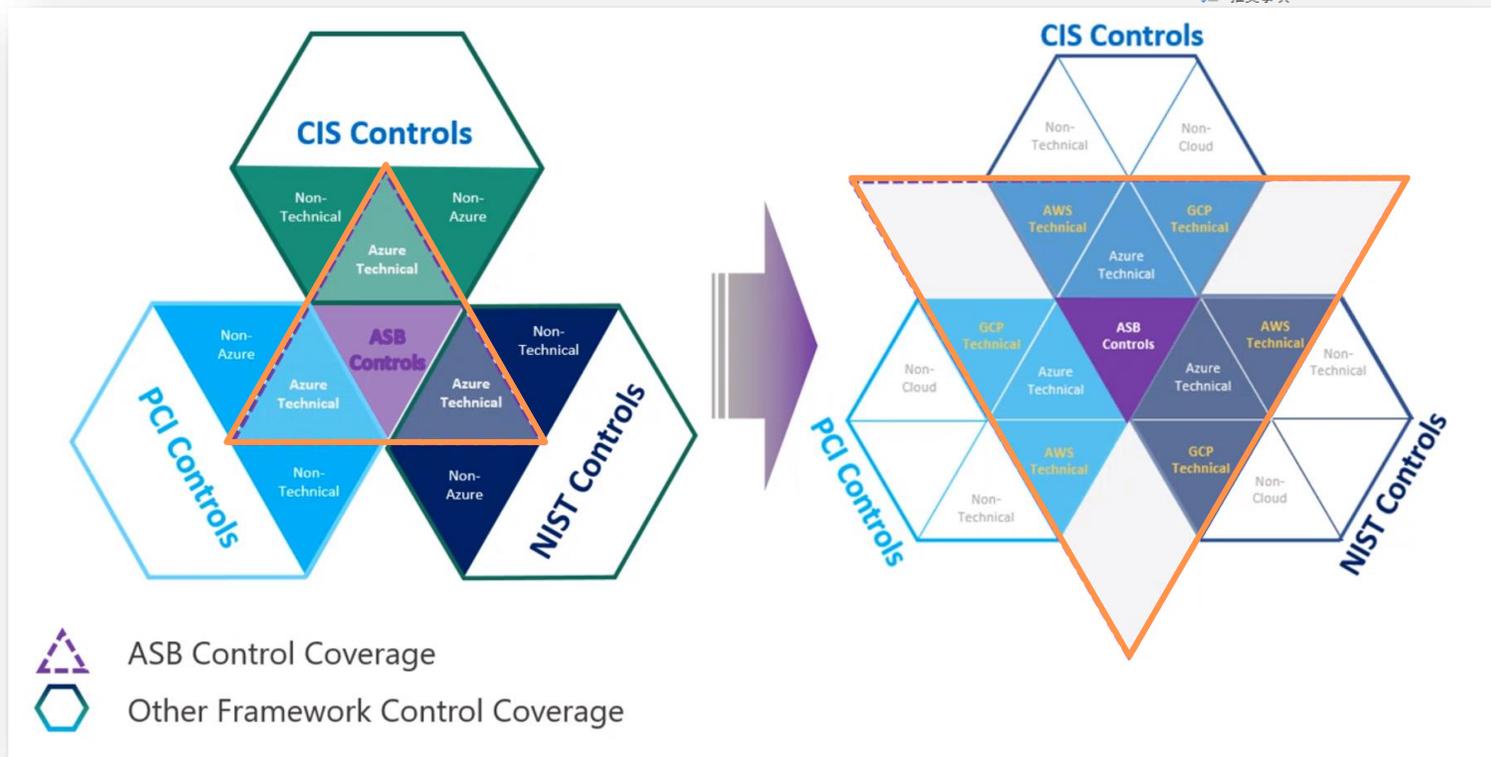
- AWS, Azure, GCPの環境横断的な継続的な評価を行い、単一の統合されたダッシュボード上でクラウドセキュリティコンプライアンスの管理
- 業界標準、規制コンプライアンス、クラウド特有のベンチマークを踏まえたベストプラクティス (CIS, PCI, NISTなど)



Microsoft クラウド セキュリティ ベンチマーク

クラウドセキュリティのベストプラクティスをマルチクラウド (Azure, AWS, GCP) に対して詳細な技術ガイダンスとともに提供

➤ 複数のベンチマーク適用による不要なオーバーヘッドの削減



Cloud | 規制コンプライアンス

レポートのダウンロード | コンプライアンス ポリシーの管理 | クエリを開く | 経時的なコンプライアンス プラック | 監査レポート | Compt

ダッシュボードで追跡する標準を完全にカスタマイズできるようになりました。上の [コンプライアンス ポリシーの管理] を選択して、ダッシュボードを更新してください。 →

すべてのコンプライアンス コントロールを展開する

NS. ネットワーク セキュリティ

NS-1. ネットワーク セグメント化の境界を確立する コントロールの詳細 MS C

Automated assessments - Azure

- サブネットはネットワーク セキュリティ グループに関連付けられている必要がある
- インターネットに接続されていない仮想マシンをネットワーク セキュリティ グループで保護する必要がある
- アダプティブ ネットワーク強化の推奨事項をインターネット接続仮想マシンに適用する必要がある
- ご使用の仮想マシンに関連付けられたネットワーク セキュリティ グループでは、すべてのネットワーク ポートを制限する必要がある
- インターネットに接続されている仮想マシンをネットワーク セキュリティ グループで保護する必要がある

検索結果: 1 - 5 / 5 件。

Automated assessments - AWS

- EC2 サブネットでは、パブリック IP アドレスを自動的に割り当てないようにする必要があります
- 未使用の EC2 セキュリティ グループは削除する必要があります
- リモート サーバー管理ポートに対して 0.0.0.0/0 からのインGRESS トラフィックを許可するネットワーク ACL が 1 つもないことを確
- VPC の既定のセキュリティ グループは、すべてのトラフィックを制限する必要があります
- セキュリティ グループでは、リスクの高いポートに対して無制限のアクセスを許可しないようにする必要があります

検索結果: 1 - 5 / 14 件。

Automated assessments - GCP (preview)

- GKE クラスタでネットワーク ポリシーを有効にする必要があります
- ファイアウォールは、汎用アクセスを許可する開かれた NETBIOS ポートを持つように構成しないでください
- 既定のネットワークがプロジェクトに存在しないことを確認する
- ファイアウォールは、汎用アクセスを許可する開かれた MEMCACHED ポートを持つように構成しないでください

セキュリティダッシュボード

セキュリティ態勢に関する集約されたビュー

→ Azure、AWS、GCPのセキュリティ態勢を集約

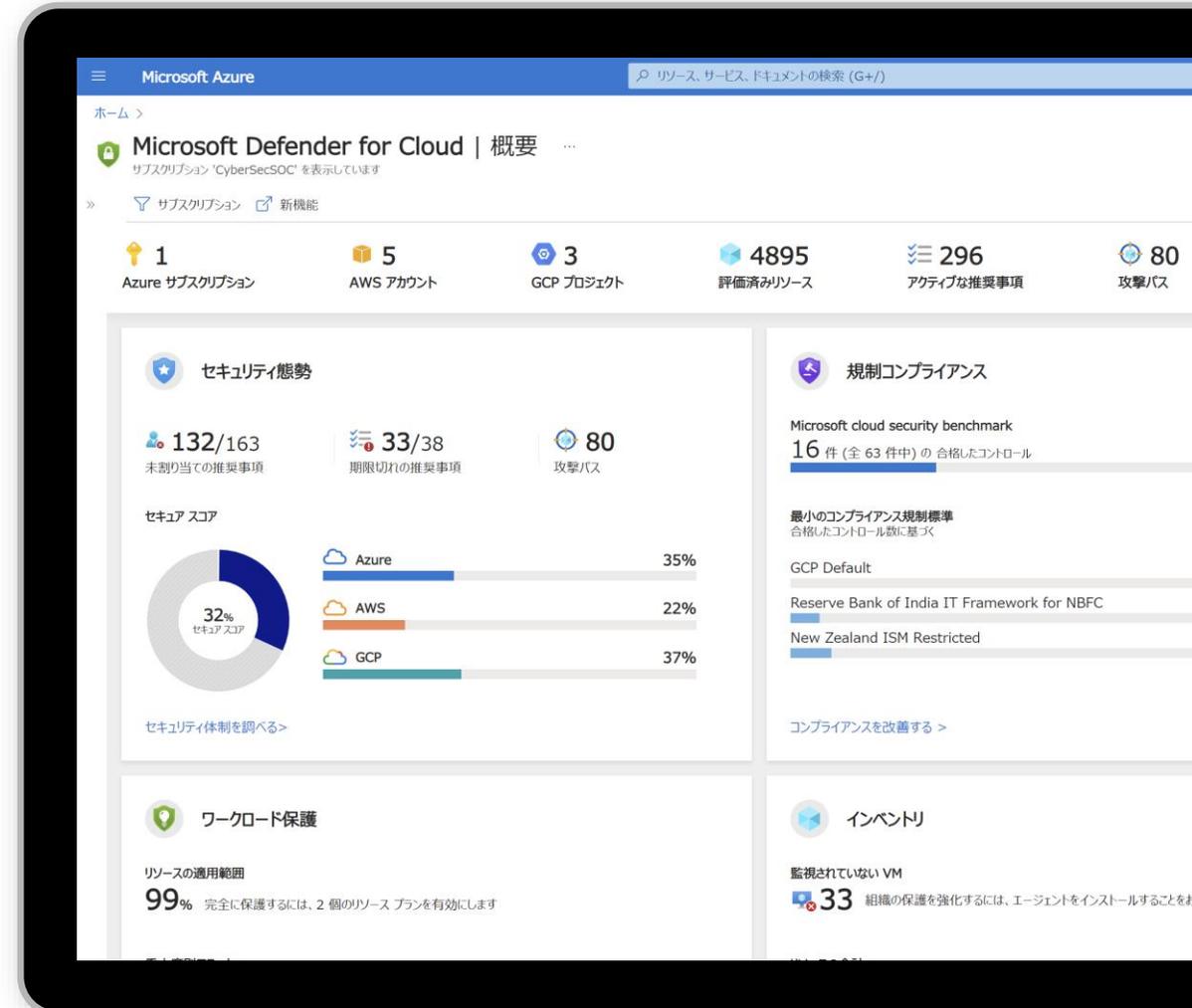
シンプルなメニュー

→ セキュリティ態勢、リソースインベントリ、ワークロード保護など目的に沿って詳細を確認可能なビューを用意

優先順位付けに必要な洞察を提示

→ どの推奨事項を優先的に実施すべきか

→ 最も攻撃されているリソースへの対処



推奨事項

利用環境に示される推奨事項の一覧

- Microsoft Cloud Security Benchmarkに基づく
- 推奨事項を実施した場合のセキュアスコア上昇の可能性とともに提示。どの推奨事項を優先的に実施すべきかの検討に利用

シンプルなメニュー

- Azure、AWS、GCPリソースに対する推奨事項の一覧を1クリックで切り替え可能
- マルチクラウドプラットフォームに渡る一定の尺度によるセキュリティ態勢評価

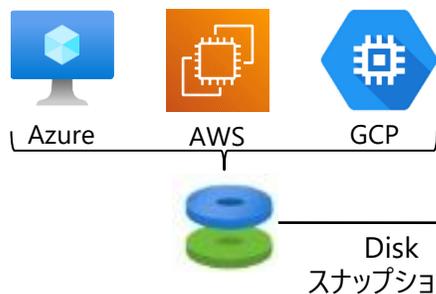
The screenshot displays the Microsoft Defender for Cloud interface. At the top, it shows the 'Microsoft Azure' header and a search bar. Below this, the 'Microsoft Defender for Cloud | 推奨事項' (Recommendations) page is visible, indicating a subscription to 'CyberSecSOC'. The main content area shows a security score of 32% and 163/235 active recommendations. A prominent '80 攻撃パス' (Attack Paths) alert is shown, indicating the most dangerous recommendations. Below this, there are filters for recommendation status, importance, resource type, and maturity. A table lists various recommendations with their maximum and current scores.

名前	最大スコア	現在のスコア
MFA を有効にする	10	0.00
管理ポートをセキュリティで保護する	8	4.41
脆弱性を修復する	6	0.97
システムの更新プログラムの適用	6	3.10
転送中のデータを暗号化する	4	1.84
アクセスとアクセス許可の管理	4	2.14
保存時の暗号化を有効にする	4	0.45
セキュリティ構成を修正する	4	1.90
承認されていないネットワーク アクセスを制限する	4	1.30
適応型アプリケーション制御の適用	3	1.56

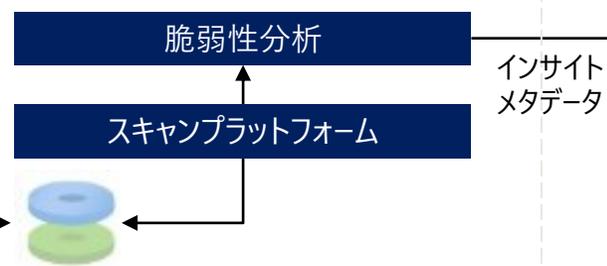
エージェントレススキャン

これまで課題となっていた「新たな管理エージェントをインストールすることによる VM への負荷」をクリア

お客様環境の仮想マシン



隔離されたスキャン環境



Defender for Cloud ポータル



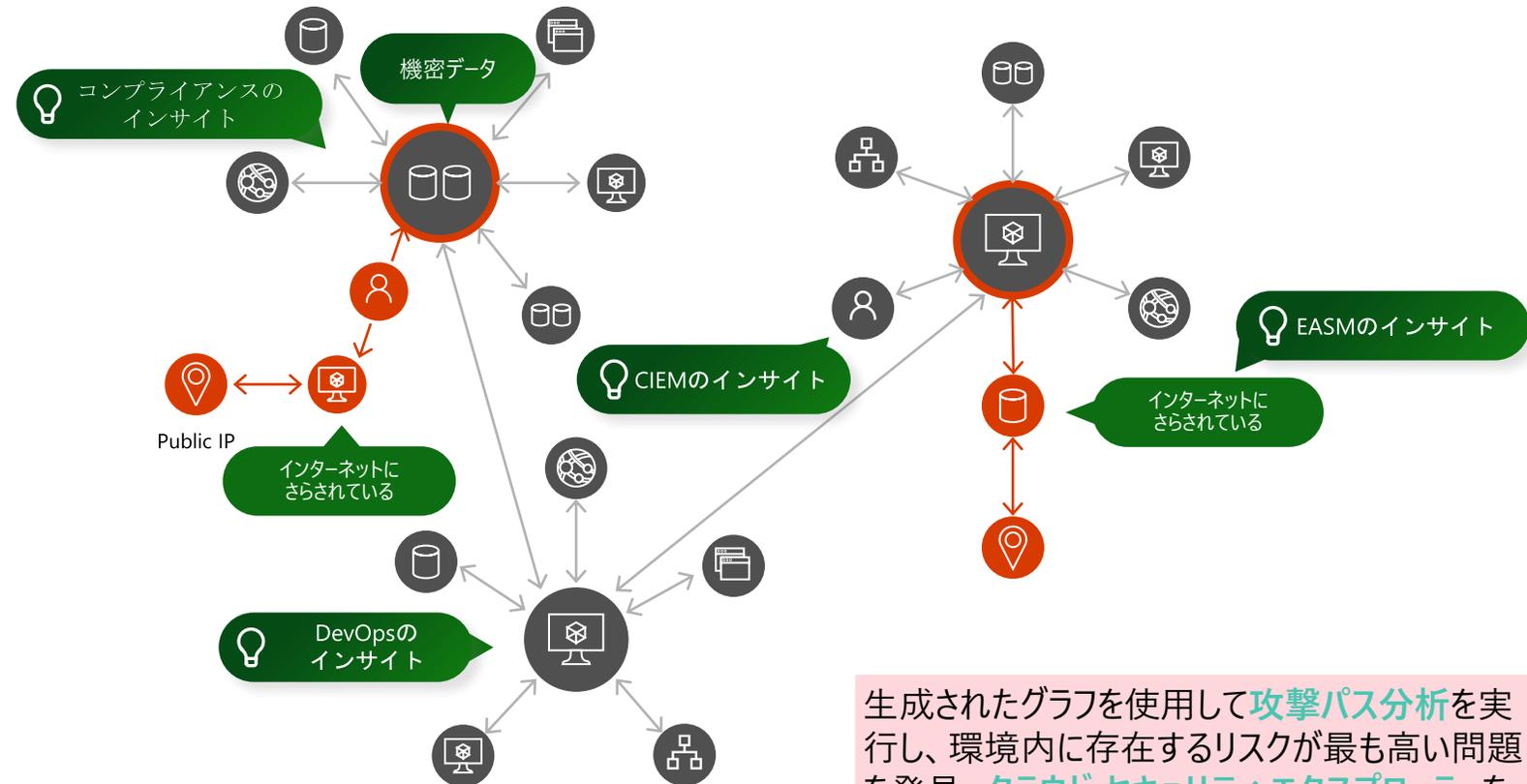
メリット

-  **スピード** - 脆弱性の状況を大規模に、簡単に、迅速に可視化
-  **負荷軽減** - 追加実装やパフォーマンス、社内調整などの影響を低減
-  **コストパフォーマンス** - Defender for Endpoint の脆弱性管理のエンジンを利用
-  **安全性** - スキャン環境は隔離された環境にあり、高い揮発性

攻撃影響範囲を分析するクラウドセキュリティグラフ

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

- ≫ 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**ラテラルムーブメント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**意識したポスチャ管理を統合して、コンテキスト データを使用**



生成されたグラフを使用して**攻撃パス分析**を実行し、環境内に存在するリスクが最も高い問題を発見。**クラウドセキュリティエクスペローラー**を使用してグラフのクエリを実行することも可能

攻撃パス解析とコンテキストセキュリティ機能

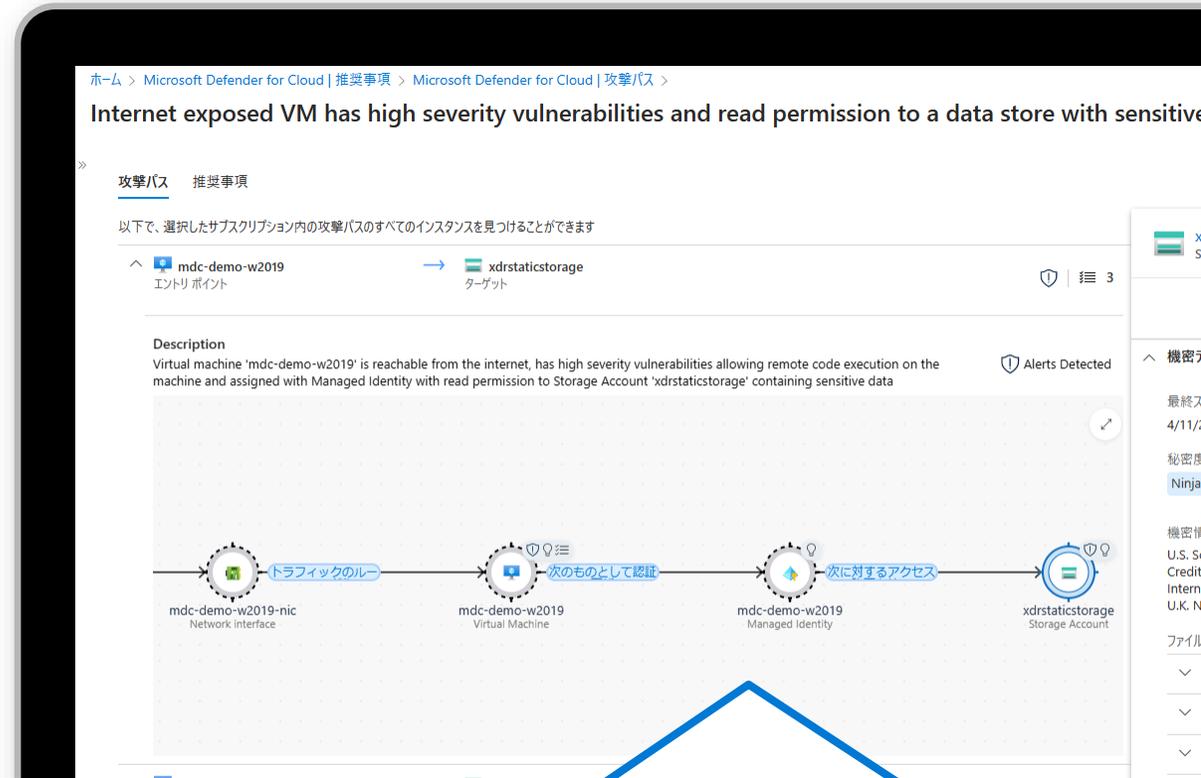
コンテキストに応じたクラウドセキュリティでリスクに優先順位を付ける

攻撃パス分析

- 潜在的な悪用可能なラテラルムーブメントパスに沿って、最も脆弱なリソースを特定
- 関連する CVE データとリスク コンテキストを表示して、修復に集中する

クラウドセキュリティエクスプローラー

- カスタマイズ可能なクエリを使用してクラウドセキュリティグラフを積極的に検索し、組織の主要な懸念事項に基づいて環境内のセキュリティリスクを見つけます。
- 特定の CVE、インターネットへの公開、公開されたマシン、運用およびビジネス タグなどでクエリを実行します



攻撃パス分析での検出例：

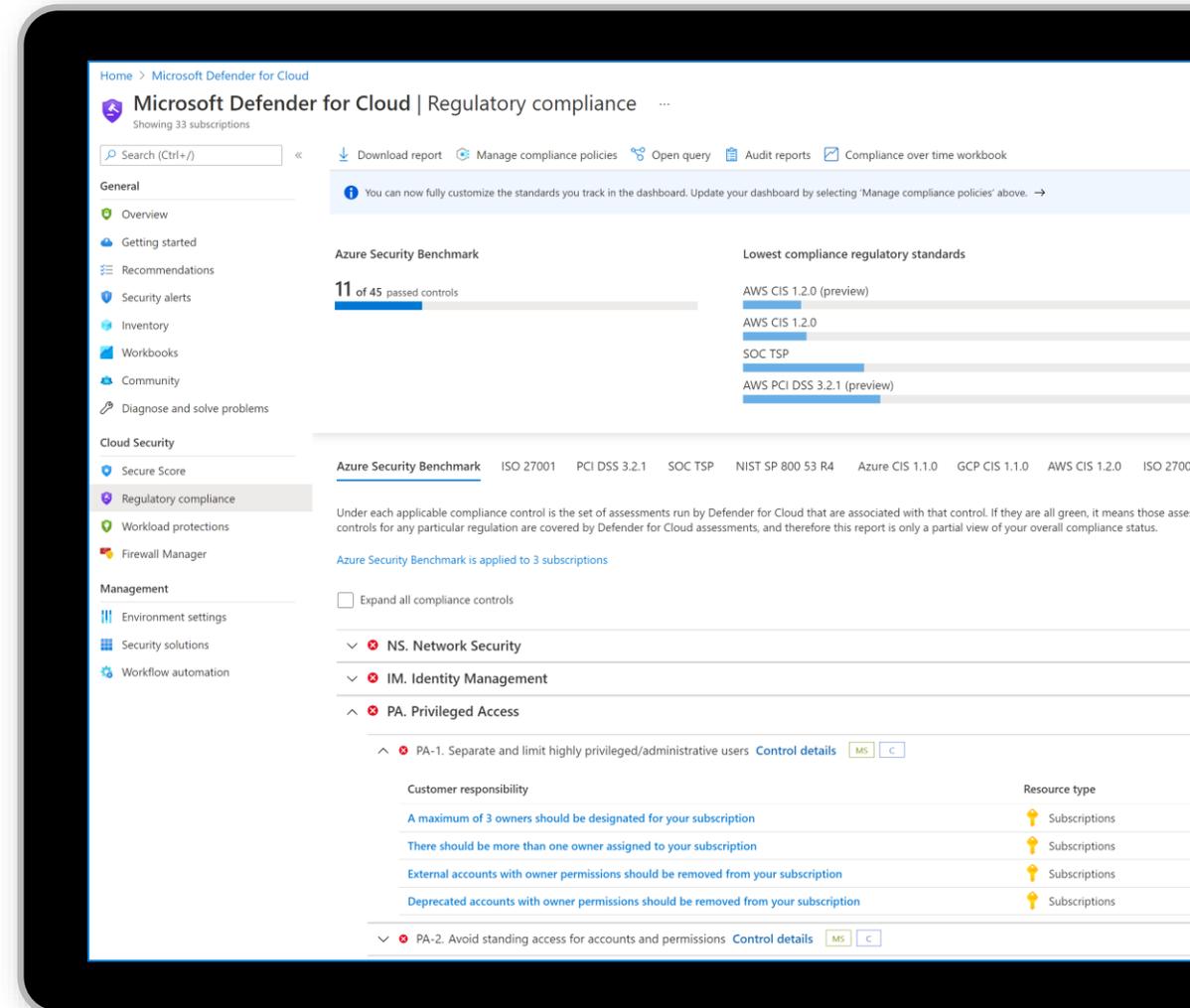
高い緊急度の脆弱性を持ち、インターネットに晒されているVMがストレージアカウントへの参照権限を持っている。かつそのストレージアカウントには機微な情報が含まれている -> 危険性高！

コンプライアンス評価と管理

- クラウドリソースの継続的な評価による、コンプライアンス状況の評価と管理
- 業界標準、規制遵守の枠組み、およびベンダーが提供するベンチマークを使用して、セキュリティとコンプライアンスのベストプラクティスを実装する
- 組織固有のニーズに対応するカスタムな推奨事項の作成

幅広い規制コンプライアンスをサポート:

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Microsoft Cloud Security Benchmark
- ✓ AWS Foundational Security best practices



データ対応セキュリティ態勢

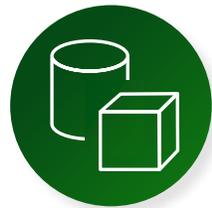
クラウド データ資産とデータ侵害のリスクを明らかにすることで、クラウド データセキュリティ態勢を強化します

オンボード



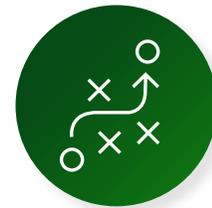
マルチクラウドデータリソースの
エージェントレスオンボーディング、
ワンクリック対応

自動検出



クラウド データ資産を自動的に検
出して、アクセシビリティ、機密
データ、データ フローを明らかにする

リスクの発見



クラウドセキュリティエクスプローラーと
攻撃パス分析でデータリソースへの
リスクを発見

リスクの修復



組み込みのインサイト、推奨事
項、Quick Fix でクラウドデータ
セキュリティ態勢を強化

コンテナセキュリティ態勢

- Defender CSPMで、コンテナ態勢を改善するための機能群を提供
- 攻撃パス分析など活用してKubernetes環境のリスク可視化、エージェントレスでの検出機能を強化

◆Kubernetesエージェントレススキャン

間隔をおいて取得したスナップショットに基づき、Kubernetesクラスターのアーキテクチャ、ワークロードオブジェクト、セットアップに関する情報を検出



◆コンテナレジストリの脆弱性評価

Microsoft Defender 脆弱性の管理 (MDVM)を利用し、エージェントのインストール、ネットワーク接続要件、またはコンテナへの影響を必要とせずに脆弱性の評価結果を取得



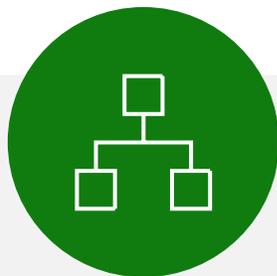
脅威の検出とワークロードの保護 (CWPP)

クラウドやオンプレミスの全レイヤーを脅威から保護



脅威検出

コンピューティング、データベース、クラウドサービスなどの階層で優先順位付けされた警告を活用



MITRE ATT&CK® フレームワーク マッピング

攻撃者の攻撃ライフサイクルにおける戦術を理解する



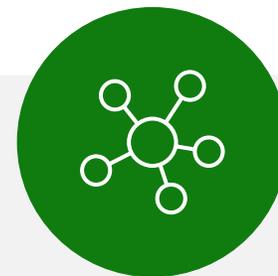
最先端の脅威 インテリジェンス

マイクロソフトの脅威インテリジェンスを基盤とする高度に洗練されたリソース別の警告



脆弱性の管理

脆弱性を悪用される前に特定して修復

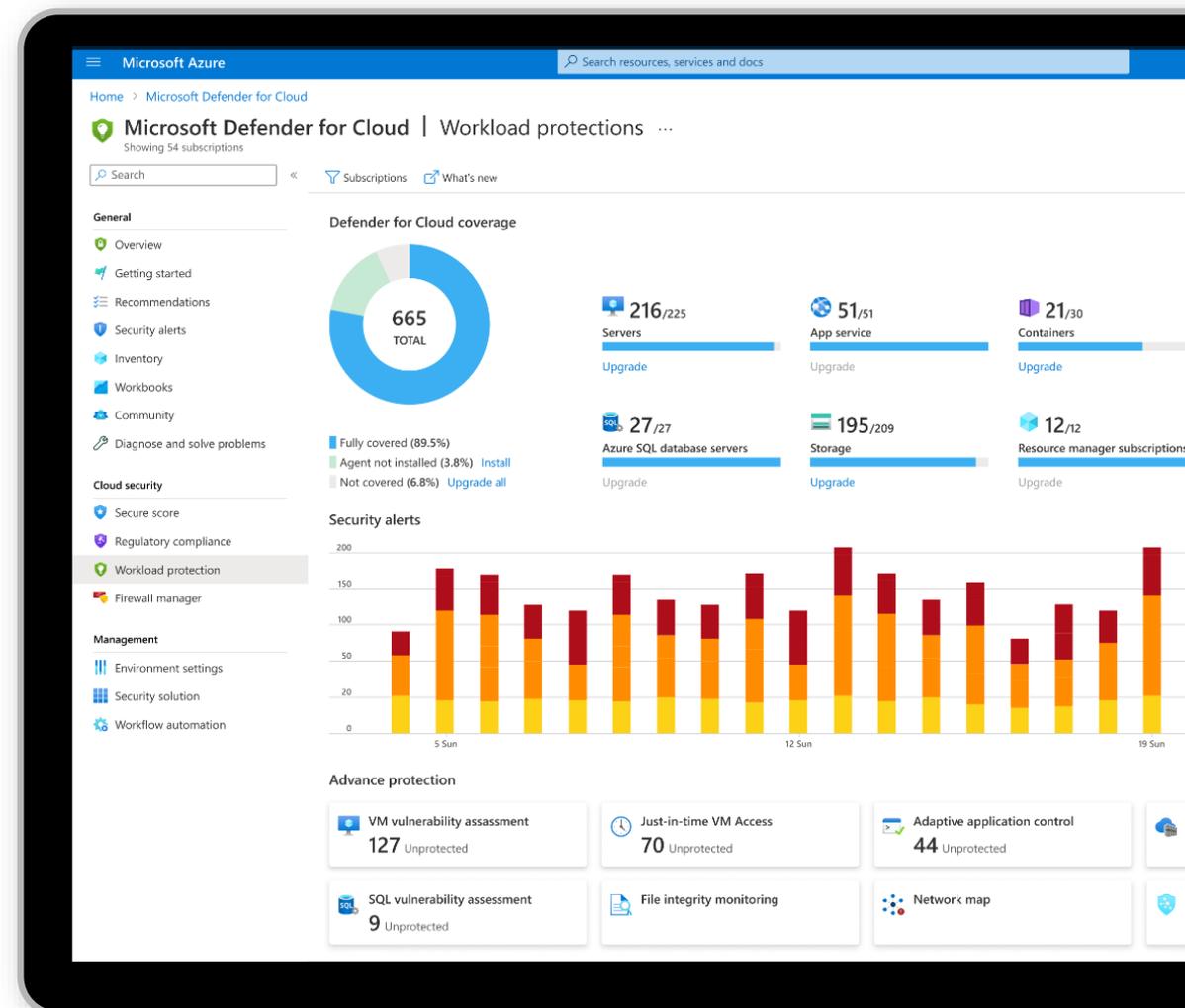


警告の 相関関係

インシデントごとにグループ化された警告で容易に優先順位付け

クラウドとオンプレミスのワークロードを保護

- マイクロソフトの脅威インテリジェンスの強力なインサイトを基盤に、リソースの種類に固有の攻撃ベクトルに合わせた検出を活用
- ワークロードの継続的なスキャンによって脆弱性を特定して対応し、攻撃にさらされる領域を縮小
- 新しいワークロードがデプロイされたら**すぐ自動的に保護**
- SIEM との統合によりインシデント管理が容易に



Microsoft Defender for Cloud の CWPP

Microsoft Defender for Cloud は、統一されたエクスペリエンスで、Azure上のサービスとオンプレミスやAWS, GCP のサーバーに対する脅威の保護を提供



Microsoft Defender
for Servers
(multi-cloud)



Microsoft Defender
for App Service



Microsoft Defender
for SQL
(multi-cloud)



Microsoft Defender
for Storage



Microsoft Defender
for Containers



Microsoft Defender
for Key Vault



Microsoft Defender
for Resource Manager



Microsoft Defender
for Resource Manager

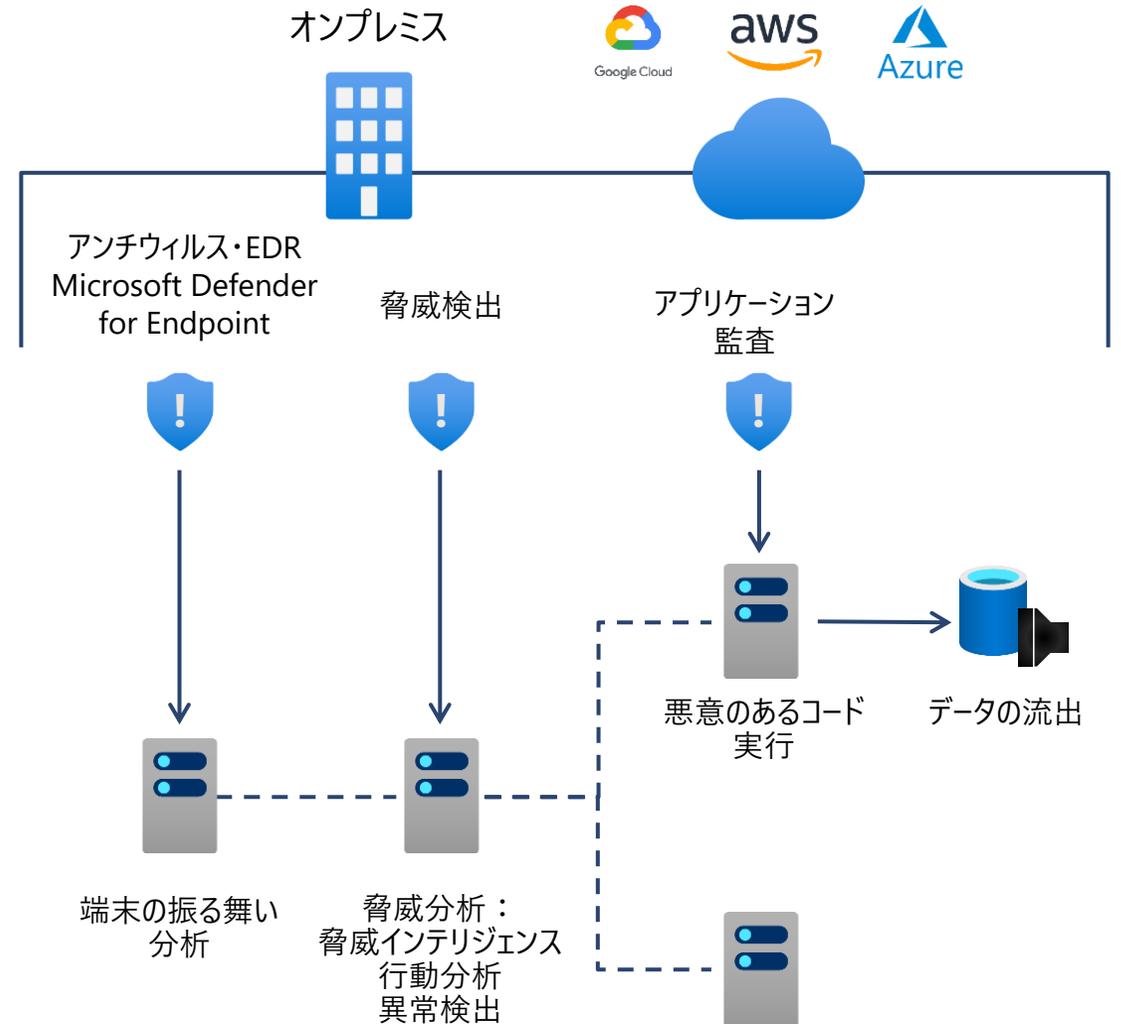


Defender for Servers

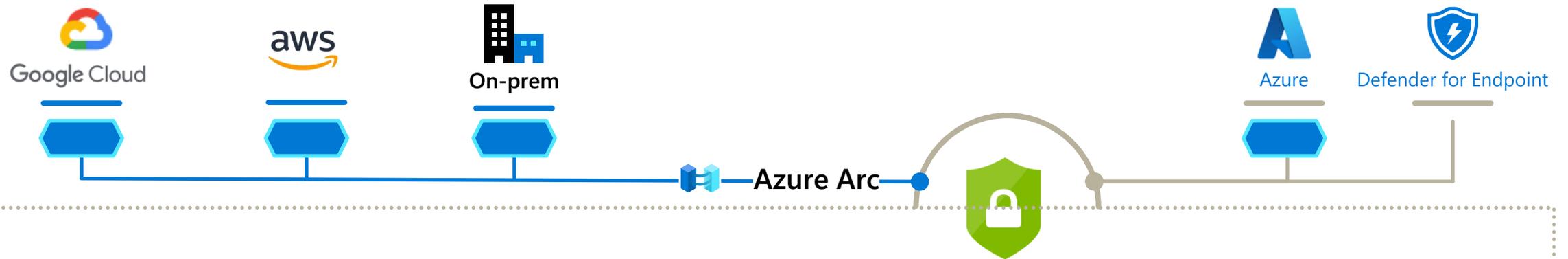
Microsoft Defender for Servers

サーバーを脅威から保護

- VM のセキュリティを 1 か所で把握
- スムーズな自動プロビジョニングでオンボーディングを簡素化
- マシンリソース、インベントリ一覧や脆弱性有無の確認



Microsoft Defender for Servers P1 / P2



セキュリティ 状況確認

セキュアスコア

規制
コンプライアンス

ネットワークマップ

脆弱性管理
(Qualys / MDE)

エージェントレス
スキャン

高度な クラウド防御

適応型
アプリケーション制御
(Adaptive Application Control)

VM への
JIT アクセス
(Just In Time)

Azure サービス上の
ネットワークふるまい検知
(Adaptive Network Hardening)

Docker をホストする
VMの保護
(Docker Host Hardening)

ファイル改ざん検知/
整合性監視
(File Integrity Monitoring)

脅威検知と対処

EDR

ファイルレス攻撃
の検出

Linux auditd ML

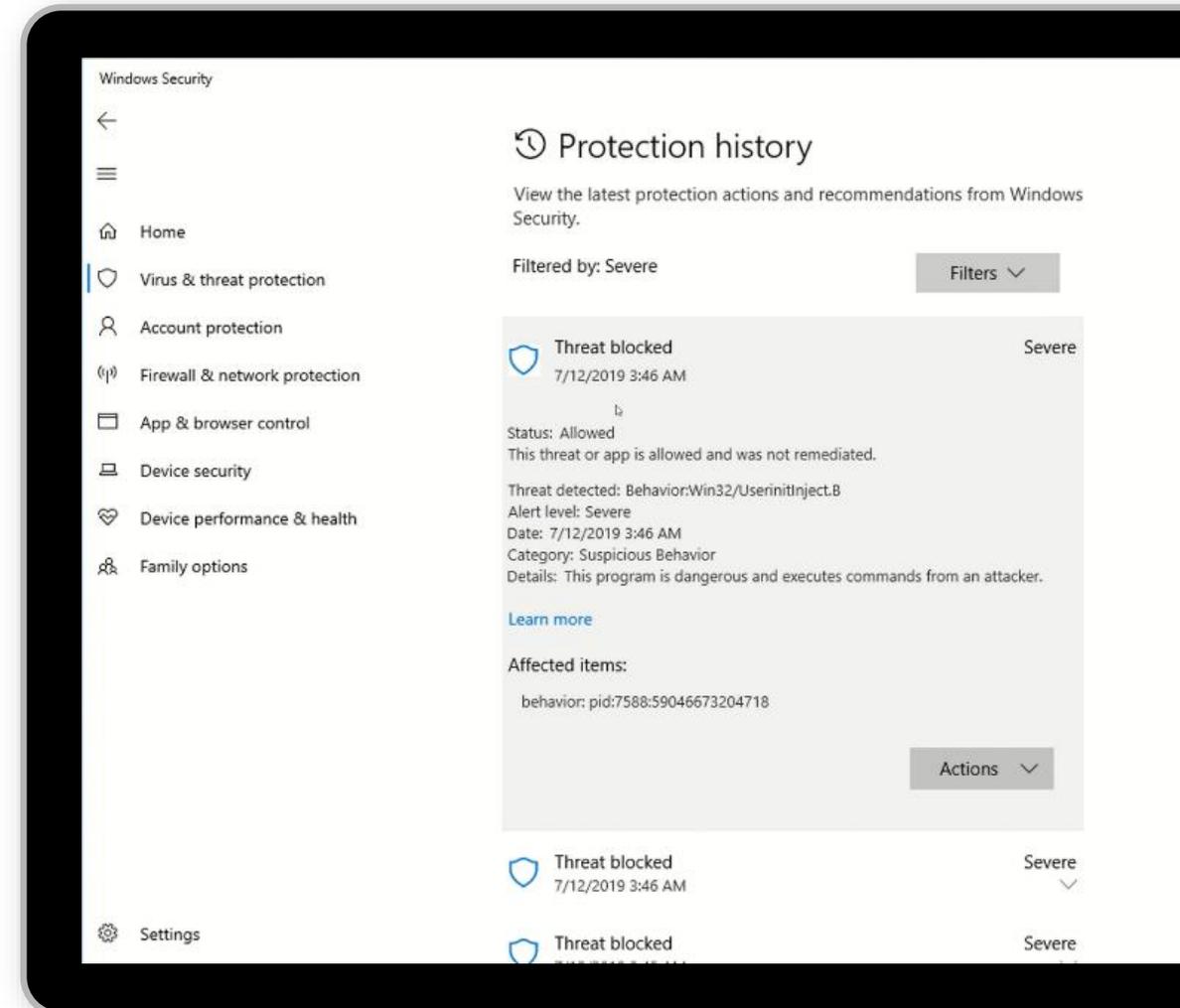
ワークフローによる
自動化

次世代ウイルス対策

Microsoft Defender for Endpoint が基盤

巧妙な脅威とマルウェアを阻止、対処

- 挙動ベースのリアルタイム保護
- ファイルベース/ファイルレス マルウェアをブロック
- 信頼済み/信頼されていないアプリケーションの悪意あるアクティビティを阻止



エンドポイントでの検出と応答

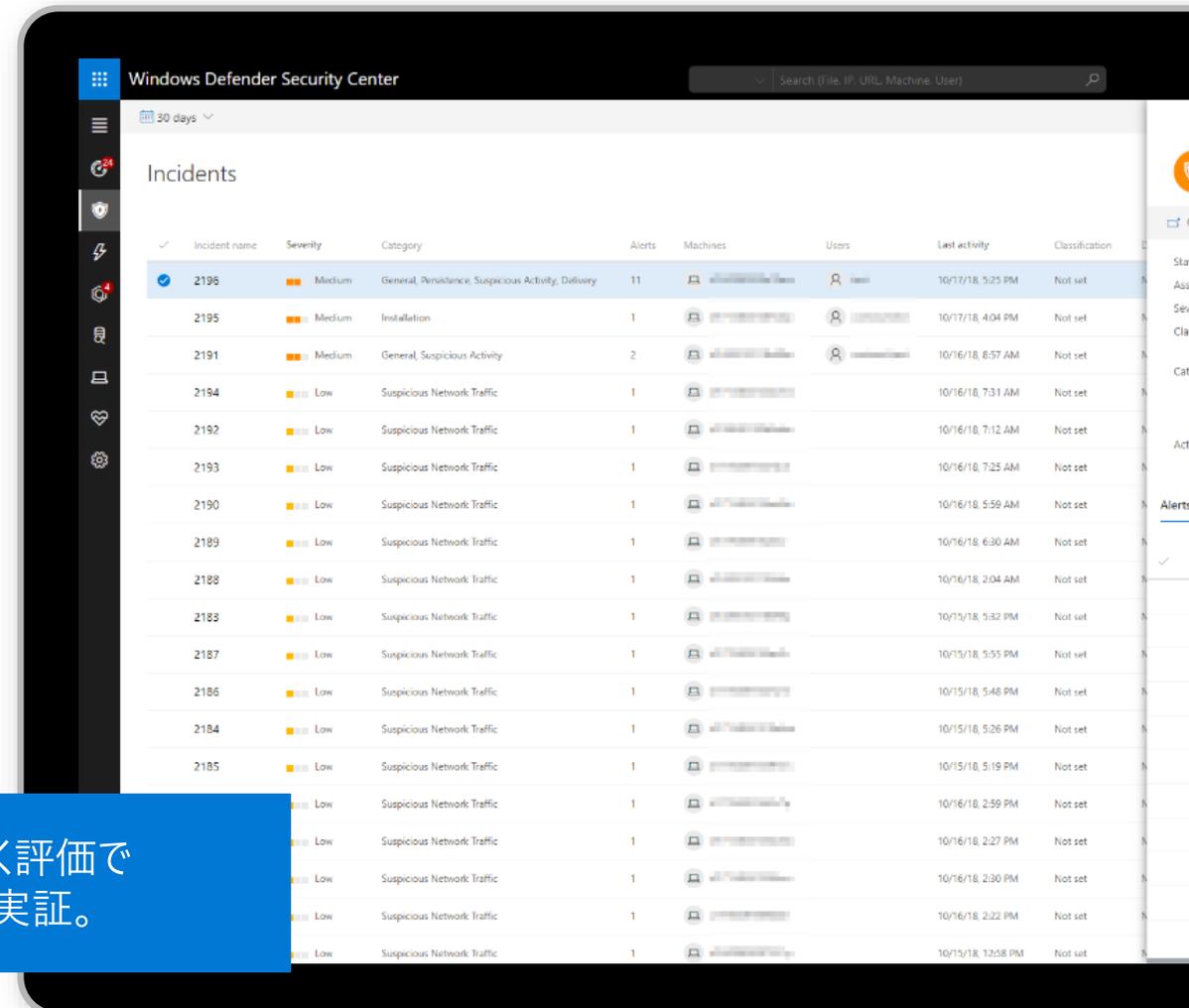
Microsoft Defender for Endpoint が基盤

標的型攻撃の検出と調査

- 相関関係のある挙動を警告
- 6 か月分のデータを調査
- さまざまな対応策



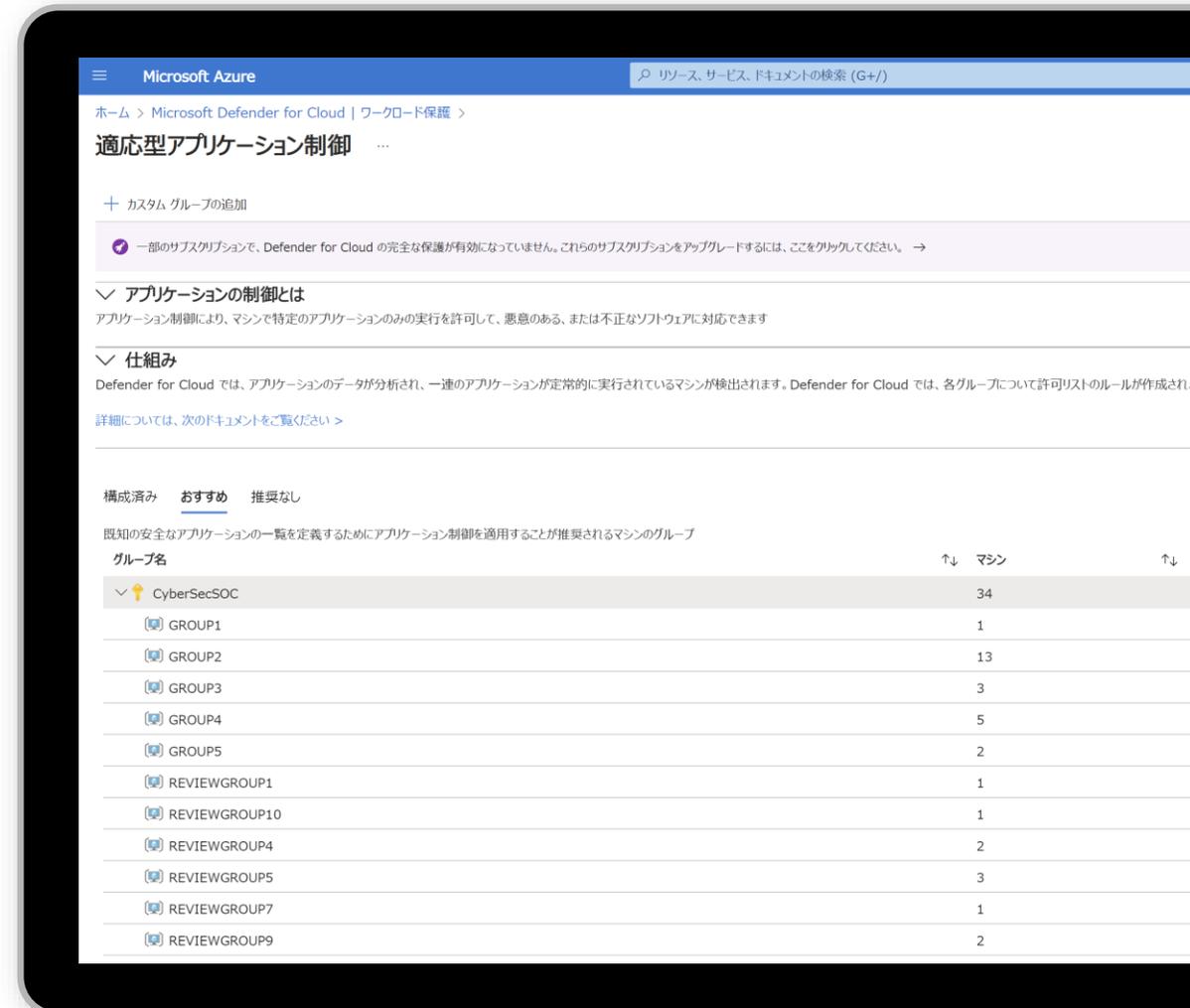
MITRE ATT&CK® に基づく評価で
業界最先端の検出性能を実証。



適応型アプリケーション制御

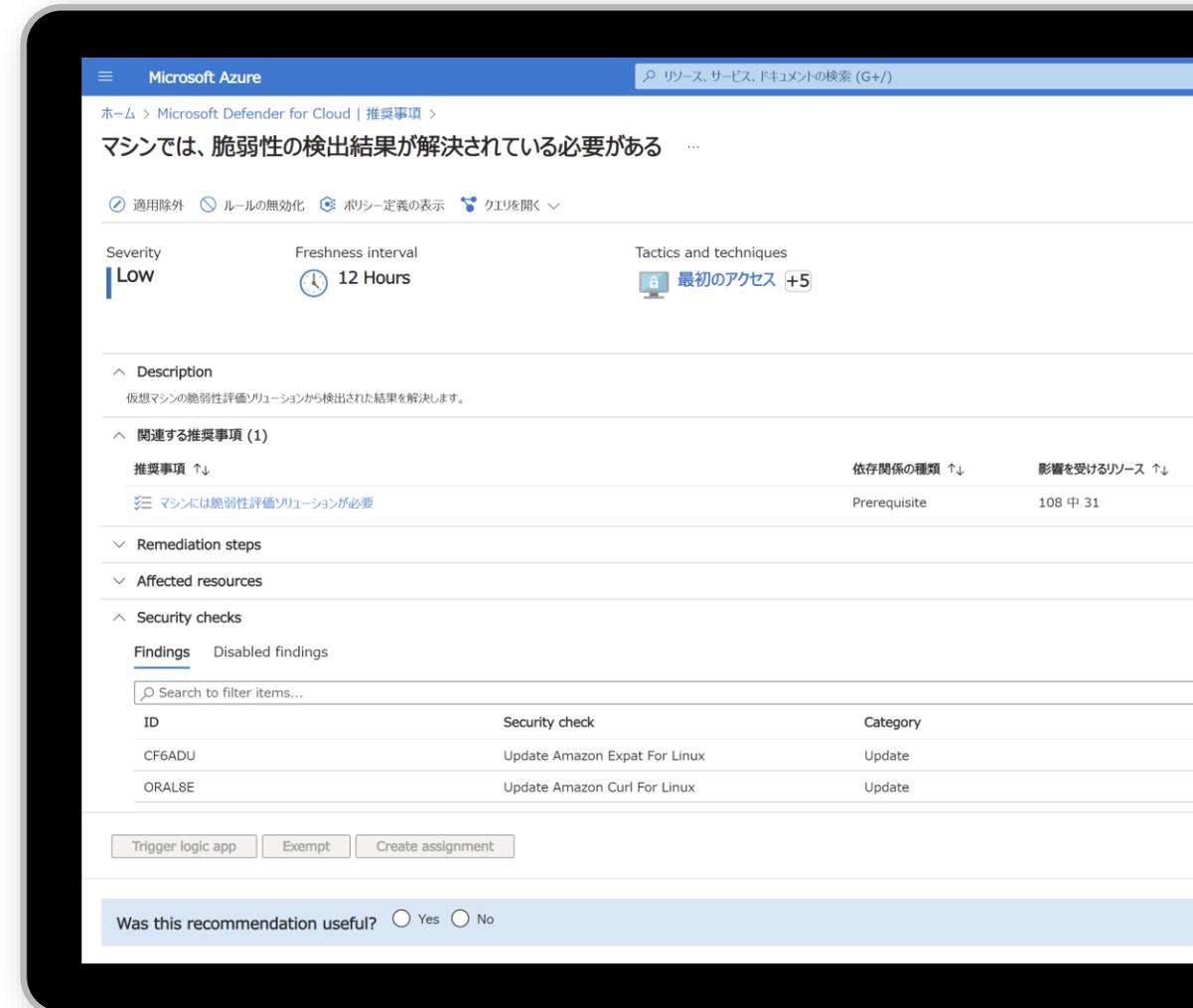
- 既知の安全なアプリケーションの許可リストを定義（ホワイトリスト）
- 機械学習によりホワイトリストを提示しリストに含まれていないアプリケーションが実行された場合にログ取得/実行禁止
- 組織によって禁止されているソフトウェアや古いバージョン/EOSのアプリケーションを特定

特定のグループのVM/サーバー上で稼働しているアプリケーションのうち、利用頻度が高く許可リストに定義を推奨するアプリケーション一覧の提示や、利用されていることは検出されているが許可すべきか確認を推奨するリストを提示するため、リスト作成の負荷を軽減。



VMやコンテナの脆弱性評価

- 脆弱性スキャナーを自動的にデプロイ
- インストール済みアプリケーションを継続的にスキャンしてLinux VM や Windows VM の脆弱性を検出
- 脆弱性の検出結果は Defender for Cloudのポータルや API で確認
- Qualys または マイクロソフトの脅威と脆弱性管理機能を選択（注：Qualysあるいは脆弱性管理アドオン機能を利用する場合はDefender for Servers Plan2が必要）



Just-In-Time の VM アクセス

- VMへのインバウンドトラフィックをロックダウンし、必要な時にだけVMにアクセスできる環境を実現
- 関連するIPアドレス/IPレンジから選択したポートへのインバウンドトラフィック(RDP/SSH)を許可するようにNSGとAzureファイアウォールを構成可能



ファイルの整合性の監視

- OS ファイル、Windows のレジストリ、アプリケーションソフトウェア、Linux のシステム ファイルなどに攻撃があったことを示す変更がないか検証
- 提案または独自のロジックに基づいて監視したいファイルを選択

The screenshot displays the Microsoft Azure portal interface for configuring file integrity monitoring. The page title is "Microsoft Azure" and the breadcrumb is "ホーム > Microsoft Defender for Cloud | 推奨事項 > マシンでファイルの整合性の監視を有効にする必要がある".

Key information shown includes:

- Severity:** High
- Freshness interval:** 24 時間
- Tactics and techniques:** 資格情報のアクセス +4

The **Description** section explains that Defender for Cloud identifies machines without file integrity monitoring and recommends enabling it for important files and registry keys. It also notes that monitoring is only effective if data collection rules are assigned to the machines and files are defined.

The **Affected resources** section shows 7 unhealthy resources, 0 healthy resources, and 5 not applicable resources. A table lists these resources:

Name	Subscription	Owner	Due date
<input type="checkbox"/> winsvr2012r2-sql	AIA Program External Account Subscription		
<input type="checkbox"/> winsvr2012r2	AIA Program External Account Subscription		
<input type="checkbox"/> win10-ent-0	AIA Program External Account Subscription		
<input type="checkbox"/> centos7.local	AIA Program External Account Subscription		
<input type="checkbox"/> at-avd-demo-adds-vm	AIA Program External Account Subscription		
<input type="checkbox"/> at-arc-demo-public-win2022dc-ec2	AIA Program External Account Subscription		

At the bottom, there are buttons for "Fix", "Trigger logic app", "Assign owner", and "Change owner and set ETA". A feedback question "Was this recommendation useful?" is also present with "Yes" and "No" radio buttons.

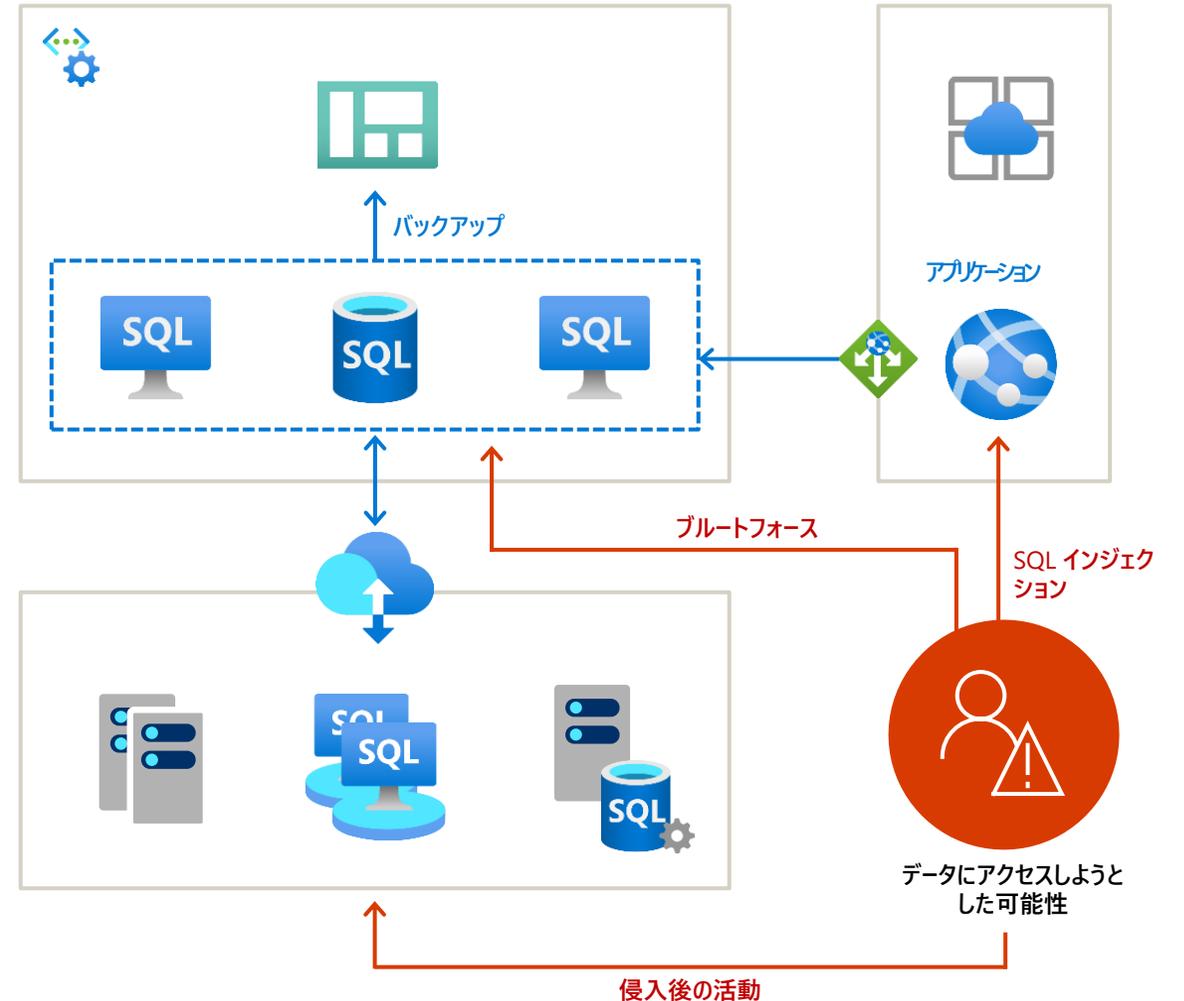


Defender for SQL

Microsoft Defender for SQL

SQLデータベースを脅威から保護

- データベースの「脆弱性」と「脅威」を検出して軽減
- Azure SQL Database と SQL サーバーの両方に対応



SQLデータベースの脆弱性評価

- データベースのセキュリティを可視化し、強化する仕組み
- Azure SQL Database に組み込まれたスキャン サービスで、セキュリティの脆弱性を検出
- Microsoft のベスト プラクティスに基づいた規則を使って誤った設定、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検出
- 評価レポートは利用環境に合わせてカスタマイズ可能

The screenshot displays the Microsoft Defender for SQL interface. At the top, it shows the resource name 'contosocrmdb (contocrmsrv/contosocrmdb)'. Below this, there are navigation options like 'スキャン' (Scan) and 'クエリを開く' (Open query). A summary table shows the overall security status:

Resource	脆弱性の合計	重大度別の脆弱性	最終スキャン時刻
contosocrmdb	3	High 2, Medium 0, Low 1	2023/10/19 23:20:19 (UTC+9)

Below the summary, there is a table of detected security checks:

ID	Security check	Category
VA2108	Minimal set of principals should be members of fixed high impact database roles	Authentication And Auth
VA1258	Database owners are as expected	Auditing And Logging
VA2130	Track all users with access to the database	Authentication And Auth

At the bottom, it indicates '検索結果: 1 - 3 / 3 件。' (Search results: 1 - 3 / 3 items).

SQLデータベースに対する脅威検出

クエリ分析

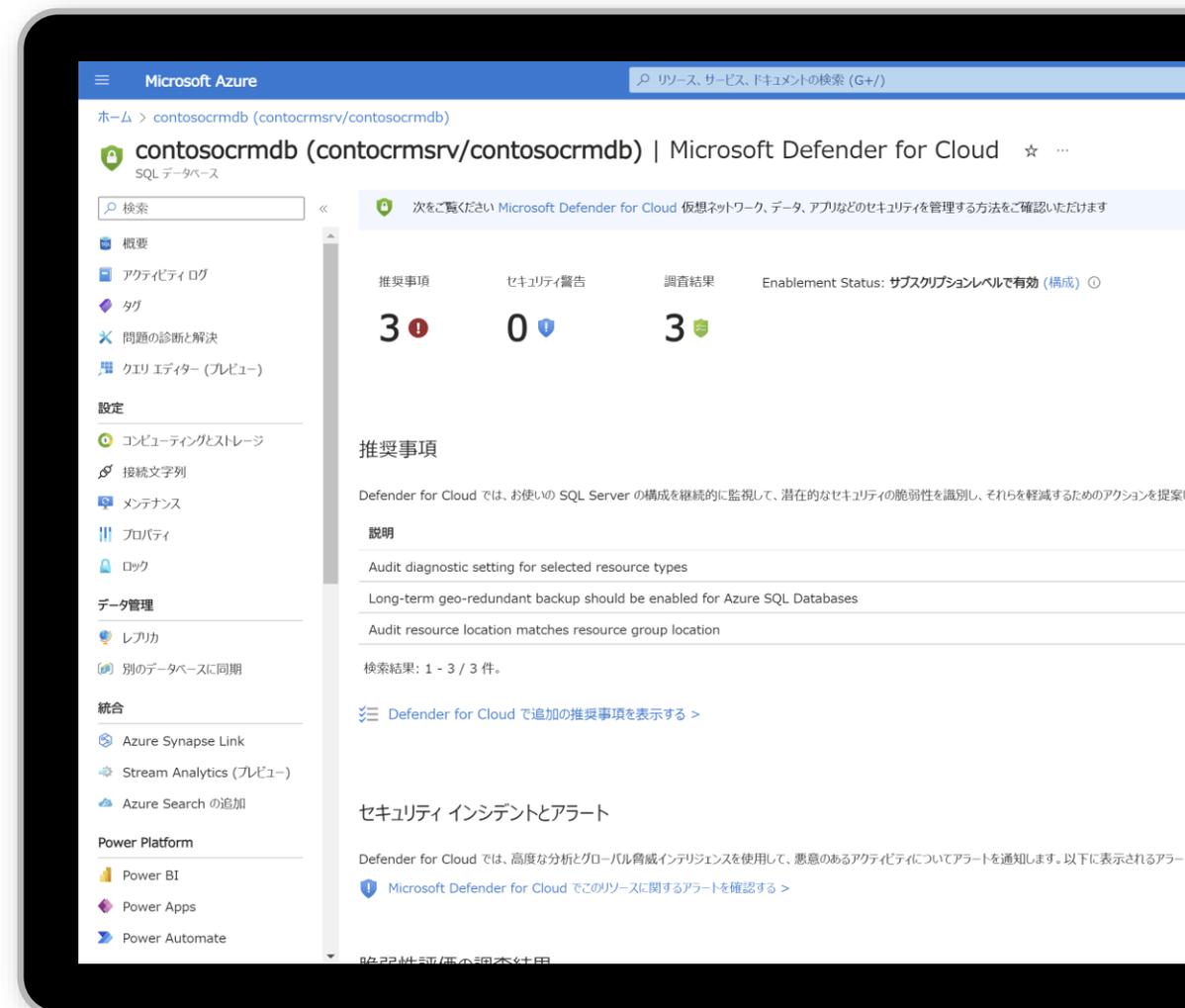
- SQL インジェクションの可能性
- SQL インジェクションに対する脆弱性
- 異常な量のデータ抽出
- 普段とは異なるデータ抽出先

脅威インテリジェンス

- 普段見られない場所からのアクセス
- 不審な IP からのアクセス
- プリンシパルの異常
- 不審なアプリ

ブルートフォース

- ブルートフォースの可能性
- 有効なユーザーに対するブルートフォースの可能性
- 成功した可能性があるブルートフォース





まとめ

Topics

1. クラウド時代のセキュリティリスク
2. Defender for Cloud 概要
 1. MS Defender / Defender for Cloud
 2. CSPM , CWPP
3. CSPM
4. CWPP
 1. Defender for Server
 2. Defender for SQL



MICROSOFT CONFIDENTIAL

本資料には、マイクロソフトの秘密情報が含まれます。本資料は、合理的に知る必要のある貴社内関係者のみ閲覧できるものとし、マイクロソフトの承諾がない限り、それ以外の第三者に対して、開示、共有等してはならず、また複製も禁じられます。

本資料は情報提供のみを目的としており、本資料に記載されている情報は、本資料作成時点でのマイクロソフトの見解を示したものです。状況等の変化により、内容は変更される場合があります。本資料に表記されている内容（提示されている条件等を含みます）は、貴社との有効な契約を通じて決定されます。それまでは、正式に確定するものではありません。従って、本資料の記載内容とは異なる場合があります。また、本資料に記載されている価格はいずれも、別段の表記がない限り、参考価格となります。貴社の最終的な購入価格は、貴社のリセラー様により決定されます。マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。

© Copyright Microsoft Corporation. All rights reserved.