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

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

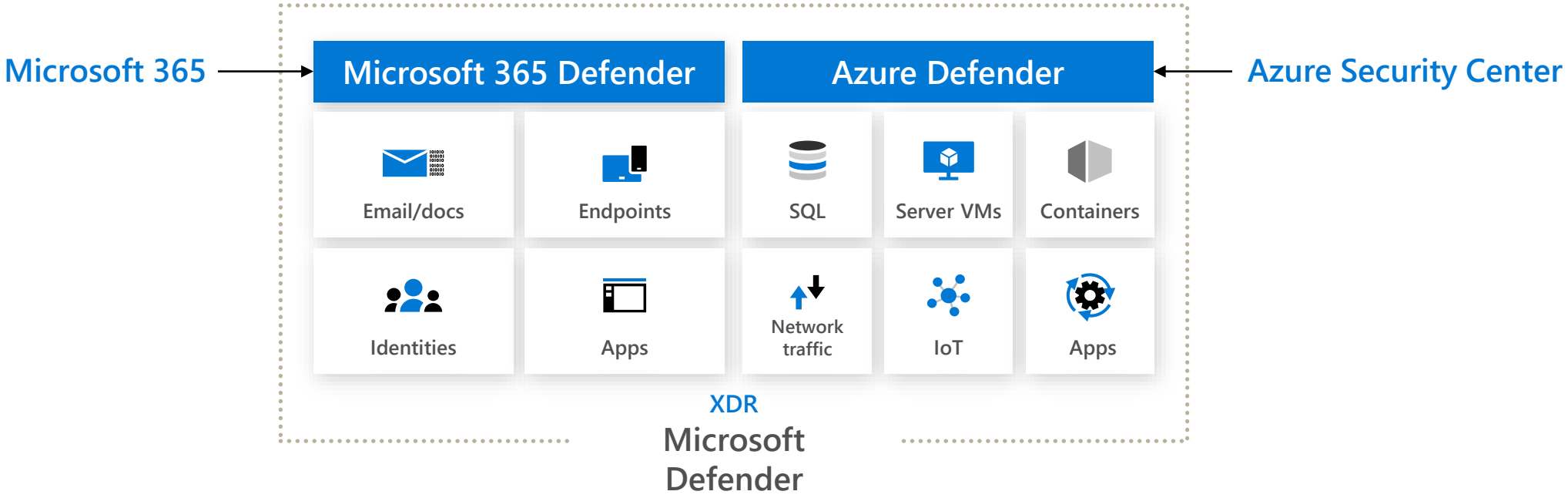
$4.24M

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 のポスチャー管理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

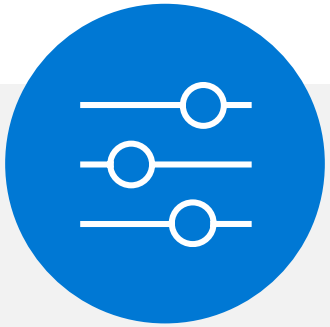
高度な脅威からの保護

- 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、アノマリー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

Microsoft

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

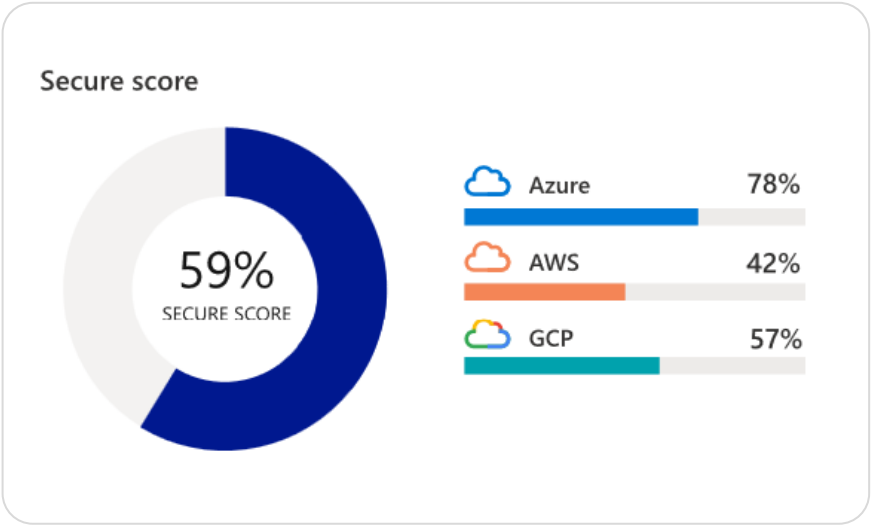
ガバナンス管理
所有者の自動割り当て | 組織におけるアカウンタビリティの推進 | 猶予期間 | 修正にかかる時間を短縮

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
- インベントリー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

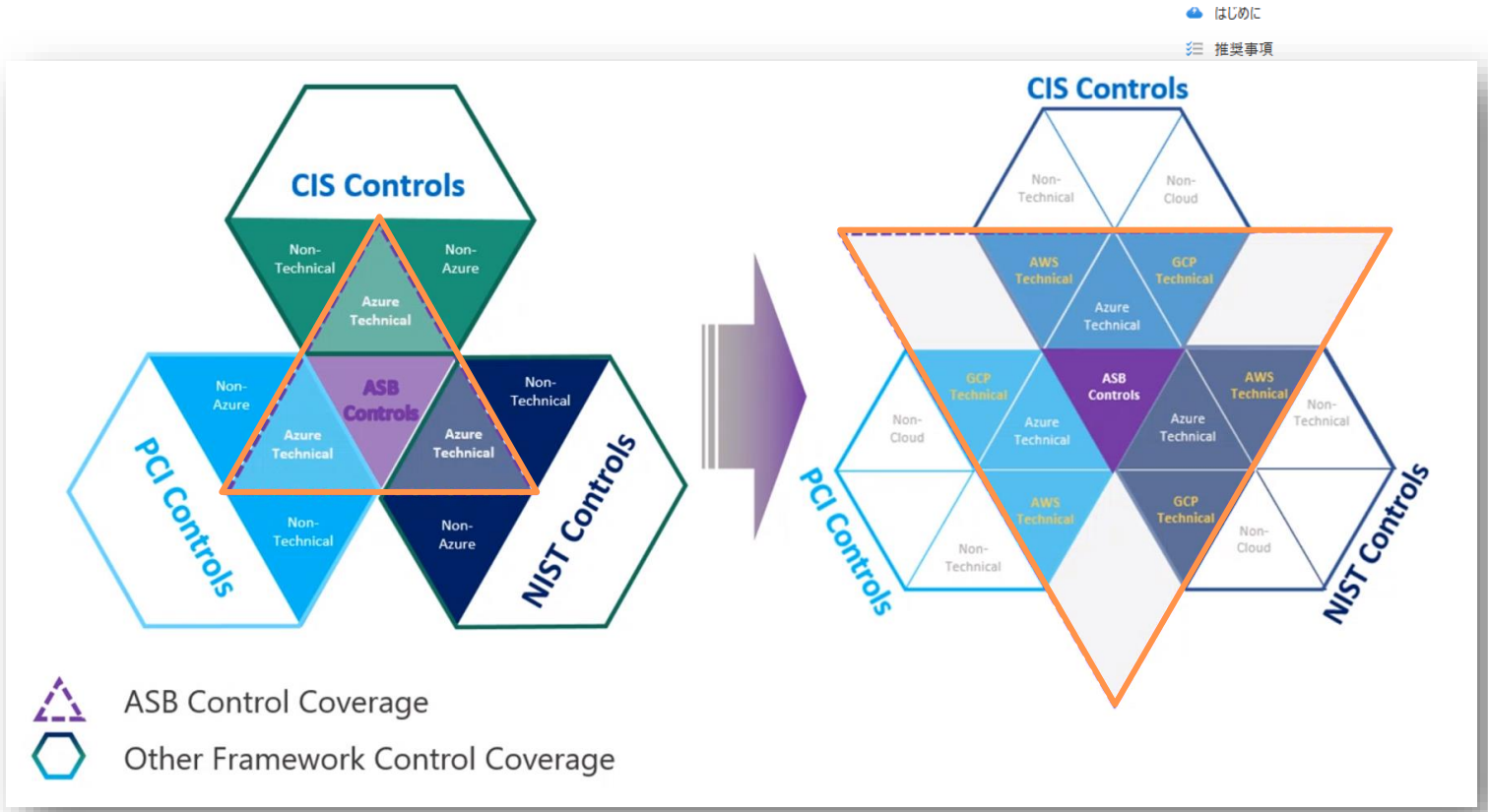
- AWS, Azure, GCPの環境横断的な継続的な評価を行い、単一の統合されたダッシュボード上でクラウドセキュリティコンプライアンスの管理
- 業界標準、規制コンプライアンス、クラウド特有のベンチマークを踏まえたベストプラクティス
  (CIS, PCI, NISTなど)

基本的なCSPM

Microsoft クラウド セキュリティ ベンチマーク (MCSB)

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



Microsoft クラウド セキュリティ ベンチマークの概要 | Microsoft Learn

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

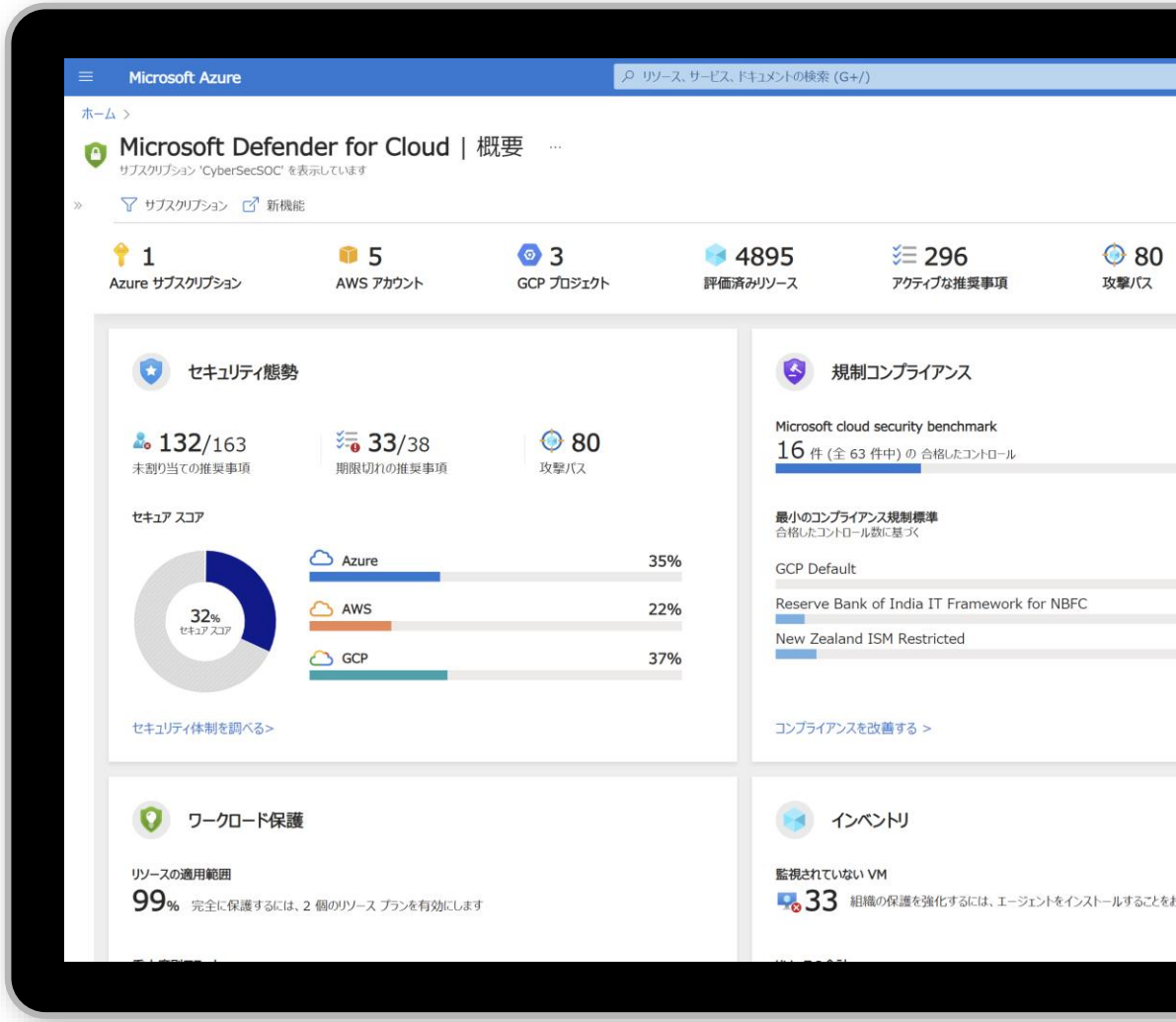
シンプルなメニュー

→ 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



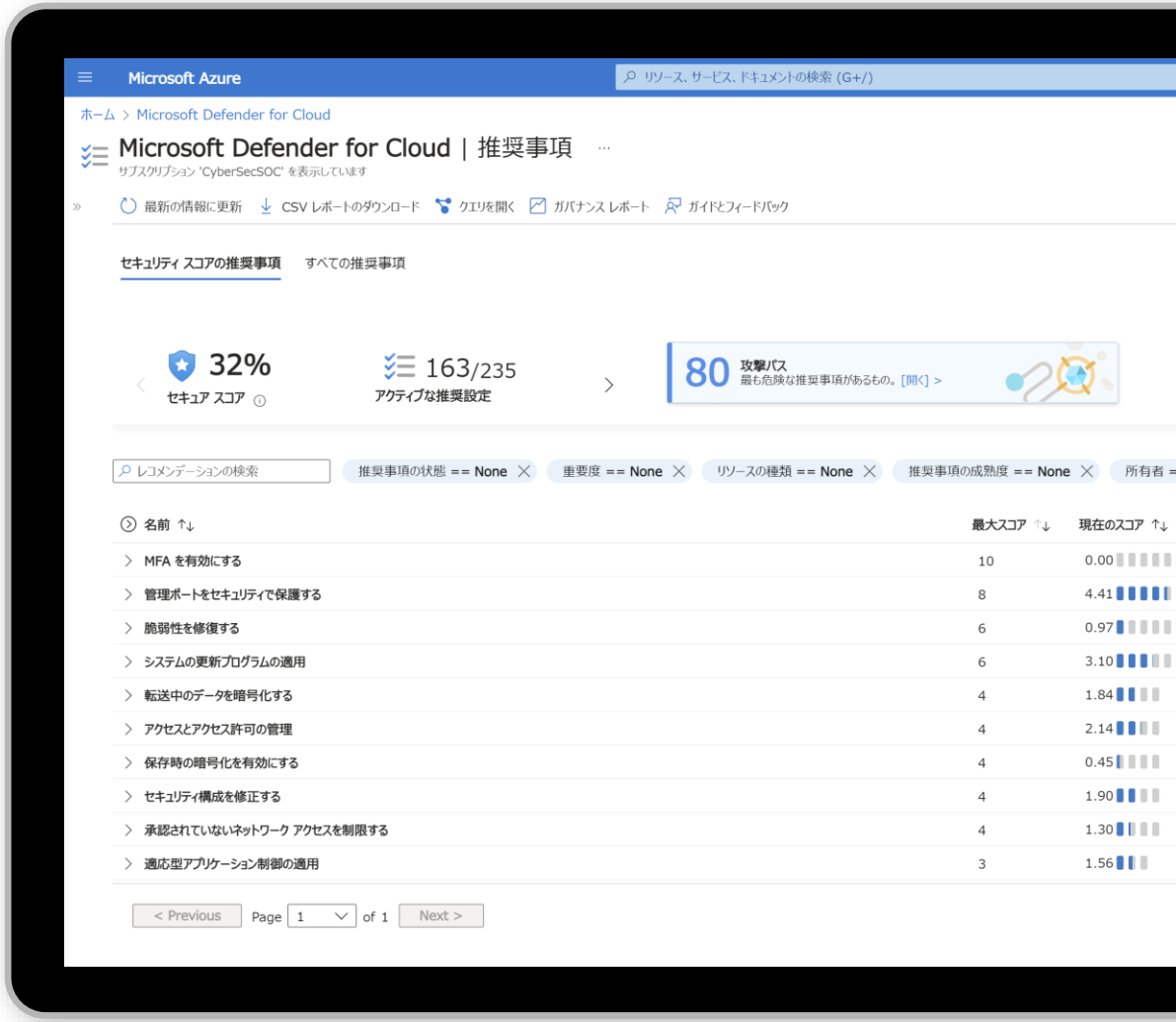
推奨事項

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

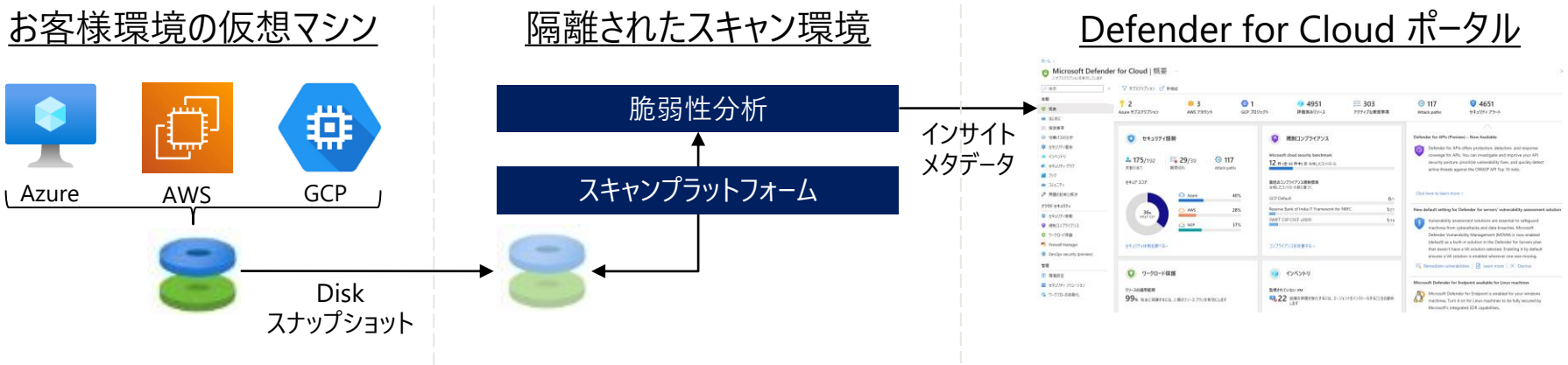


Defender CSPM

Defender for Servers P2

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



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

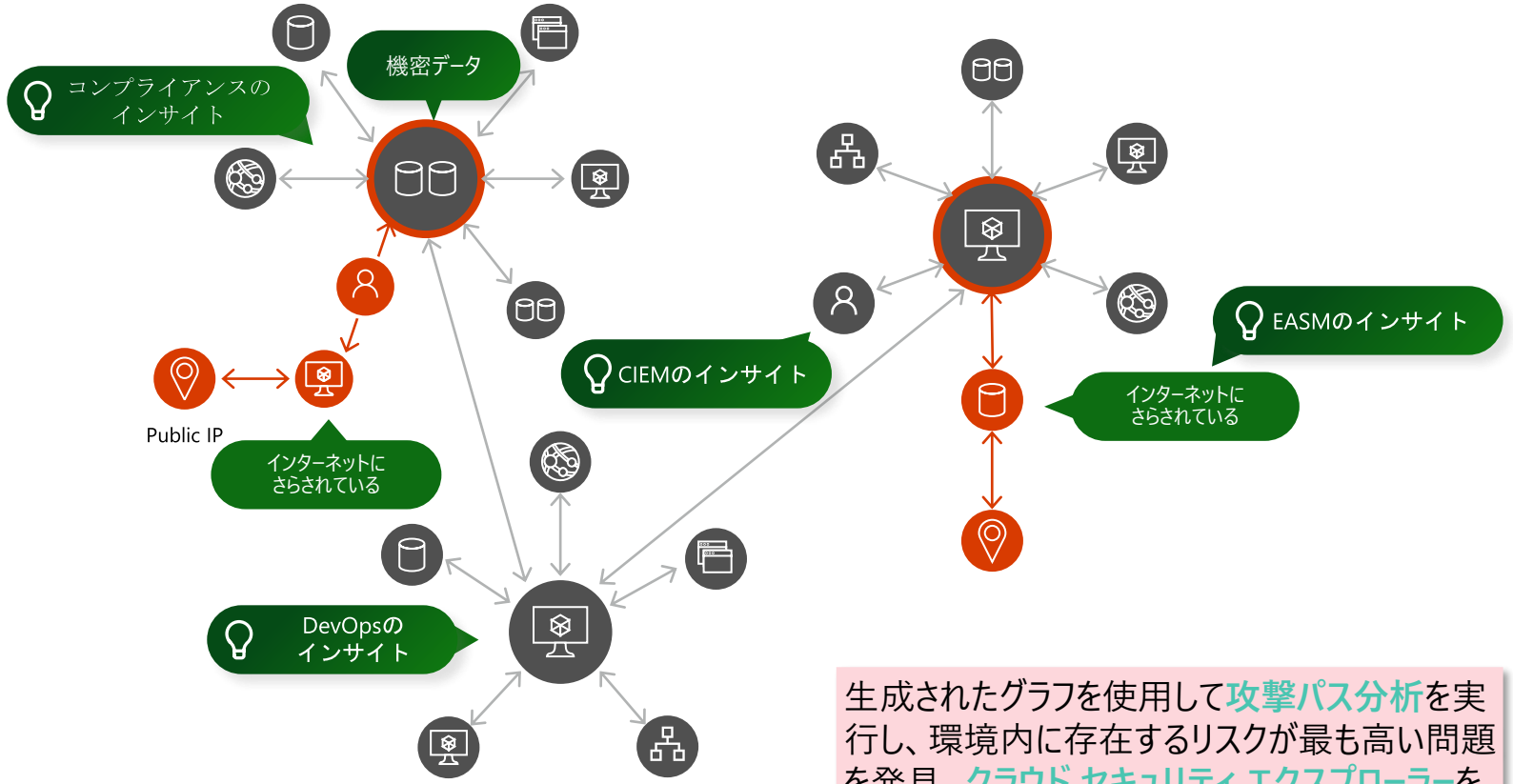
VM のエージェントレス スキャンについて学習する - Microsoft Defender for Cloud | Microsoft Learn

Defender CSPM

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 インサイトを使用して、**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 エクスプローラー**を使用してグラフのクエリを実行することも可能

Defender CSPM

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

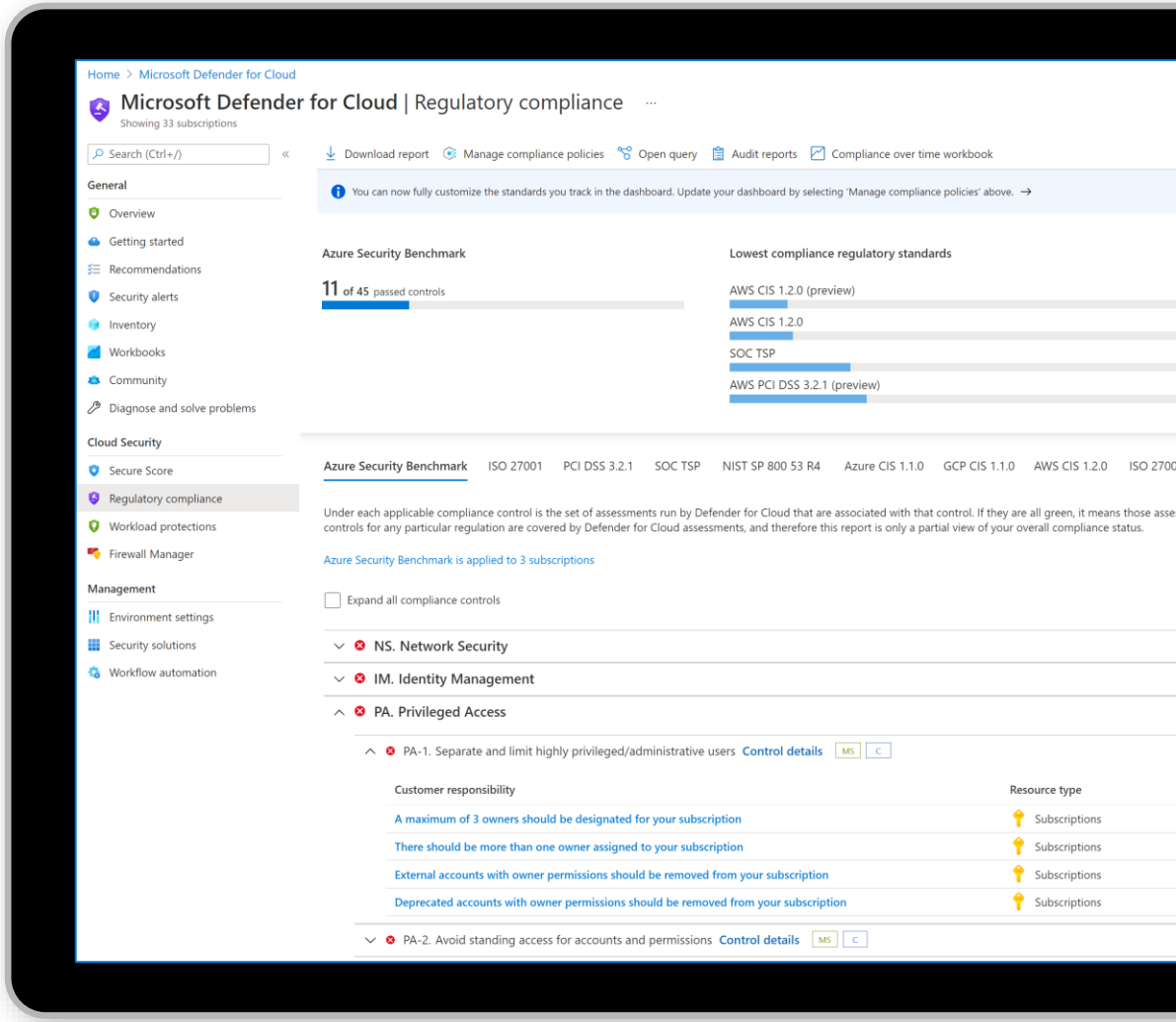
攻撃パス分析での検出例：
高い緊急度の脆弱性を持ち、インターネットに晒されているVMがストレージアカウントへの参照権限を持っている。かつそのストレージアカウントには機微な情報が含まれている -> **危険性高！**

Defender CSPM

他Defenderの有償プラン

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:

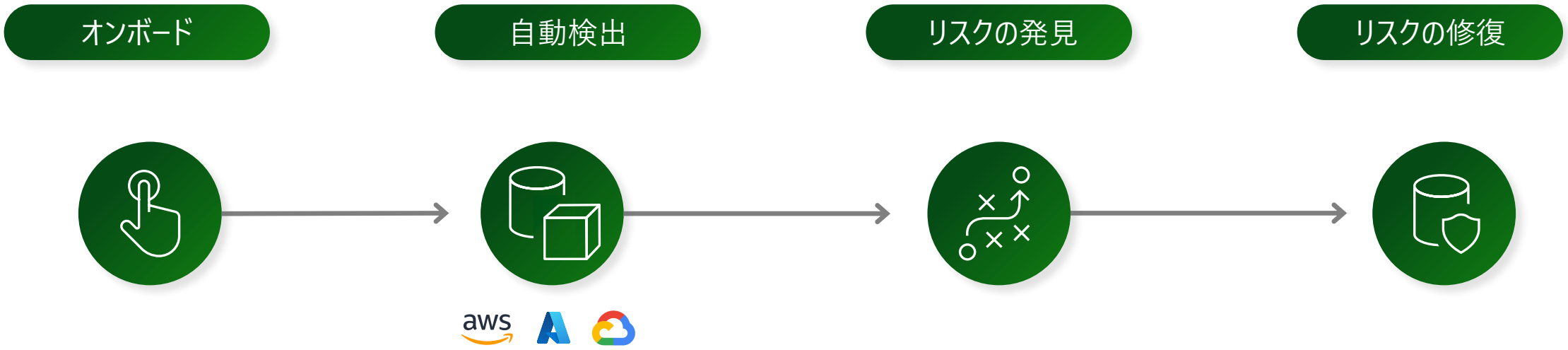
- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Microsoft Cloud Security Benchmark
- ✓ AWS Foundational Security best practices

Defender CSPM

Defender for Storage

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



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

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

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**

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**

Defender CSPM

Defender for Containers

コンテナーセキュリティ態勢

- Defender CSPMで、コンテナー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Kubenetes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、Kubenetes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

◆コンテナー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、またはコンテナーへの影響を必要とせずに脆弱性の評価結果を取得

Agentless Container Posture for Microsoft Defender for Cloud | Microsoft Learn

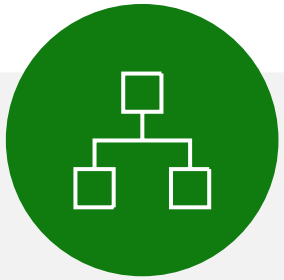
Microsoft

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

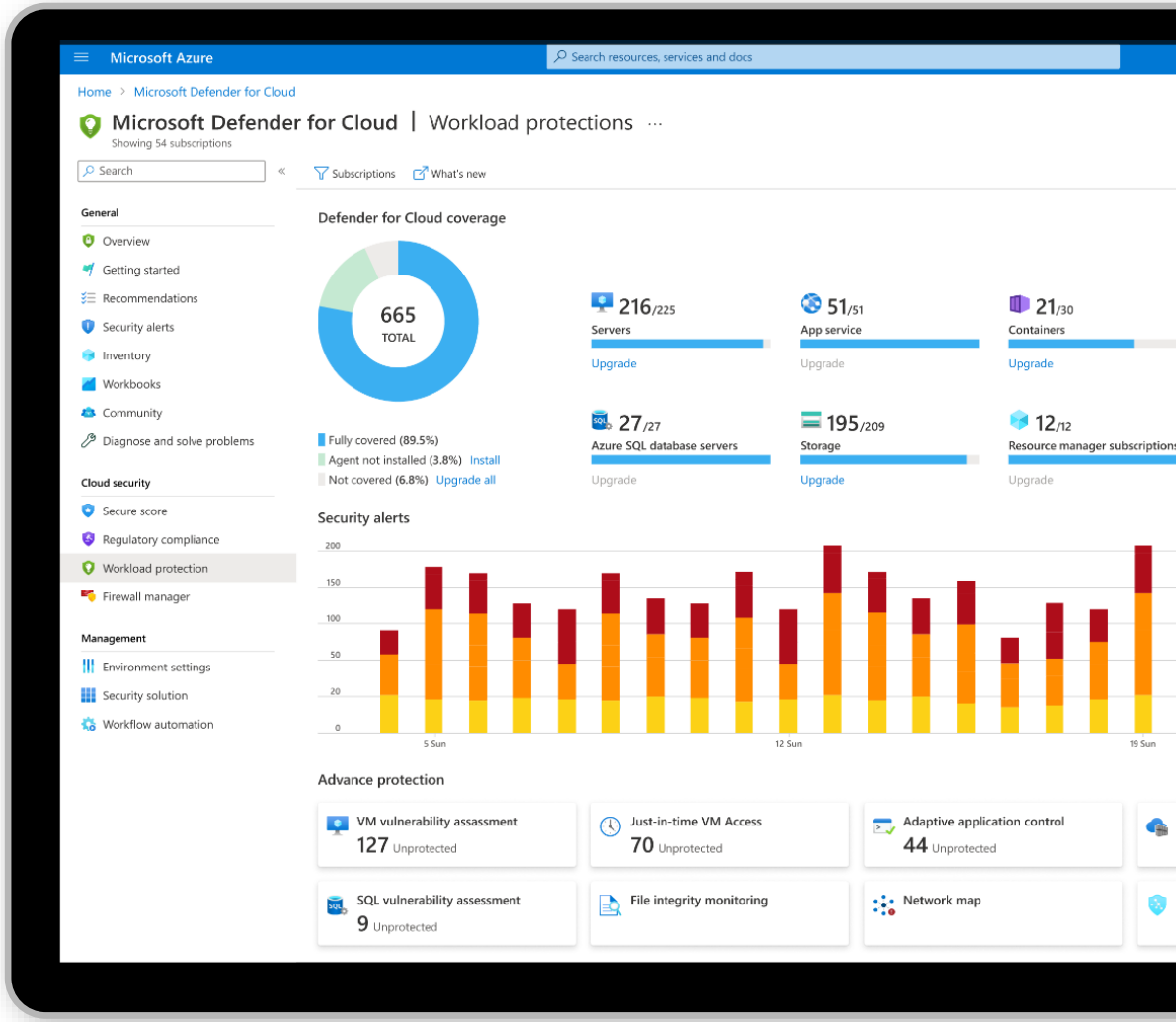
脆弱性を悪用される前に特定して修復

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 Containes

Microsoft Defender for Key Vault

Microsoft Defender for Resource Manager

Microsoft Defender for Resource Manager

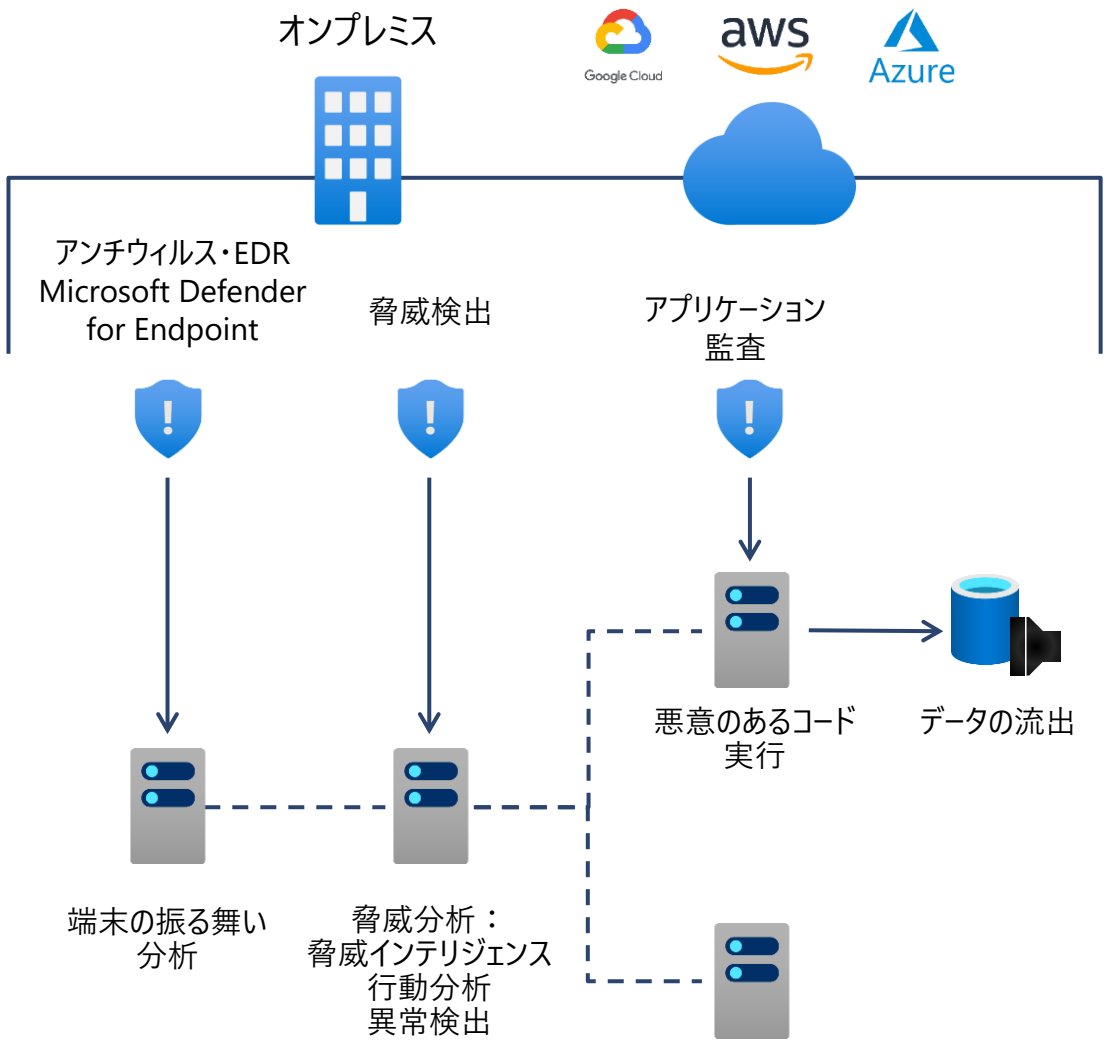
Microsoft

Defender for Servers

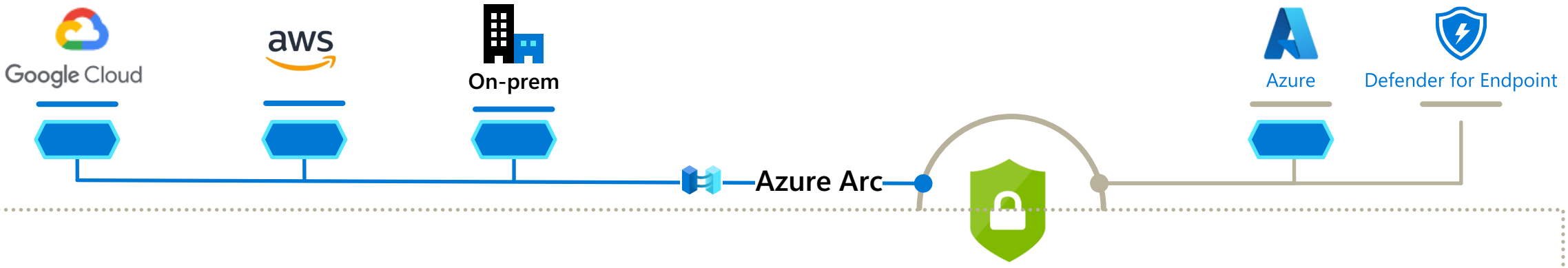
Microsoft Defender for Servers

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

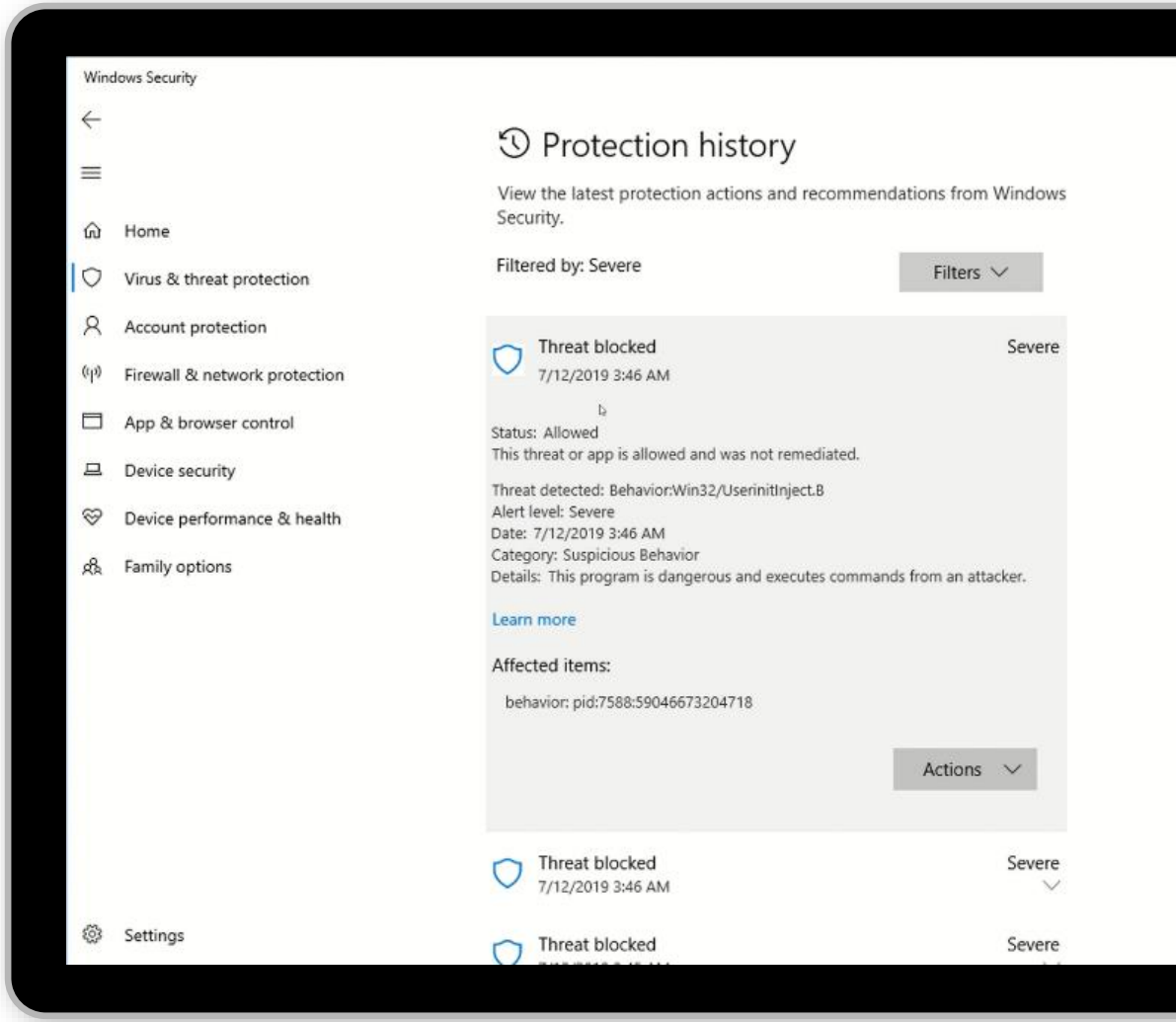
Defender for Servers
Plan 1/2

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



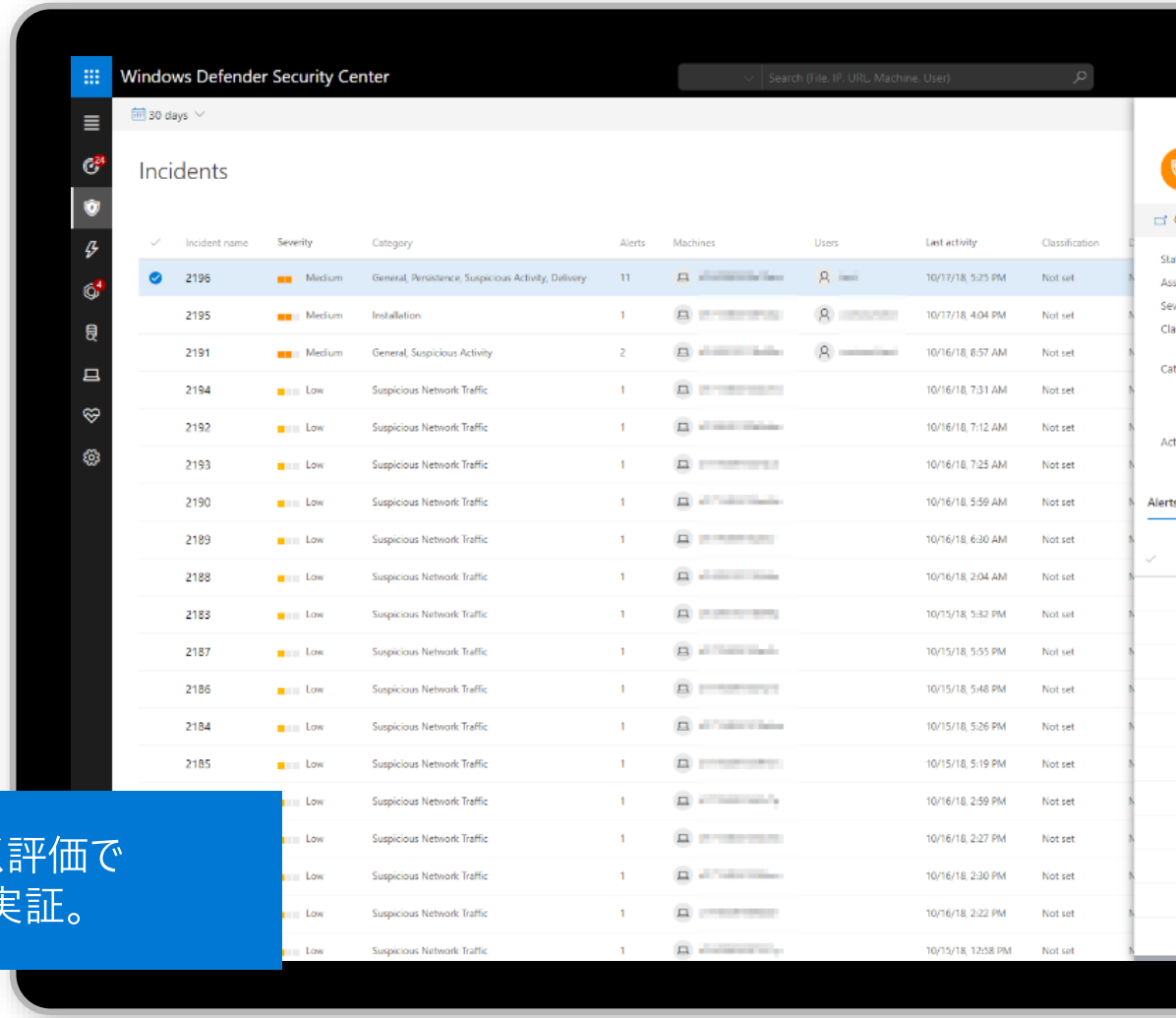
Defender for Servers
Plan 1/2

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



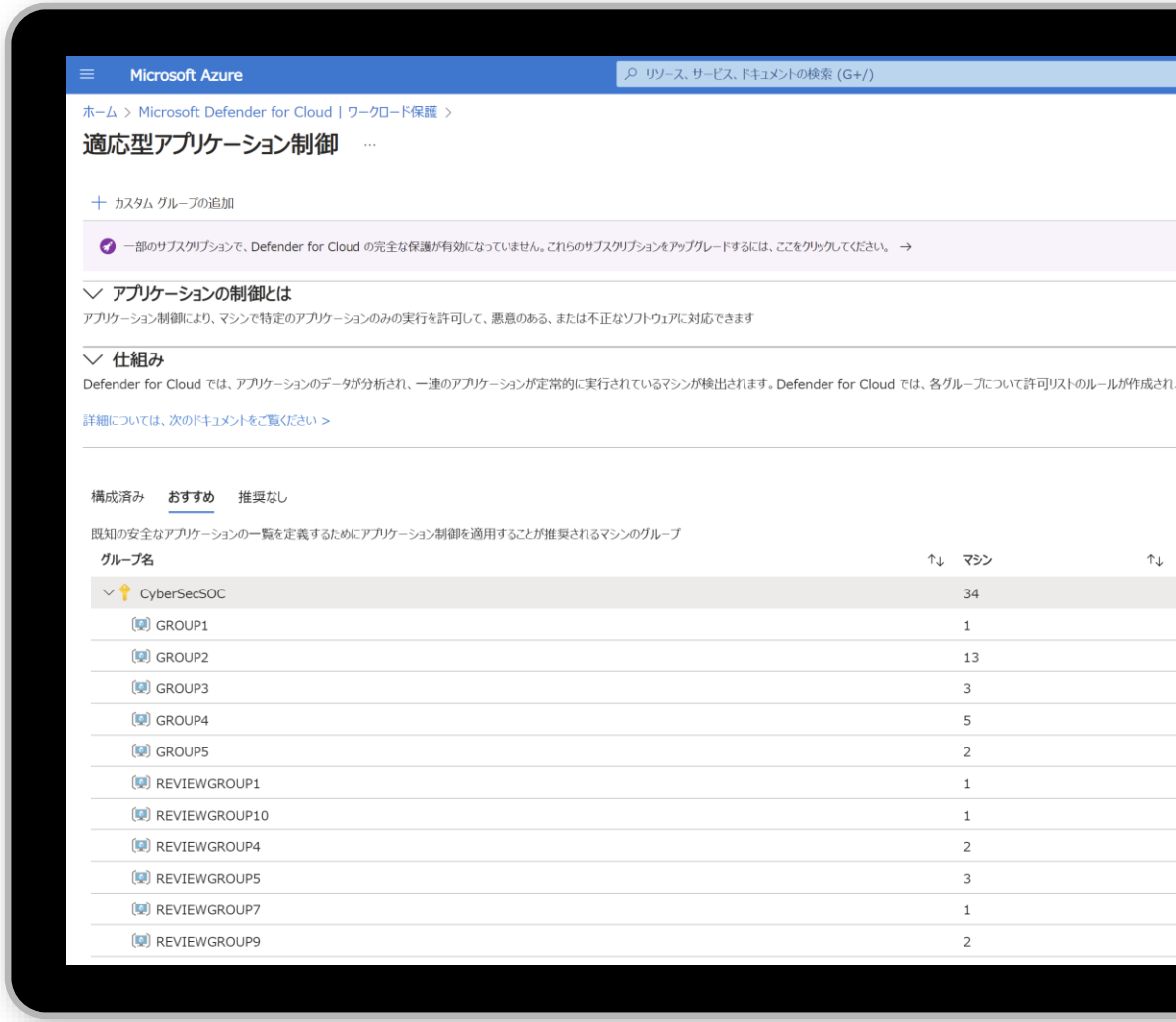
MITRE ATT&CK® に基づく評価で
業界最先端の検出性能を実証。

Defender for Servers Plan 2

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

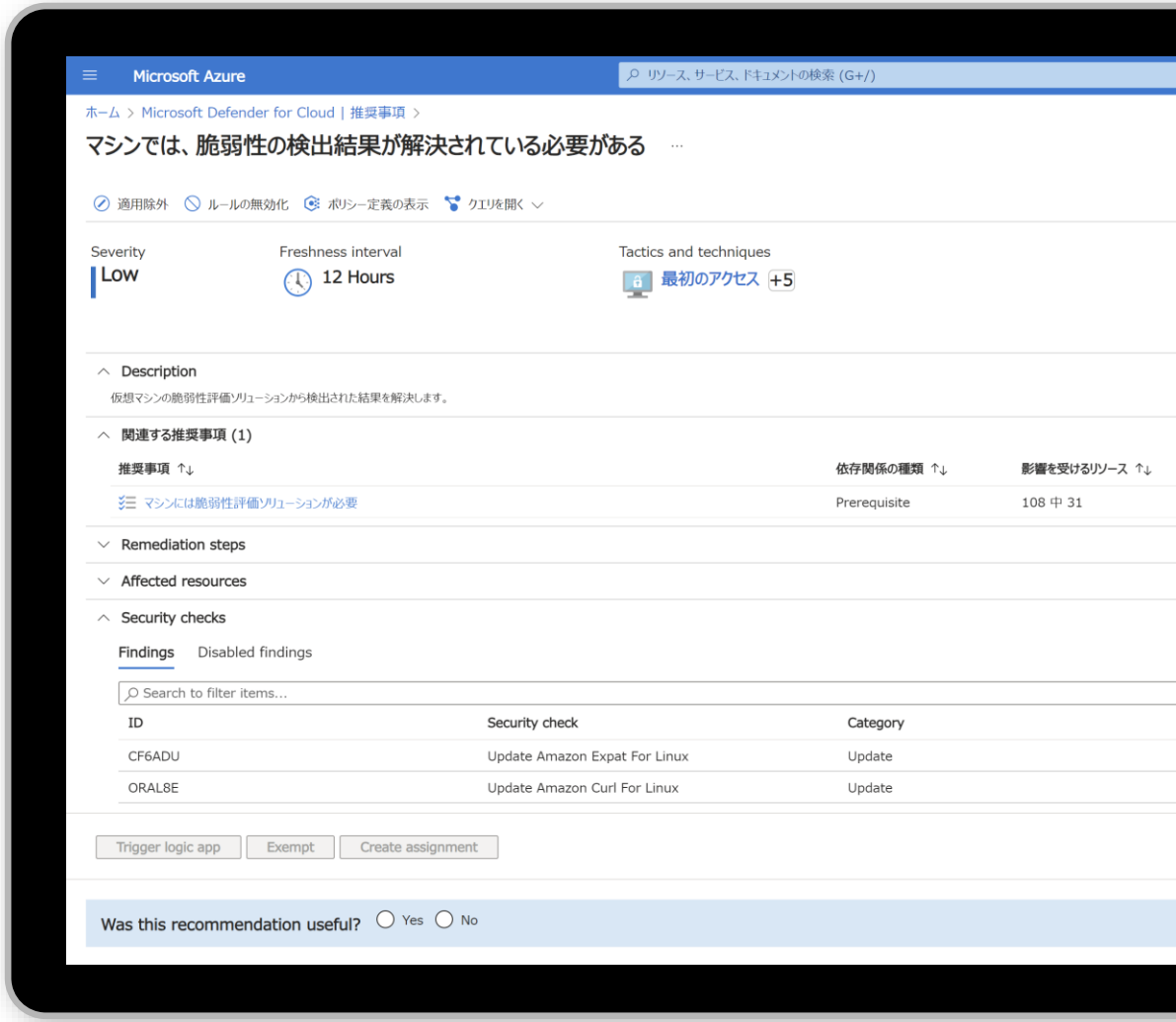
特定のグループのVM/サーバー上で稼働しているアプリケーションのうち、利用頻度が高く許可リストに定義を推奨するアプリケーション一覧の提示や、利用されていることは検出されているが許可すべきか確認を推奨するリストを提示するため、リスト作成の負荷を軽減。



Defender for Servers Plan 1/2

VMやコンテナーの脆弱性評価

- 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）



Defender for Servers Plan 2

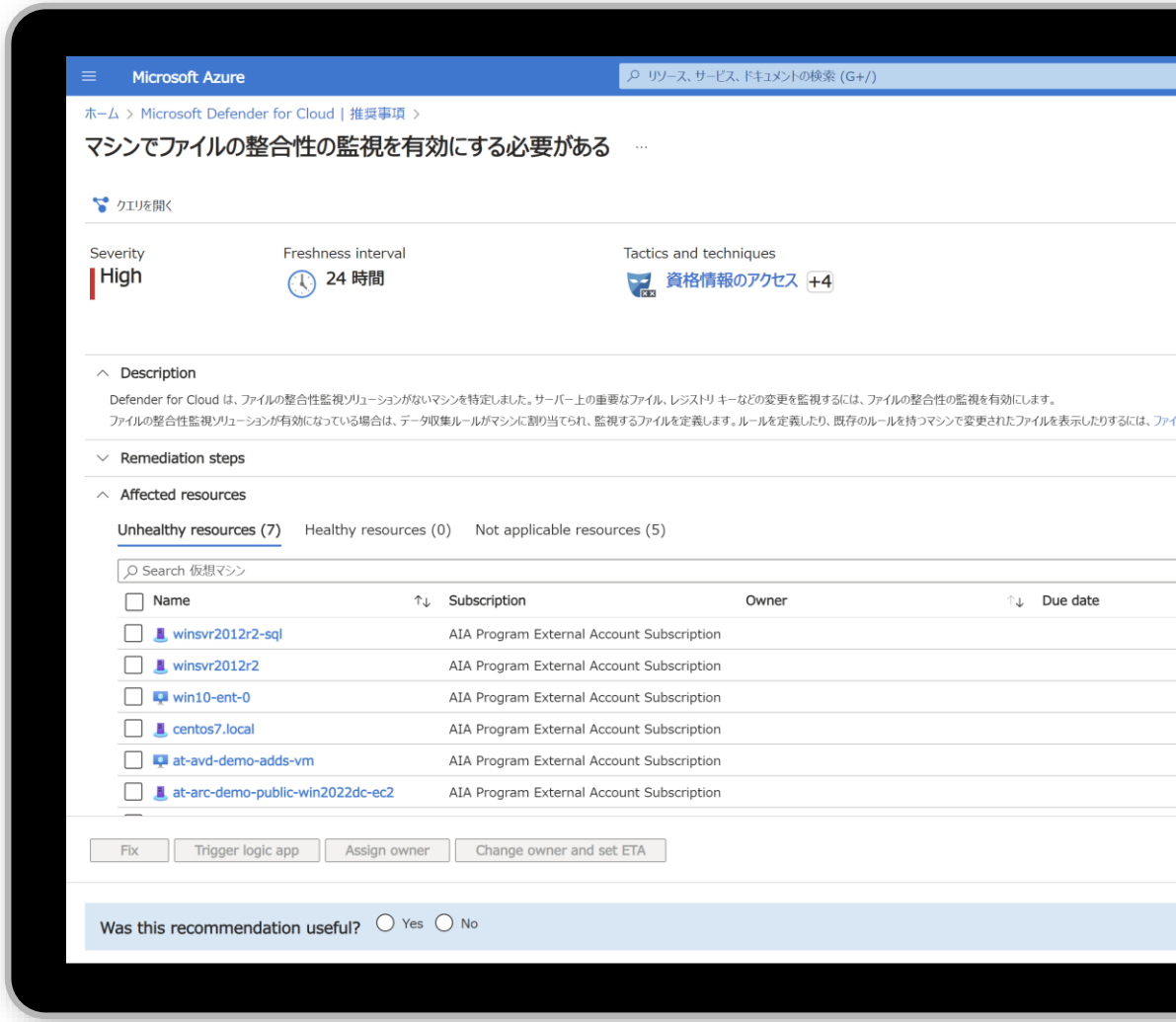
Just-In-Time の VM アクセス

- 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

Defender for Servers Plan 2

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



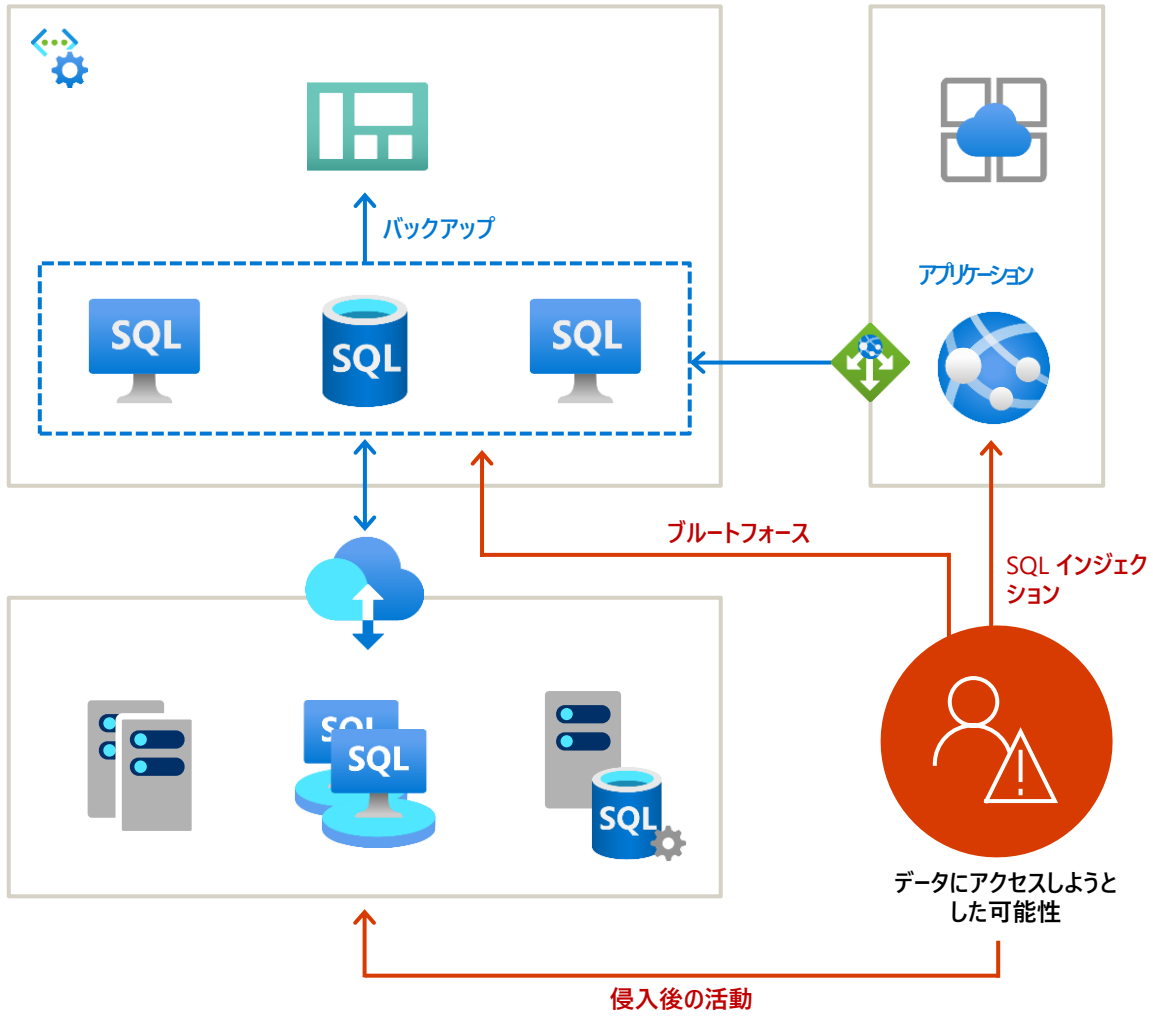
Microsoft

Defender for SQL

Microsoft Defender for SQL

SQLデータベースを脅威から保護

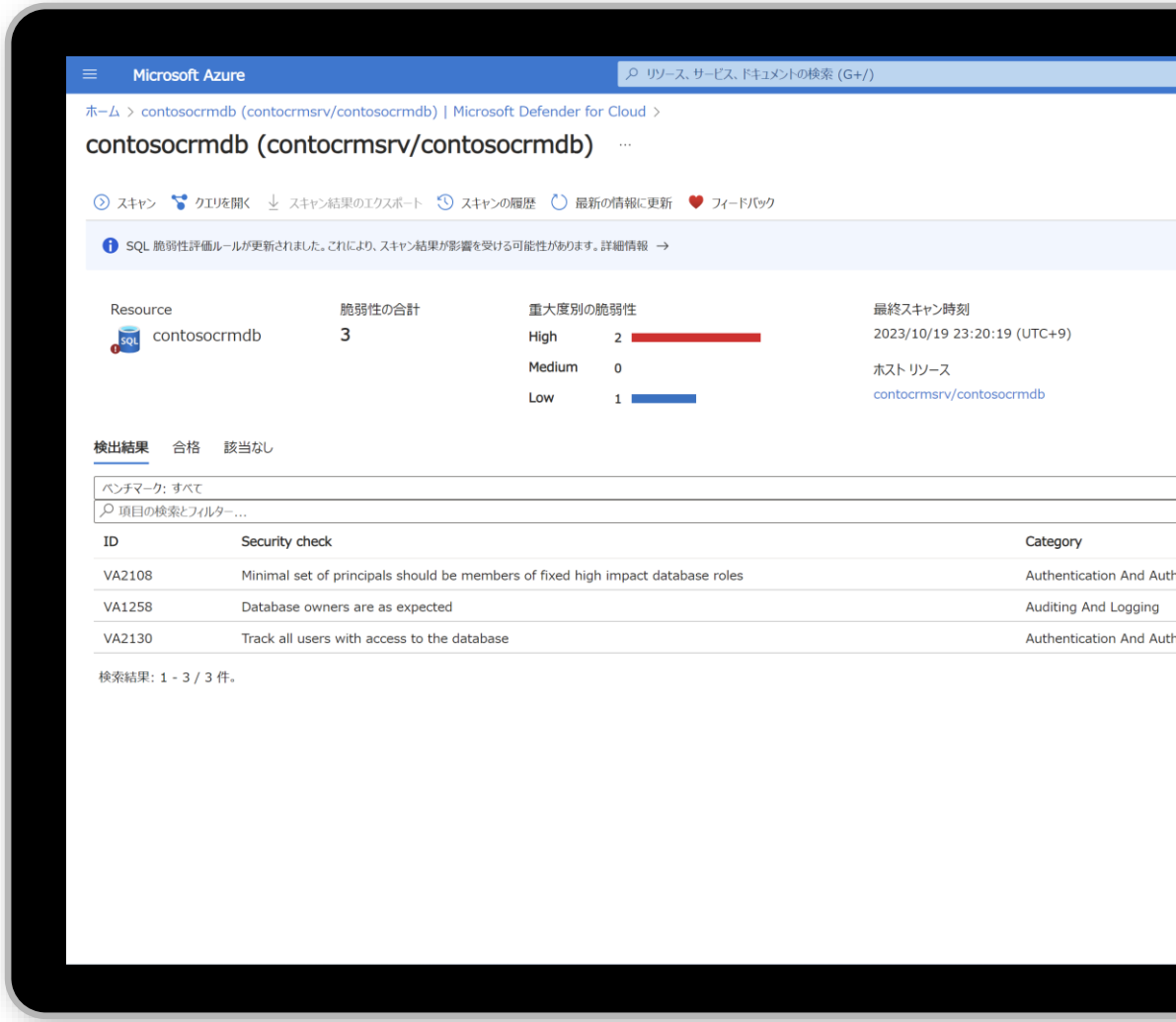
- データベースの「**脆弱性**」と「**脅威**」を検出して軽減
- Azure SQL Database と SQL サーバーの両方に対応



Defender for SQL

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



Defender for SQL

SQLデータベースに対する脅威検出

クエリ分析

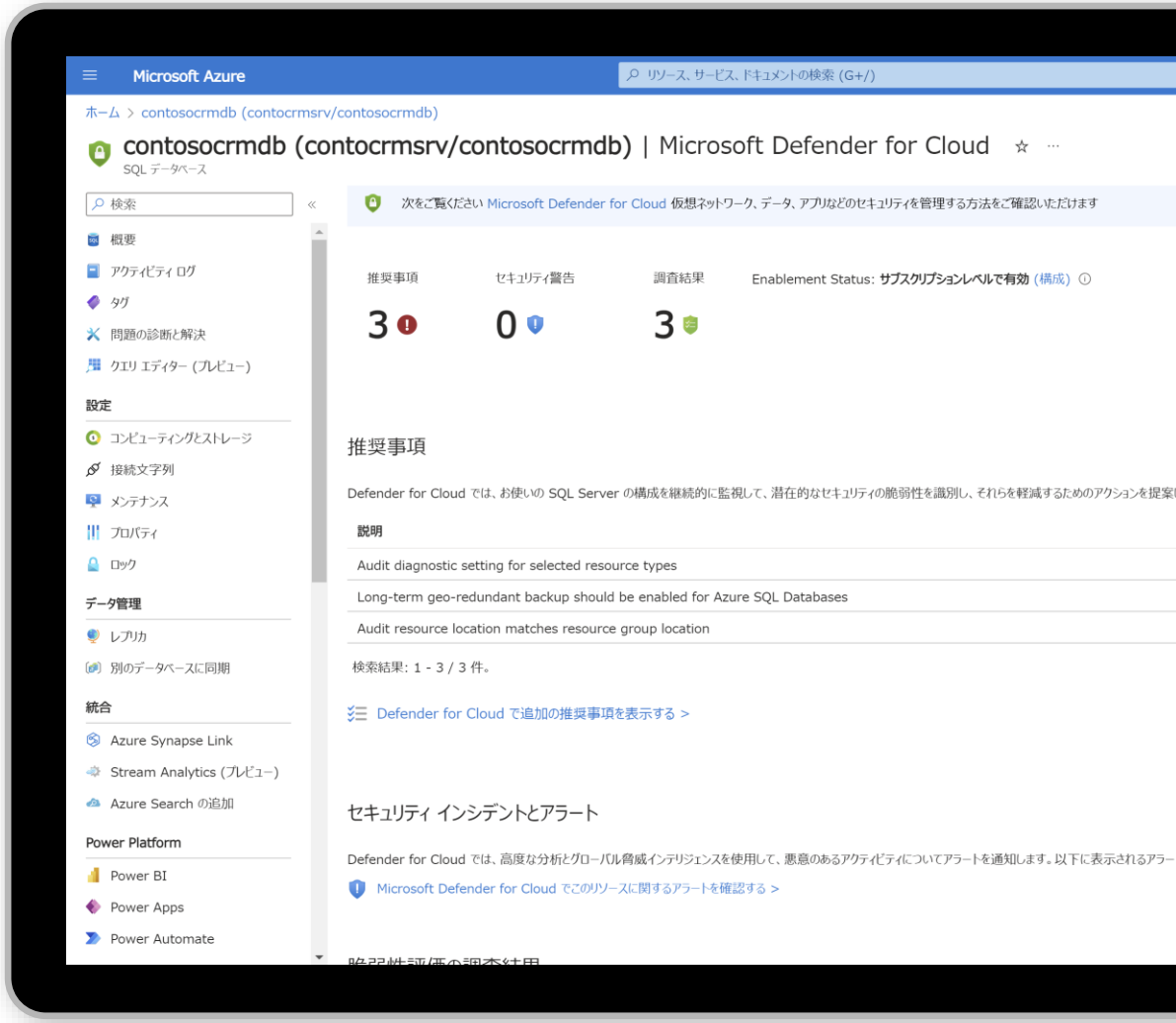
- SQL インジェクションの可能性
- SQL インジェクションに対する脆弱性
- 異常な量の データ抽出
- 普段とは異なるデータ抽出先

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



Microsoft

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