SC-200

補足資料

SC-200 で登場する 主なポータル

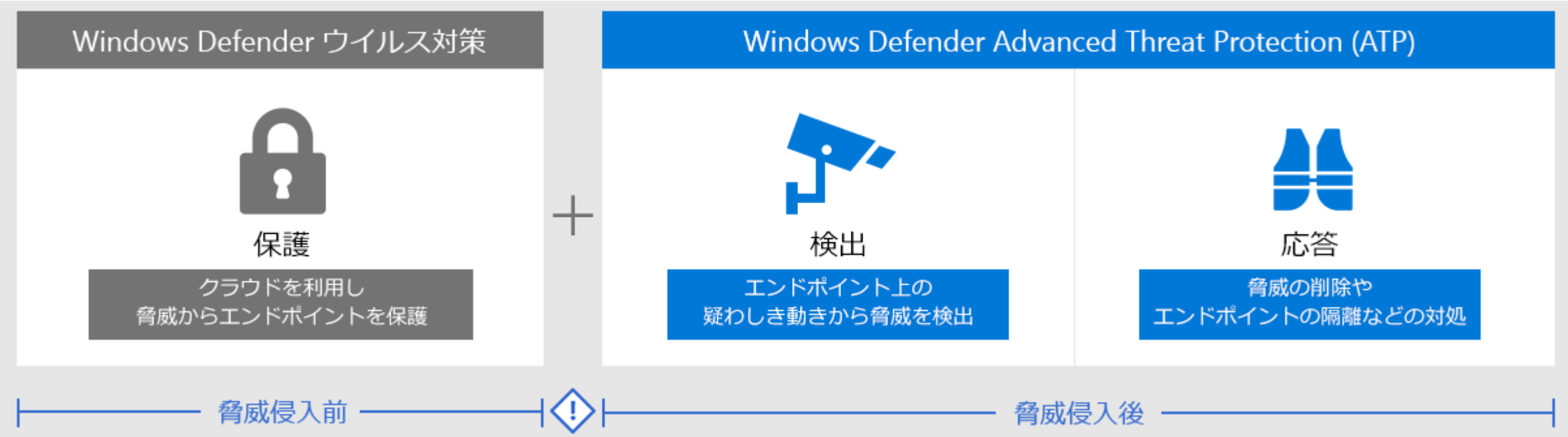
Azure Portal	Microsoft 365 Defender	Microsoft Sentinel
Microsoft Defender for Cloud	Microsoft Defender for Endpoint	
	Microsoft Defender for Office 365	
	Microsoft Defender for Cloud Apps	
	Microsoft Defender for Identity	

Microsoft 365 Defender の整理

Windows 端末	Microsoft Defender for Endpoint	エンドポイントの保護
Microsoft ID	Microsoft Defender for Identity	IDの保護
Office 365	Microsoft Defender for Office 365	E-mailの保護
Cloud App	Microsoft Defender for Cloud Apps	クラウドアプリの保護

Microsoft Defender for Endpoint 4

- エンドポイント上の高度な脅威を検出、調査、対応することを可能にするセキュリティ機能
- Windows Defender Advanced Threat Protection (ATP) から名称変更

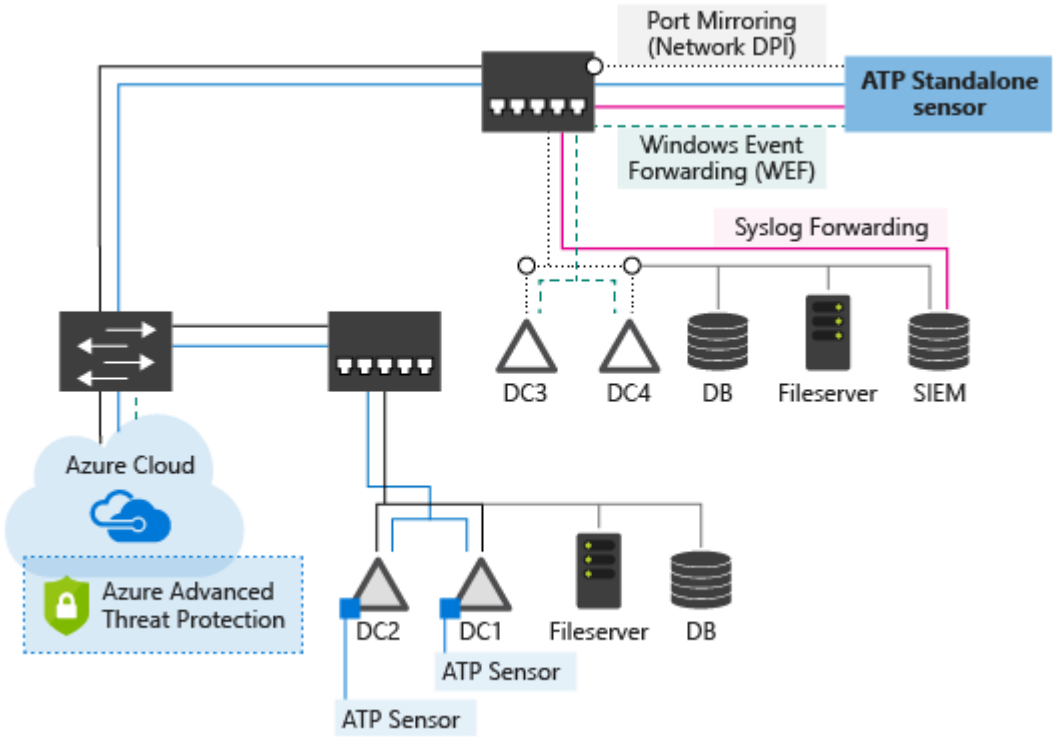


Microsoft Defender for Identity

- 複数の種類の高度な対象となるサイバー攻撃や内部の脅威から、エンタープライズのハイブリッド環境を保護するためのクラウド サービス
- サイバーキルチェーンの複数のフェーズ（偵察、感染活動、目的の実行 <ドメインの支配> ）に重点を置いて、複数の不審なアクティビティを検出

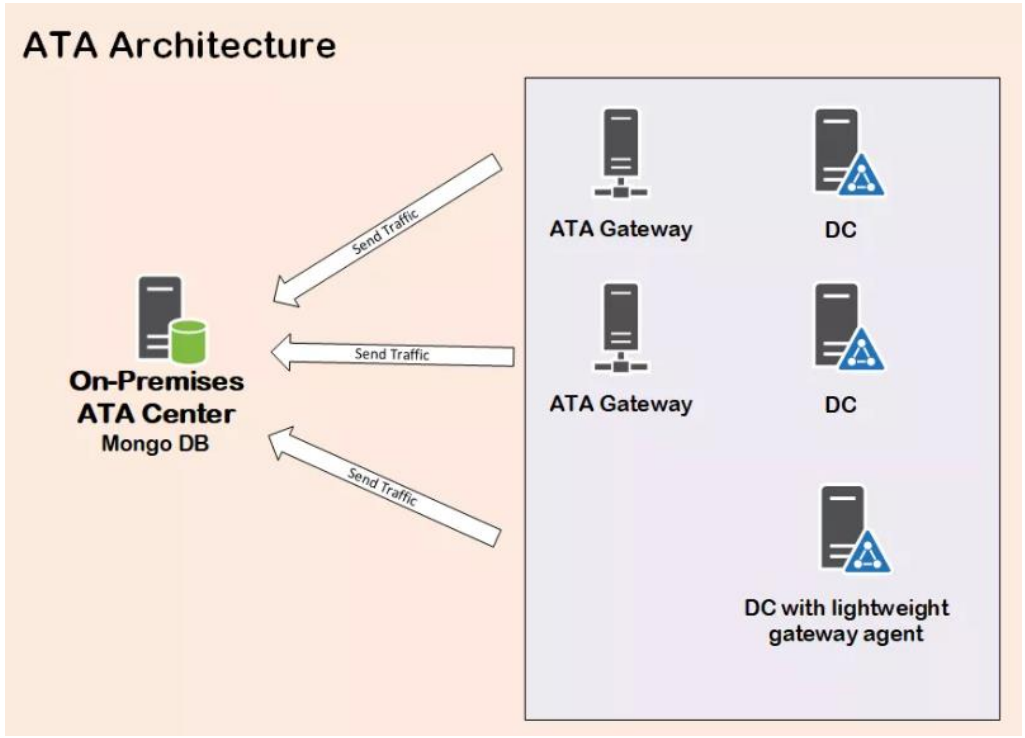
悪意のある攻撃、異常な動作、セキュリティの問題とリスクの主な種類の攻撃を検出

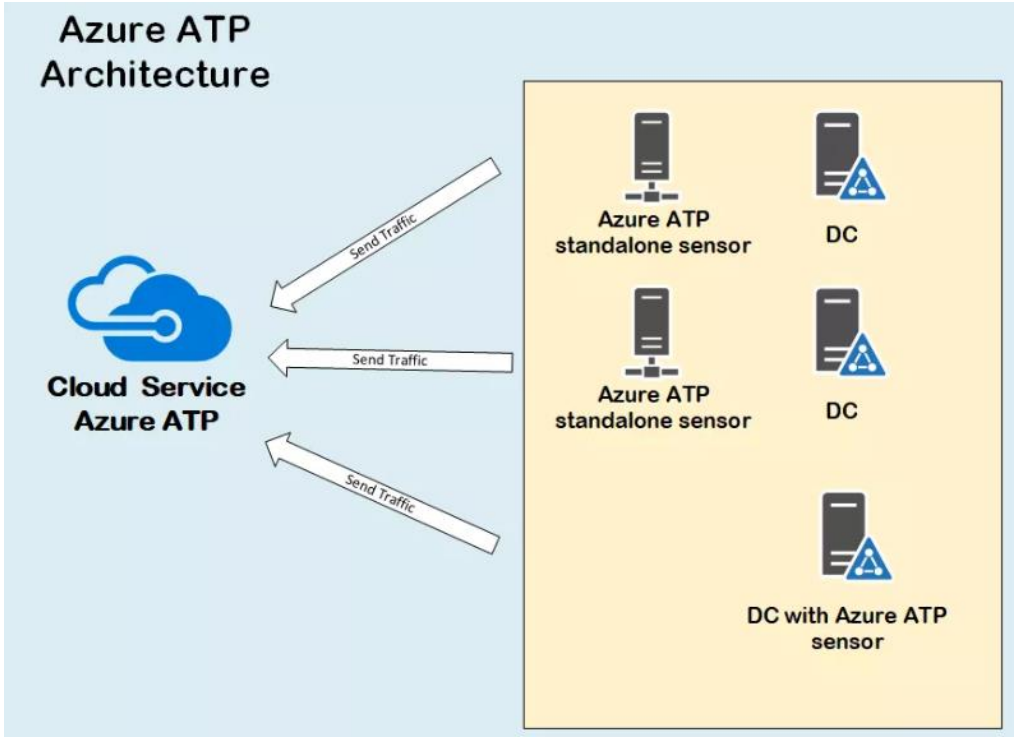
- ✓ Pass-the-Ticket (PtT)
- ✓ Pass-the-Hash (PtH)
- ✓ Overpass-the-Hash
- ✓ 偽造 PAC (MS14 068)
- ✓ ゴールデン チケット
- ✓ 悪意のあるレプリケーション
- ✓ ディレクトリ サービス列挙
- ✓ SMB セッション列挙
- ✓ DNS 偵察
- ✓ 水平ブルート フォース
- ✓ 垂直ブルート フォース
- ✓ スケルトン キー
- ✓ 不自然なプロトコル
- ✓ 暗号化のダウングレード
- ✓ リモート実行
- ✓ 悪意のあるサービスの作成



（参考）Microsoft advanced threat analytics

- Microsoftの高度な脅威分析 （ ATAとも呼ばれていた）のクラウドベースソリューションが Azure ATP（Microsoft Defender for Identityへ名称変更）
  - オンプレミスドメインコントローラからデータを収集でき、Office 365およびWindowsの他のATP製品と統合されていないオンプレミスソリューション
  - IDの異常と横方向（感染活動）の動きを検出する





Defender for Office 365セキュリティの概要

3 つの主なセキュリティ サービス

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365 プラン 1 (Defender for Office P1)
- Microsoft Defender for Office 365 プラン 2 (Defender for Office P2)

Microsoftのセキュリティ体制

- Protect/Detect（脅威の防止と検出）
- Respond（調査、対応）

に機能を分類できる

Exchange Online Protection (EOP)

防止・検出	調査	対応
提供されるテクノロジ: • スパム • フィッシング • マルウェア • バルク メール • スプーフィング インテリジェンス • 偽装の検出 • 管理者検疫 • 管理者とユーザーによる誤検知と検出漏れの報告 • URL およびファイルの許可/禁止 • レポート	• 監査ログ検索 • メッセージ追跡	• ゼロ時間自動削除 (ZAP) • 許可リストと禁止リストの絞り込みとテスト

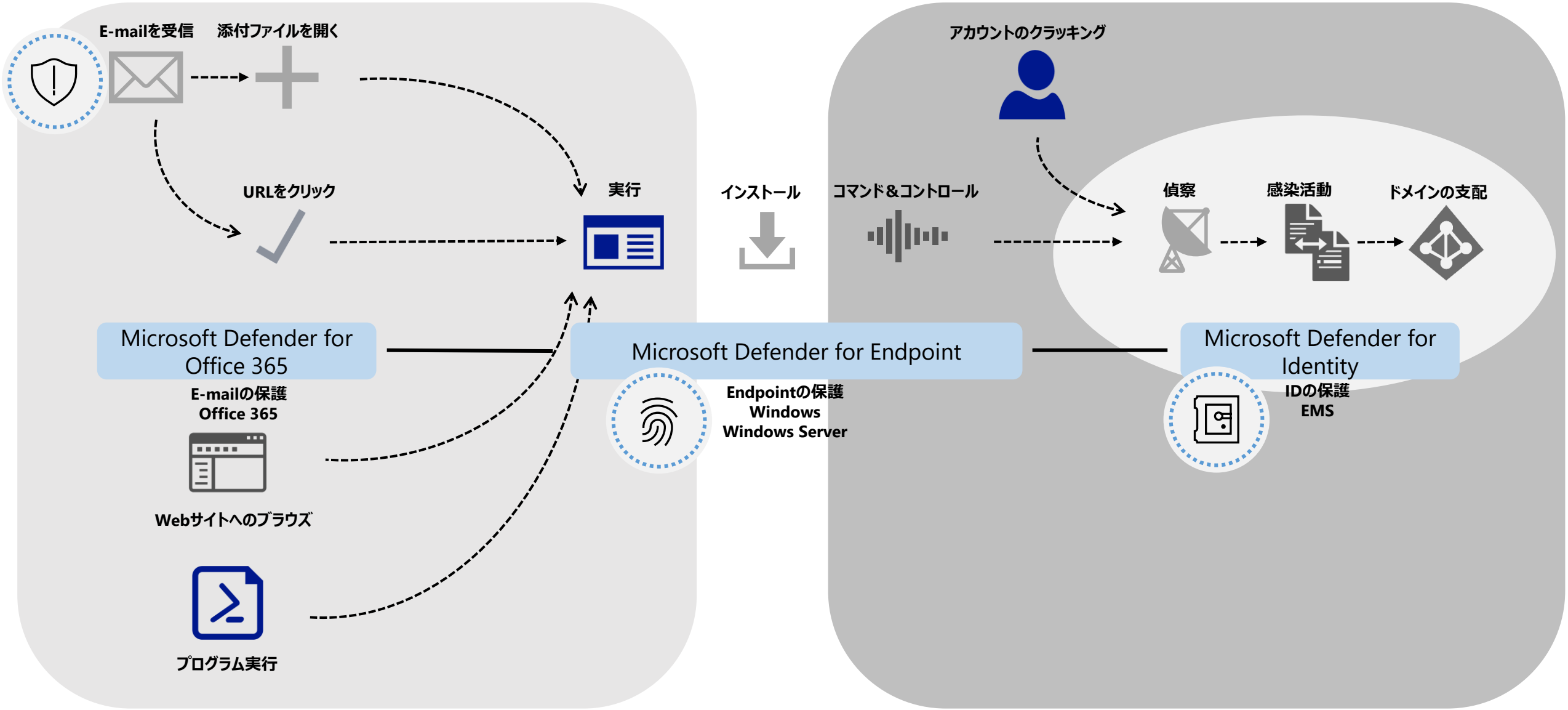
Defender for Office 365 プラン 1

防止・検出	調査	対応
EOP に含まれるすべてのテクノロジに加えて: • 安全な添付ファイル • 安全なリンク • Microsoft Defender for Office 365 によるワークロードの保護 (例: SharePoint Online、Teams、OneDrive for Business) • メール、Office クライアント、Teams でのクリック時の保護 • Microsoft Defender for Office 365 のフィッシング詐欺対策 • ユーザーの偽装とドメインの偽装の保護 • アラートおよびアラート用 SIEM 統合 API	• 検出用 SIEM 統合 API • **リアルタイム検出ツール** • URL 追跡	• 同上

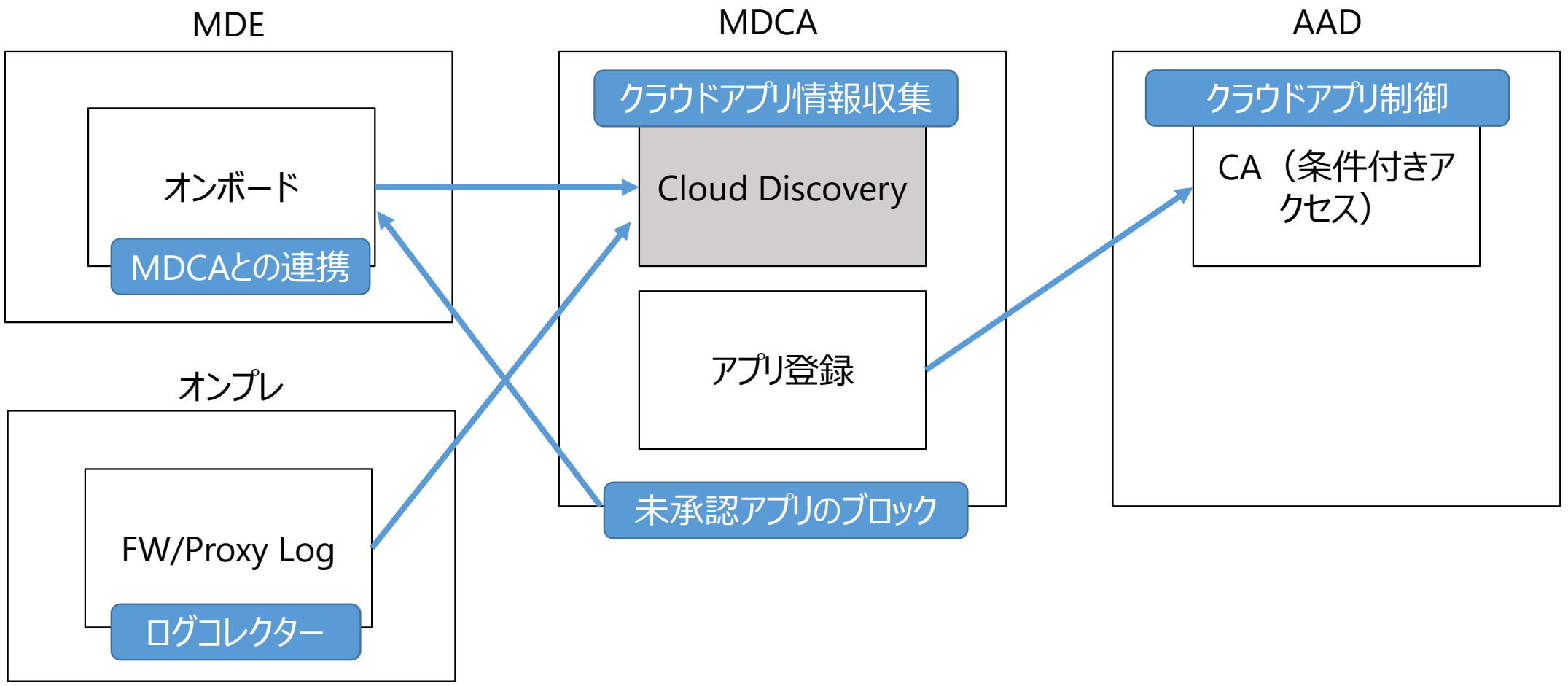
Defender for Office 365 プラン 2

防止・検出	調査	対応
EOP および Microsoft Defender for Office 365 P1に含まれるすべてのテクノロジに加えて: • 同上	• **脅威エクスプローラー** • 脅威トラッカー • キャンペーン ビュー	• 自動調査と応答 (AIR) • 脅威エクスプローラーからの AIR • 侵害されたユーザーの AIR • 自動調査用 SIEM 統合 API

攻撃段階全体を通して検出範囲を最大限にする



Microsoft Defender for Cloud Apps



情報保護のライフサイクル

Discover(検出)

機密情報タイプを定義し、機密情報が含まれていないか**自動的に検出**

Classify(分類)

分類とラベル付け

Protection (保護)

特定のラベルがついたドキュメントに対して、**任意の保護レベル**(ドキュメントの暗号化やドキュメントへのアクセス権の制限のほか、視覚的なマーキングの適用、ユーザーへのポリシー通知など)を設定

Monitor (監視)

保護された機密情報を監視する。機密情報をどのように使用・共有しているかを可視化し、ファイルが不適切に共有されたときはアクセス権を取り消すなど、どんな緊急の問題にも対処して修復できるような機能を提供

Microsoft Information Protection

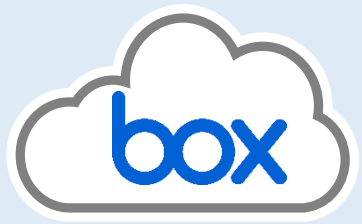
Windows Information Protection

Windows PC

Azure Information Protection

File 共有

Microsoft Defender for Cloud Apps

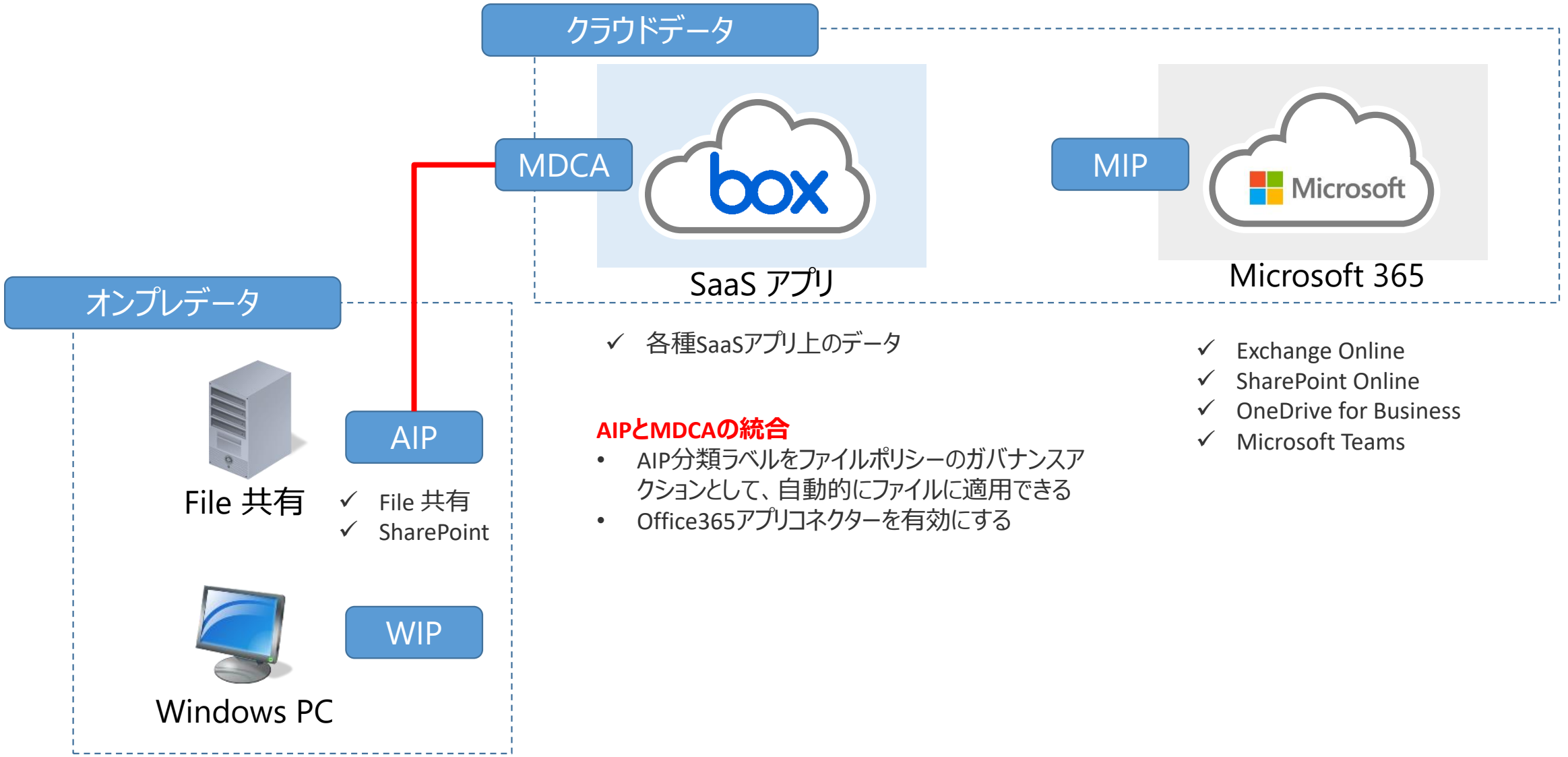


SaaS アプリ

Microsoft 365 Information Protection

Microsoft 365

MIP



- ✓ 各種SaaSアプリ上のデータ

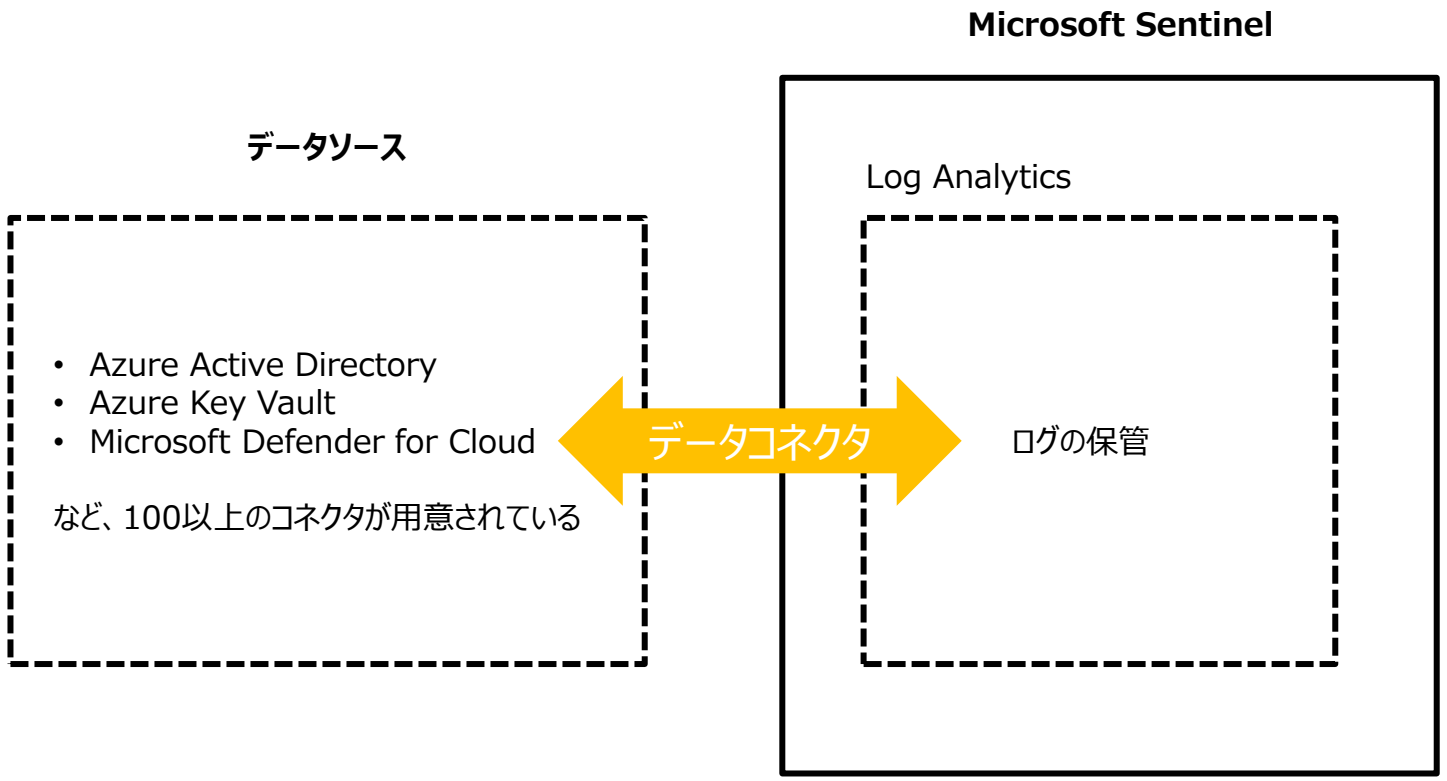
AIPとMDCAの統合

- AIP分類ラベルをファイルポリシーのガバナンスアクションとして、自動的にファイルに適用できる
- Office365アプリコネクターを有効にする

- ✓ File 共有
- ✓ SharePoint

- ✓ Exchange Online
- ✓ SharePoint Online
- ✓ OneDrive for Business
- ✓ Microsoft Teams

Microsoft Sentinel の整理



- **データ収集**
  - メニューとしてはデータコネクタ
  - AADやアクティビティログなどAzureだけではなく、イベントログなどOSのログからPalo等のNW機器など様々なデータソースからLog Analyticsにデータ収集する
- **検知**
  - メニューとしては分析
  - 収集データに対してクエリ(デフォルトで準備されているのもあります。)を実行し合致するイベントがあった時にアラートを作成する
- **調査**
  - メニューとしてはインシデント
  - 影響範囲を特定する
- **対処**
  - メニューとしてはオートメーション(プレイブック)
  - Logic Appで構成され検知したアラートに対しての処理を行う

MITRE ATT&CKフレームワーク

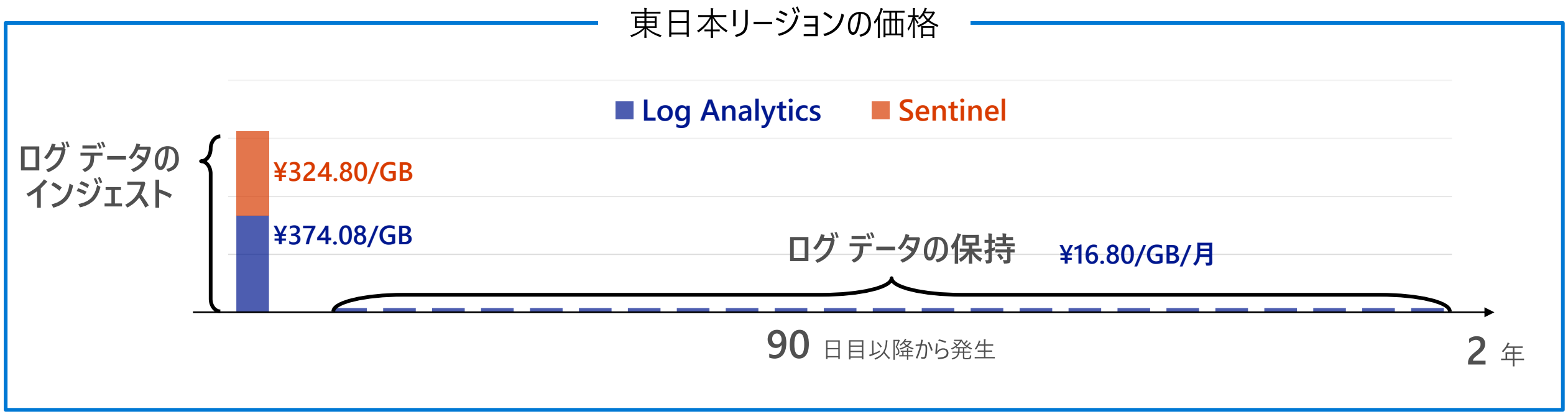
攻撃手法		概要
Initial Access	初期アクセス	攻撃者がネットワークに侵入しようとしている
Execution	実行	攻撃者が悪意のあるコードを実行しようとしている
Persistence	永続化	攻撃者が不正アクセスする環境を確保しようとしている
Privilege escalation	権限昇格	攻撃者がより高いレベルでの権限を取得しようとしている
Defense Evasion	防衛回避	攻撃者が検知されないようにしている
Credential Access	認証情報アクセス	攻撃者がアカウント名とパスワードを盗もうとしている
Discovery	探索	攻撃者がアクセス先の環境を理解しようとしている
Lateral Movement	水平展開	攻撃者がアクセス先の環境を移動しようとしている
Collection	収集	攻撃者が関心のあるデータを収集しようとしている。
Command and control	C&C	攻撃者が侵害されたシステムと通信し制御しようとしている
Exfiltration	持ち出し	攻撃者が情報を持ち出そうとしている
Impact	影響	攻撃者がシステムとデータを操作、中断、破壊しようとしている

攻撃が成功に向かって大きく変化するポイント

実害が発生するポイント

Microsoft Sentinel 価格

Microsoft Sentinel の課金は、
ログ データのインジェスト (Log Analytics + Sentinel)
ログ データの保持 (90 日目以降から、Log Analytics のみ)
の 2 段階課金



ログデータのインジェスト費用が無料のデータソース

	テーブル名	必要な権限
Office 365	OfficeActivity 無償	全体管理者 セキュリティ管理者
Azure AD	SigninLogs AuditLogs	全体管理者 セキュリティ管理者
Microsoft 365 Defender		全体管理者 セキュリティ管理者
Microsoft Defender for Endpoint の生ログ	DeviceInfo DeviceNetworkInfo DeviceProcessEvents DeviceNetworkEvents DeviceFileEvents DeviceRegistryEvents DeviceLogonEvents DeviceImageLoadEvents DeviceEvents DeviceFileCertificateInfo	
Microsoft Defender for Office 365 の生ログ	EmailEvents EmailUrlinfo EmailAttachmentInfo EmailPostDeliveryEvents	
Microsoft Defender for Identity の生ログ *DCへのログオンイベント *DNS クエリ等	Coming Soon	
Microsoft Cloud App Security の生ログ *接続アプリのイベント *接続アプリのファイルイベント	Coming Soon	
Microsoft Defender for Office 365	SecurityAlert 無償	全体管理者 セキュリティ管理者
Microsoft Defender for Endpoint	SecurityAlert 無償	全体管理者 セキュリティ管理者
Azure AD Identity Protection	SecurityAlert 無償	全体管理者 セキュリティ管理者
Microsoft Defender for Identity	SecurityAlert 無償	全体管理者 セキュリティ管理者
Microsoft Defender for Cloud App	SecurityAlert 無償 McasShadowItReporting	全体管理者 セキュリティ管理者
Azure Information Protection	SecurityAlert 無償 InformationProtectionLogs_CL	全体管理者 セキュリティ管理者 Azure Information Protection管理者

無料データソース https://docs.microsoft.com/ja-jp/azure/sentinel/azure-sentinel-billing#free-data-sources