# MicrosoftDefender について

SB C&S株式会社
ICT事業本部 ｸﾗｳﾄﾞ・ｿﾌﾄｳｪｱ推進本部
ｸﾗｳﾄﾞﾌﾟﾗｯﾄﾌｫｰﾑ推進統括部
ｸﾗｳﾄﾞﾌﾟﾗｯﾄﾌｫｰﾑﾏｰｹﾃｨﾝｸﾞ部 販売推進課

SB C&S

# Microsoft Defenderとは？

SB C&S

以前のDefender はアンチウィルスを目的とした製品でしたが、

現在はMicrosoftの提供するセキュリティ製品のシリーズ名となりました

以下の製品はWindowsの標準機能として搭載されています。
- Microsoft Defender AntiVirus
- Microsoft Defender FireWall
- Microsoft Defender SmartScreen
- Microsoft Defender Application Guard
- ※Microsoft Defender DeviceGuard
- ※Microsoft Defender Credential Guard

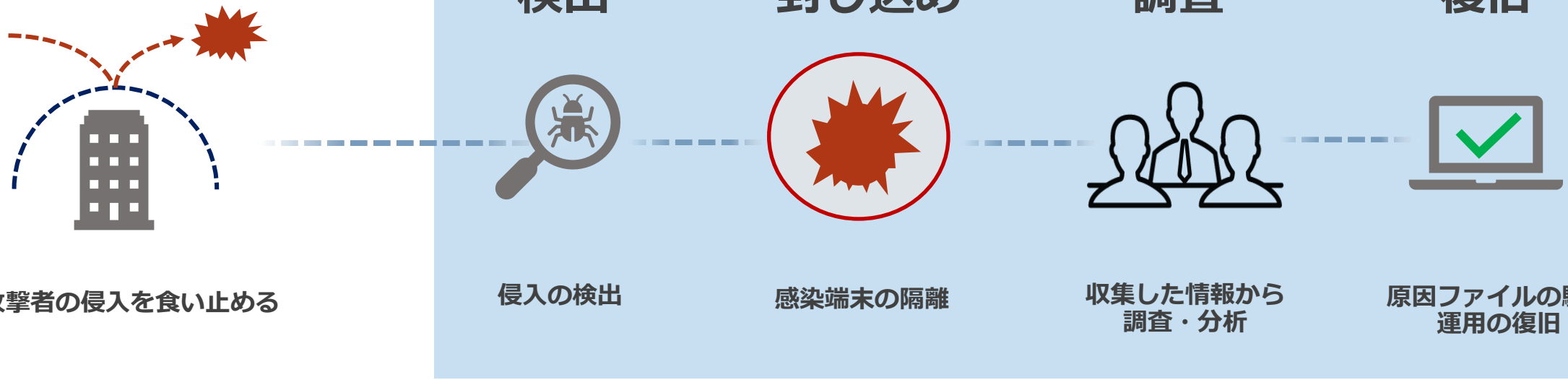
※：※Windows Enterprise/Educationのみ利用可

以下の製品は有償ライセンスが必要です、本資料ではこちらについてご紹介します。
- Microsoft Defender For Endpoint(Plan1,Plan2)
- Microsoft Defender For Business(Server)
- Microsoft Defender Fot Cloud Server
- Microsoft Defender For Office365(Plan1,Plan2)
- Microsoft Defender For Cloud Apps
- Microsoft Defender For Identity

# エンドポイントセキュリティ(EDR)
# For Endpoint/Business

# 境界型ウィルス対策とEDR

SB C&S




これまでの対策

これからの対策

**FW/UTM/EPP/NGAVなど**
-侵入そのものを防御する-

**EDR(Endpoint Detection and Response)**
-侵入後の動きを可視化して対処する-

**脅威の侵入防御**

**侵入後の検出/調査/対応/回復を提供**

**攻撃は100%防げないことを前提に侵入後対策を考える**

# Microsoft Defender ForEndpoint/ Business

SB C&S

## EDR機能を含んだ、クラウドベースの エンドポイントセキュリティの統合プラットフォーム

- 場所を選ばず24/365で端末を監視・保護
- クロスプラットフォーム対応
- インシデントの検出～修復までを一元対応
- 他のDefenderとの連携によるゼロトラストアプローチ

# Microsoft製EDRの特徴

SB C&S

## エンドポイント アクティビティを監視し、あらゆる種類の悪意ある攻撃を特定

### フルクラウド管理

クラウド管理でインフラ構築不要
Win OSでは標準組み込みの
動作センサーで詳細なログを記録

### 業界をリードする
### 脅威インテリジェンス

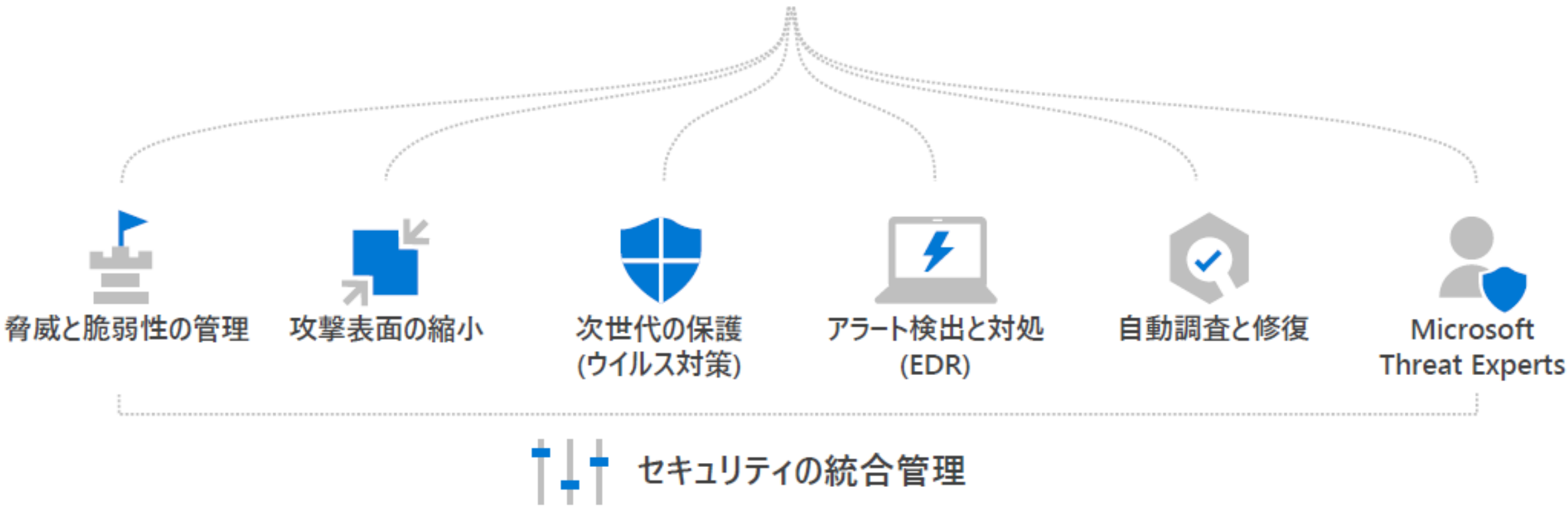
ビッグデータ・機械学習などを駆使したMSの分析力でリアルタイムの可視性を提供

### 自動化されたセキュリティ

自動検知・修復により管理者の手を煩わすことなく
アラートから数分で対応

# Microsoft Defender for Endpoint

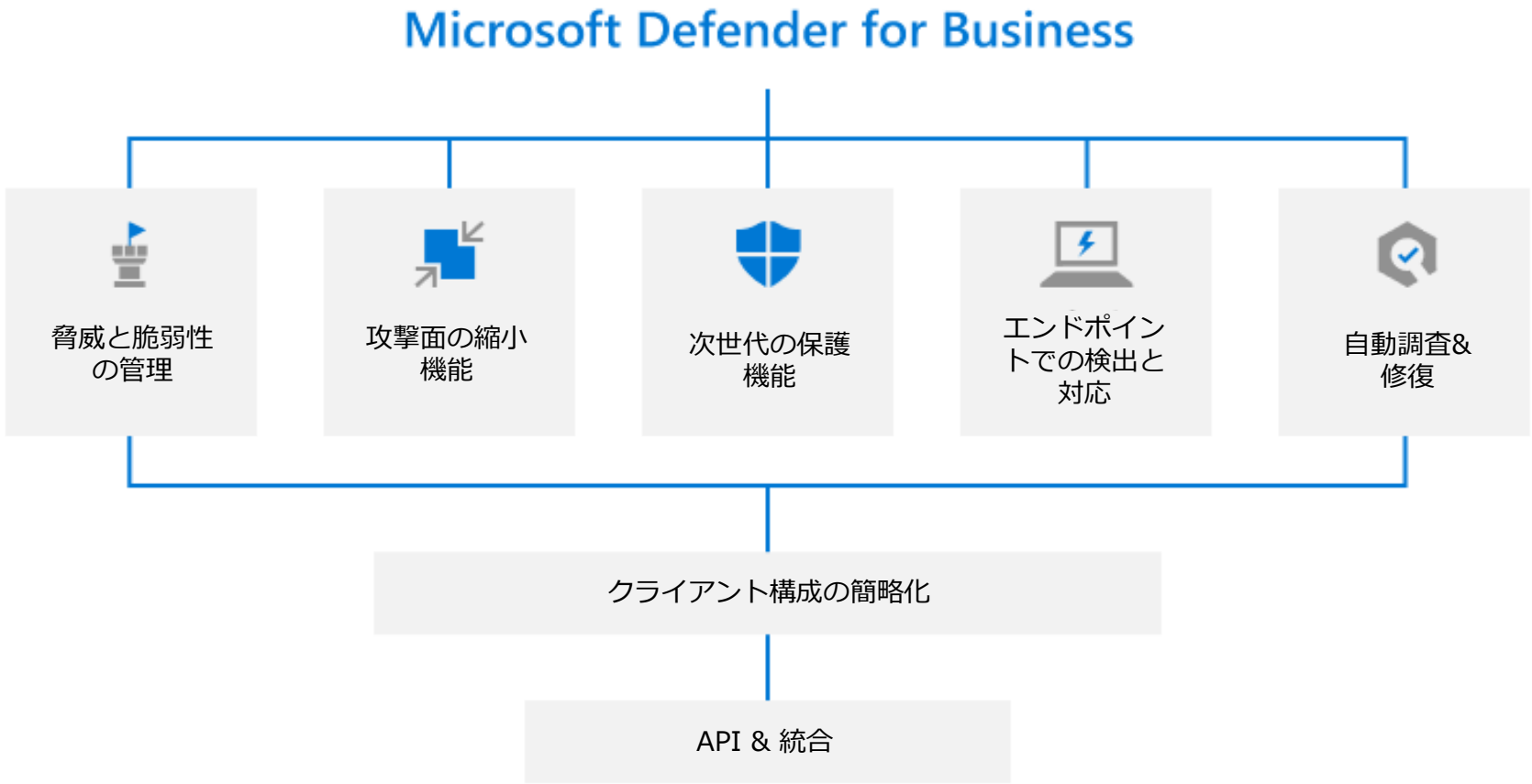
**Built-in. Cloud-powered.**



# Microsoft Defender for Business

SB C&S

2022年3月1日から提供された「Microsoft Defender for Business」は300名以下の一般法人向けの新しいエンドポイントセキュリティソリューション
ランサムウェア、マルウェア、フィッシング、その他の脅威から企業のデバイスを保護



# EDR製品・機能比較

SB C&S

## Defender for BusinessとDefender for Endpointの比較

| 機　　能 | Defender for Business | Defender for Endpoint Plan1 | Defender for Endpoint Plan2 |
|---|---|---|---|
| 集中管理 | ○ | ○ | ○ |
| クライアント構成の簡略化 | ○ | × | × |
| 脅威と脆弱性の管理 | ○ | × | ○ |
| 攻撃面の縮小機能 | ○ | ○ | ○ |
| 次世代の保護 | ○ | ○ | ○ |
| エンドポイントでの検出と対応 | ○ | × | ○ |
| 自動調査および対応 | ○ | × | ○ |
| 脅威の捜索と6か月間のデータ保持 | × | × | ○ |
| 脅威分析 | ○ | × | ○ |
| クロスプラットフォームサポート<br>(Windows、macOS、iOS、Android OS) | ○ | ○ | ○ |
| Microsoft 脅威エキスパート | × | × | ○ |
| パートナー API | ○ | ○ | ○ |
| Microsoft 365 Lighthouse統合<br>(顧客テナント間のセキュリティインシデントを表示する場合) | ○ | × | × |

# メールセキュリティ
# Defender For Office365

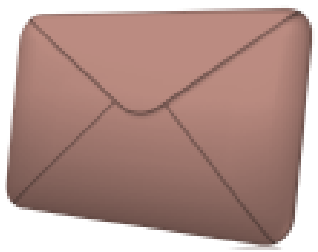
# Microsoft365のメールセキュリティ

SB C&S

## Microsoft Defender for Office 365

怪しいURL(リンク)

怪しい添付ファイル



Exchange Online Protection
（標準機能）

- アンチスパム
- アンチウィルス
- DKIM DMARC

Microsoft Defender for Office 365

- 安全なリンク チェック
- 安全な添付 チェック

身代わりチェック

正常なURLへ変更/削除

怪しい添付ファイル削除

# Defender For Office365 比較

SB C&S

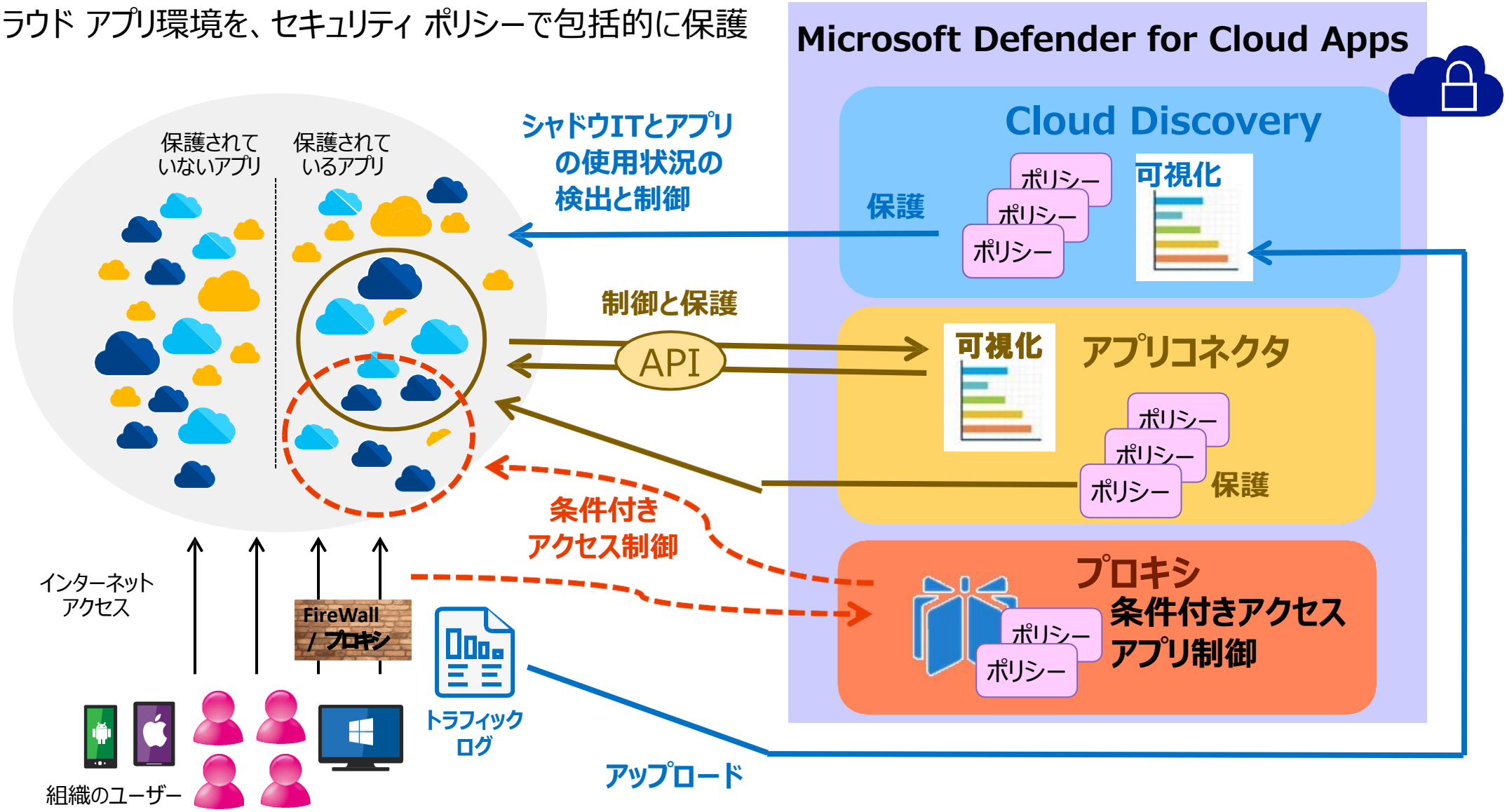
| 機　　能 | Defender for Office365 Plan1 | Defender for Office365 Plan2 |
|---|---|---|
| メール添付ファイルチェック | ● | ● |
| Teams添付ファイルチェック | ● | ● |
| メール内URL(リンク)チェック | ● | ● |
| Teams内URL(リンク)チェック | ● | ● |
| Sharepoint/Onedrive上のファイル保護 | ● | ● |
| 脅威調査 | リアルタイムスキャンのみ | 過去ログ調査可能 |
| フィッシングURLの対策ポリシー | ● | ● |
| リアルタイムレポート | ● | ● |
| 脅威トラッカー | × | ● |
| 自動調査 | × | ● |
| 攻撃シュミレーション | × | ● |
| Microsoft Defenderとの統合 | × | ● |

# クラウドアプリのセキュリティ
# Defender For Cloudapps

# Microsoft Defender for Cloud Apps

SB C&S

- 組織のクラウド アプリ環境を、セキュリティ ポリシーで包括的に保護



# Cloud Access Security Broker（CASB）

SB C&S

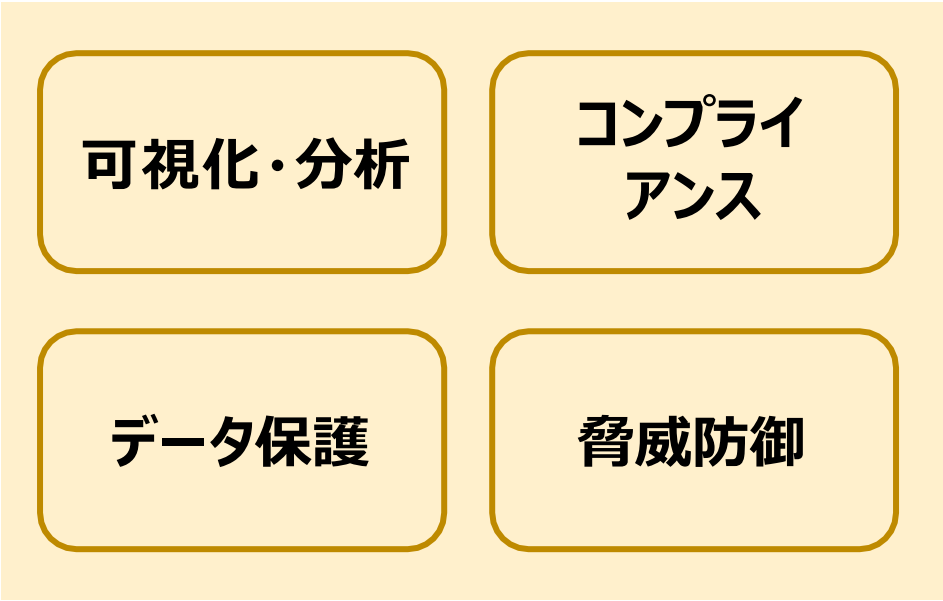
## Cloud Access Security Broker（CASB）とは

「ユーザー（企業）と複数のクラウドプロバイダー間に単一のコントロールポイントを設けて、クラウドサービスの利用状況を可視化/制御することで、一貫性のあるセキュリティポリシーを適用する」というコンセプト

- ガートナーが2012年に提唱
- クラウドの普及に伴い、急成長している分野

Microsoft Defender for Cloud Appsは、
マイクロソフトの CASB

＜CASBの大きな4つの機能＞



# Cloud Discovery機能

- 組織ネットワーク内のユーザーが使用している、クラウドアプリの使用状況の視覚化
- 組織が承認しているアプリ/承認していないアプリのタグ付け、シャドウITの検出、
  アクセス元IPアドレスの特定、使用しているユーザーの特定、アラートによる通知、などを行える

## Cloud Discovery

可視化


アプリの承認/
却下のタグ付け

アラート

## アプリコネクタ

可視化


保護

アラート

アプリ内の
コンテンツ
のスキャン

## プロキシ


**アプリの条件付きアクセス制御**

クラウドアプリに対する
リアルタイムなアクセス制御

# アプリコネクタ機能

- 特定のアプリにAPIで接続し、アプリから直接情報を取得
- 情報をスキャンして、分析し、ユーザーのアクティビティ、クラウドアプリに格納しているファイルのコンテンツ、ファイルの公開状況、クラウド アプリを使用しているユーザーなどを調査
- ユーザーの停止、非公開にする、管理者検疫、コンテンツの自動分類、管理者へのアラートなどを実行

## Cloud Discovery

可視化


アプリの承認/
却下のタグ付け

アラート

## アプリ コネクタ

可視化


保護

アラート

アプリ内の
コンテンツ
のスキャン

## プロキシ


**アプリの条件付きアクセス制御**

クラウド アプリに対する
リアルタイムなアクセス制御

# プロキシ機能

SB C&S

- Azure ADと統合しているSAMLベースのアプリを対象とし、
  条件付きのアクセス制御を行える

## Cloud Discovery

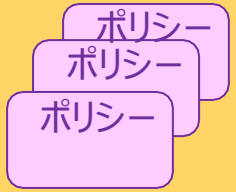
可視化


アプリの承認/
却下のタグ付け

アラート

## アプリコネクタ

可視化




保護

アラート

アプリ内の
コンテンツ
のスキャン

## プロキシ


**アプリの条件付きアクセス制御**

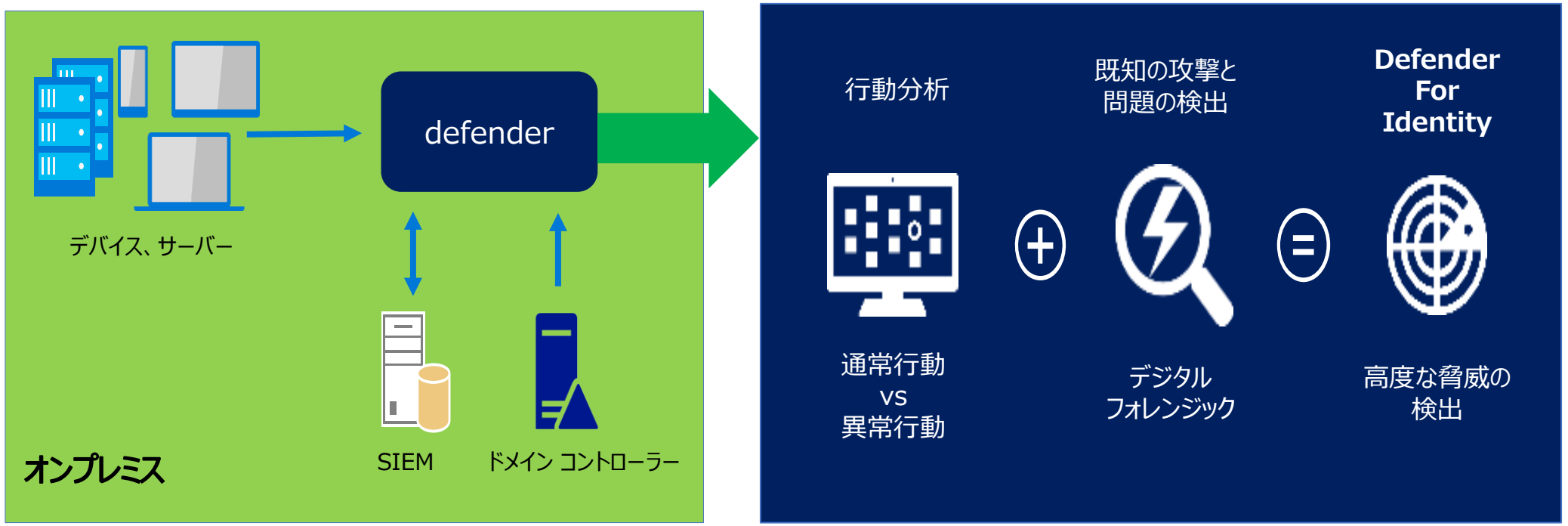
クラウドアプリに対するリアルタイム
なアクセス制御

# オンプレミス環境のセキュリティ
# Defender For Identity

# Defender for Identity

SB C&S

行動分析と機械学習を使用して、ドメイン コントローラーから発信されるトラフィックを監視
いつ、どこから、どのような攻撃が行われたかを、タイムライン（時系列）で可視化できる
ユーザーやデバイスの不審な動作を自動的に分析し、大きな損害の発生を未然に防止する、
オンプレミス環境を監視するソリューション。



ご不明な点がございましたら
お気軽にお問い合わせください。

SB C&S株式会社