Microsoft Security

Microsoft Entra Permissions Management
製品機能概要
(パートナー様向け説明会)

日本マイクロソフト株式会社
テクニカルスペシャリスト
須澤 英彰 CISSP, CEH

Agenda

- Microsoft Entra とは
- Microsoft Zero Trust architecture
- Microsoft Entra Permissions Management (MEPM)
- ライセンス

Microsoft Security

Microsoft Entra

Secure access for a connected world

Microsoft Entra

Secure access for a connected world.

Azure Active Directory

ユーザー、アプリケーション、ワークロード、デバイスを保護

Permissions Management

あらゆるクラウド上のあらゆる ID の権限を管理する
統一されたモデル

Verified ID

業界をリードするグローバルプラットフォームで、
プライバシーを尊重しながら、より安全なインタラクションを可能に

The new brand architecture for Identity aligns to the Security market and product strategy

Microsoft Security

Product categories

Identity	Security	Compliance	Privacy	Management
Microsoft **Entra**	Microsoft **Defender** Microsoft **Sentinel**	Microsoft **Purview**	Microsoft **Priva**	Microsoft **Endpoint Manager**

Product and feature name updates

Products

from	*to*
Azure Active Directory (Azure AD)	Azure Active Directory, part of Microsoft Entra
CloudKnox Permissions Management	Microsoft Entra Permissions Management
Verifiable credentials in Azure Active Directory	Microsoft Entra Verified ID
Azure Active Directory External Identities	Azure Active Directory for External Identities, part of Microsoft Entra
Microsoft Authenticator	Microsoft Entra Authenticator
Microsoft Passwordless	Microsoft Entra Passwordless (for commercial) Microsoft Passwordless (for consumer)

Licensing SKUs

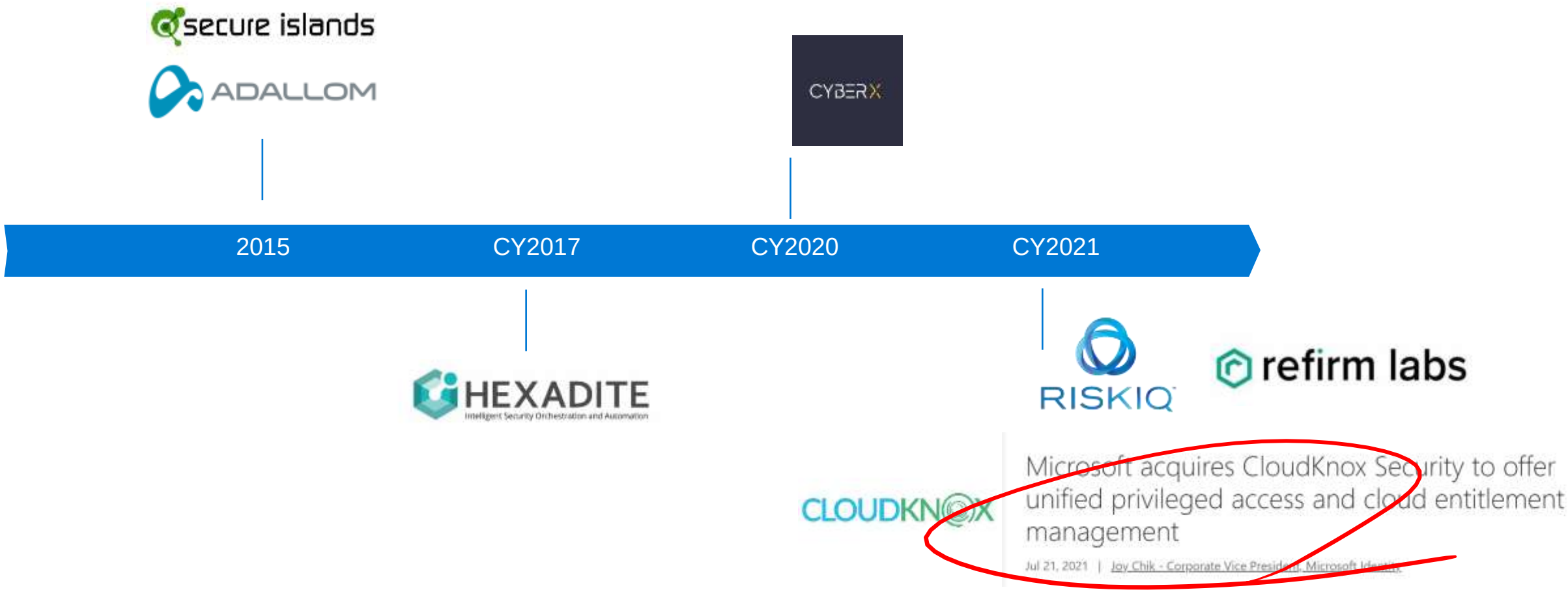
from	*to*
Azure AD Free	*No change*
Azure AD Premium 1	*No change*
Azure AD Premium 2	*No change*
CloudKnox Permissions Management	Permissions Management

Features

from	*to*
Azure AD Conditional Access	*No change*
Azure AD MFA	*No change*
Azure AD Identity Protection	*No change*
Azure AD Identity Governance	*No change*
Azure AD Privileged Identity Management	*No change*
Azure AD Access Reviews	*No change*
Azure AD Entitlement Management	*No change*
Azure AD app gallery	*No change*
Azure AD App Proxy	*No change*
Active Directory Federation Services (AD FS)	*No change*
Azure AD password hash synchronization	*No change*
Azure AD pass-through authentication	*No change*
Azure AD seamless SSO	*No change*
Azure AD Connect	*No change*
Azure AD Connect Health	*No change*
Azure AD Connect sync	*No change*
Azure AD RBAC	*No change*
Azure AD roles	*No change*
Microsoft Identity Platform	*No change*
Microsoft Identity Management (MIM)	*No change*

Microsoft's Investments

CloudKnox Security Inc
設立：2016 年　(Microsoftが 2021年 7 月に買収)
本社：米国カリフォルニア州　サンフランシスコ



Microsoft acquires CloudKnox Security to offer unified privileged access and cloud entitlement management - The Official Microsoft Blog

Microsoft Security

Microsoft Zero Trust architecture

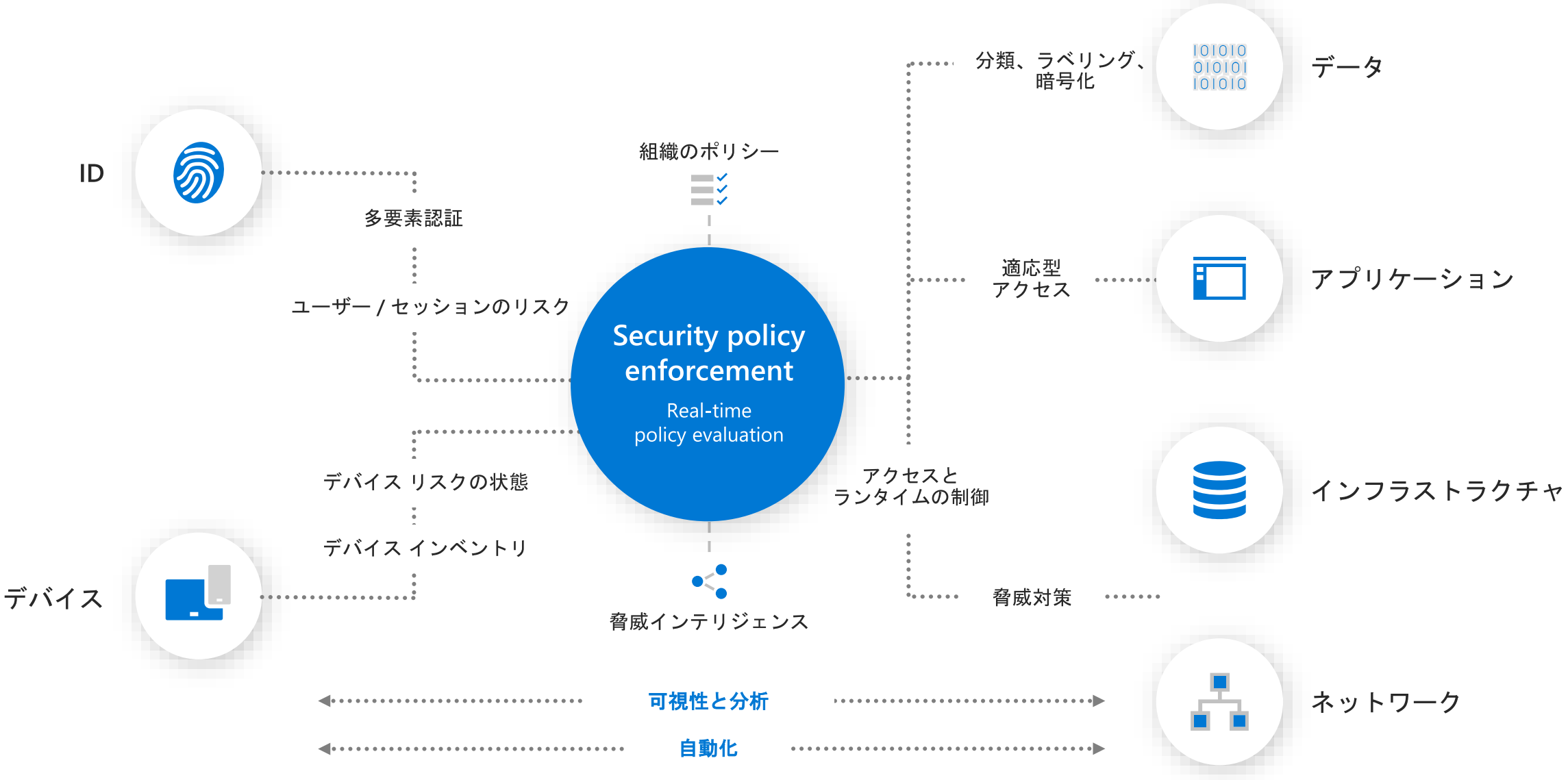
ゼロトラストの原則

明示的に検証する

最小限の
特権アクセスを使用する

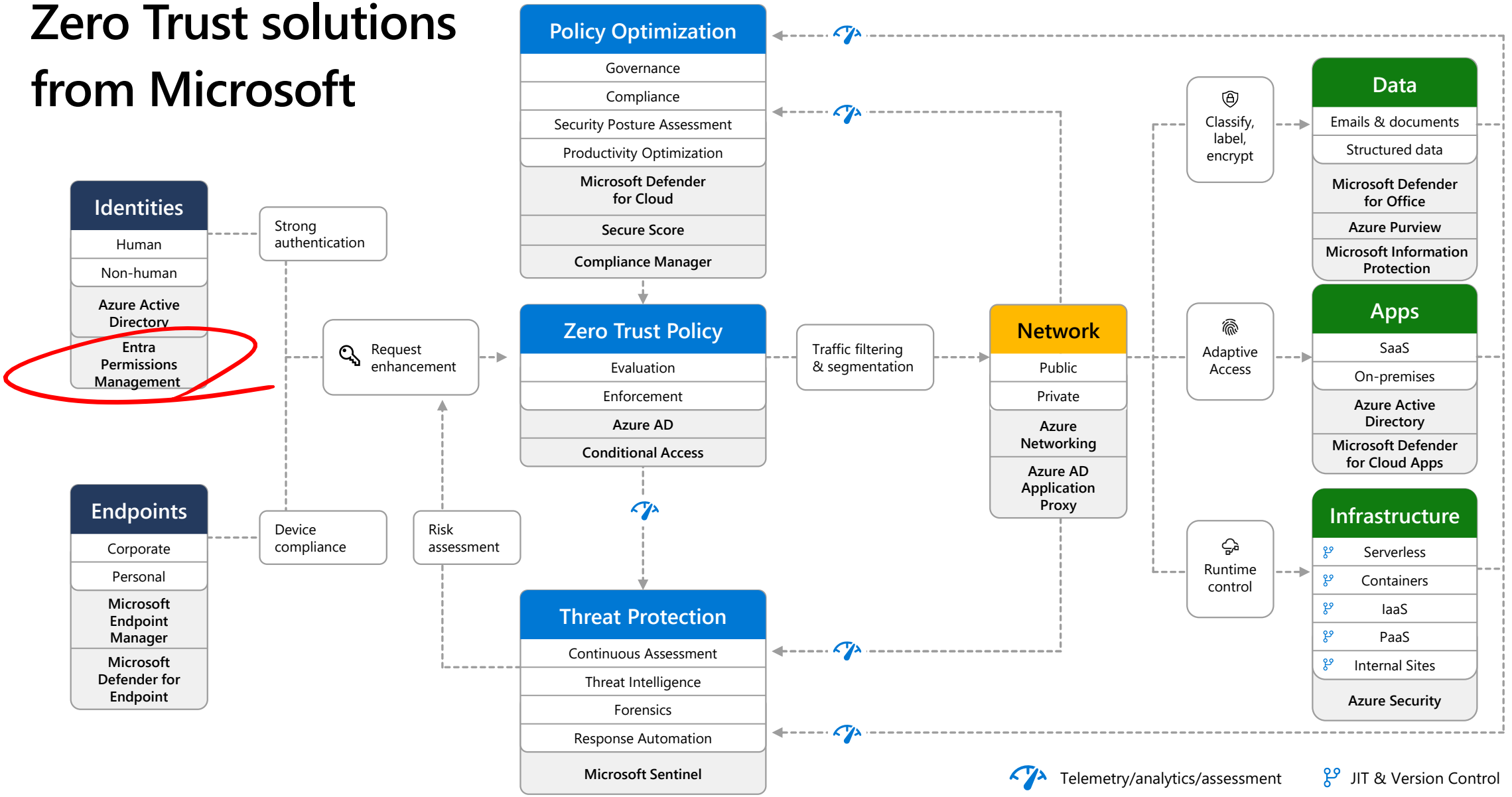
侵害を想定する

Microsoft Zero Trust architecture



Microsoft Security

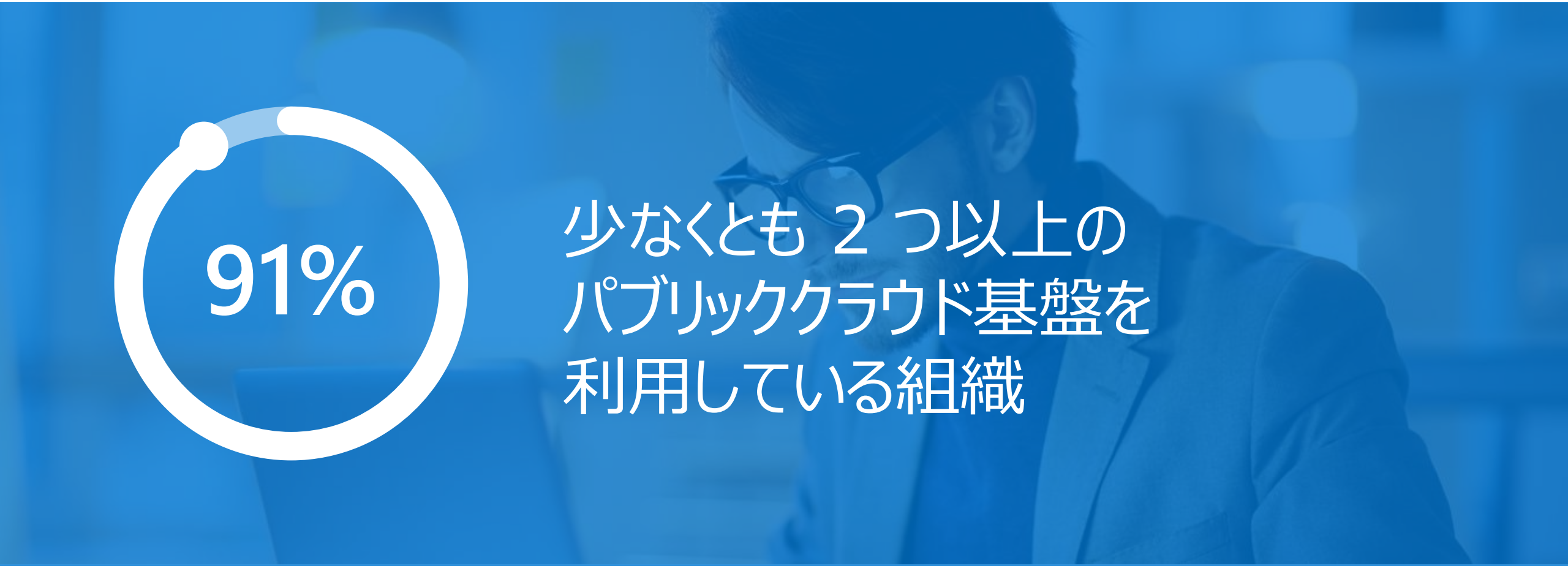
Zero Trust solutions from Microsoft



Microsoft Security

Microsoft Entra Permissions Management (MEPM)

組織ではマルチ クラウドが主流に



Source: internal Microsoft research, 2021

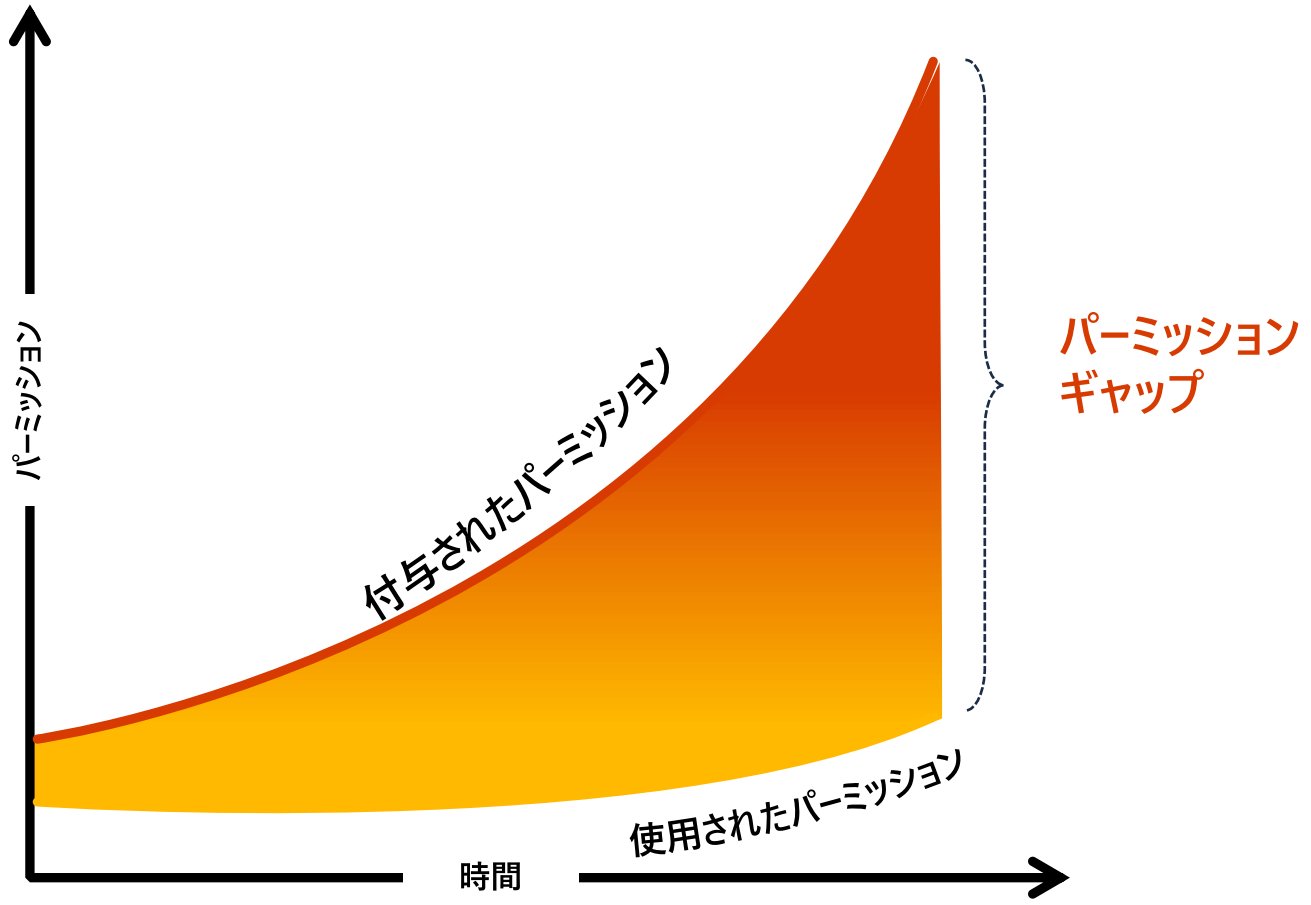
マルチ クラウドの導入により、パーミッションに関する新たな課題が発生

クラウド基盤で動作する ID、マシン、機能、スクリプトの**指数関数的成長**

90% を超える ID が、付与された**パーミッションの 5% 未満**しか使用していない

50% を超えるパーミッションが高リスクであり、壊滅的な損害を引き起こす可能性がある

管理されていないパーミッションによって攻撃面が拡大



ID、パーミッション、リソースに対する**包括的な可視性**の欠如

IAM とセキュリティのチームが、マルチクラウド環境全体でパーミッション管理を行う際の**複雑性が増大**

偶発的または悪意あるパーミッションの誤用による**侵害リスクの増加**

マルチクラウド環境全体でパーミッションを管理するには新たなアプローチが必要

現今の静的で、時代遅れなアプローチ

~~職務上の役割と責任に基づくパーミッションの付与~~

~~IAM 管理者が時間制限のないパーミッションを手動で付与~~

~~パーミッションのクリーンアップは、必要に応じて手動で実行~~

新しい、ダイナミックなアプローチ

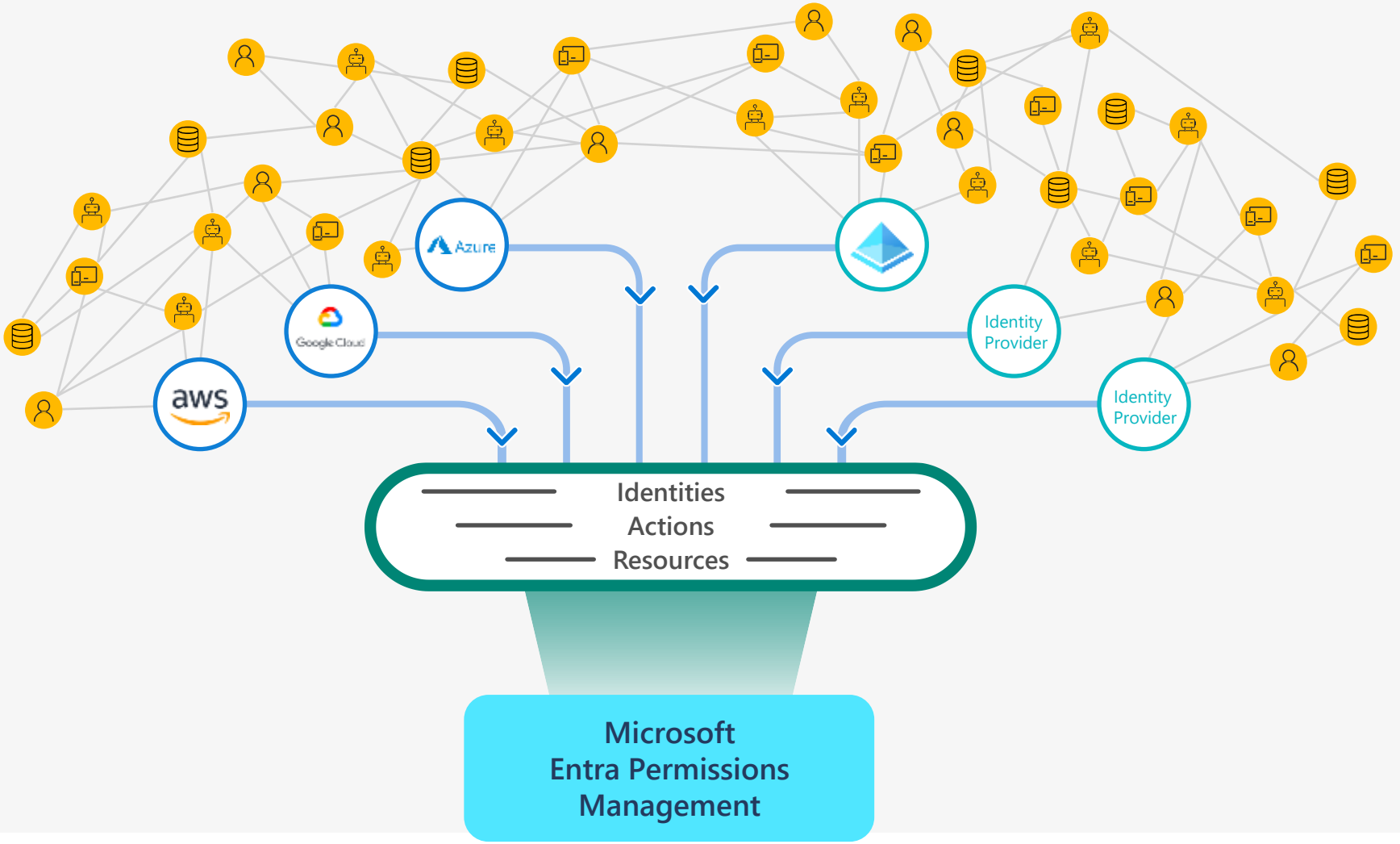
過去の使用状況やアクティビティに基づいたパーミッションの付与

オンデマンドで高リスクのパーミッションに一時的なアクセス許可

適切なサイズの ID を継続的に監視し、権限クリープを防止

Microsoft Entra Permissions Management

過去の使用状況やアクティビティに基づいたパーミッション管理



あらゆるクラウド上の、あらゆる ID のパーミッションを管理する単一の統合モデル

発見する

あらゆるリソースで、**あらゆる ID によって**実行されたすべてのアクションを**包括的に把握**する。

修復する

使用状況やアクティビティに基づいて**適切なサイズのパーミッション**を設定し、クラウドスケールで**オンデマンドなパーミッション**を適用する。

監視する

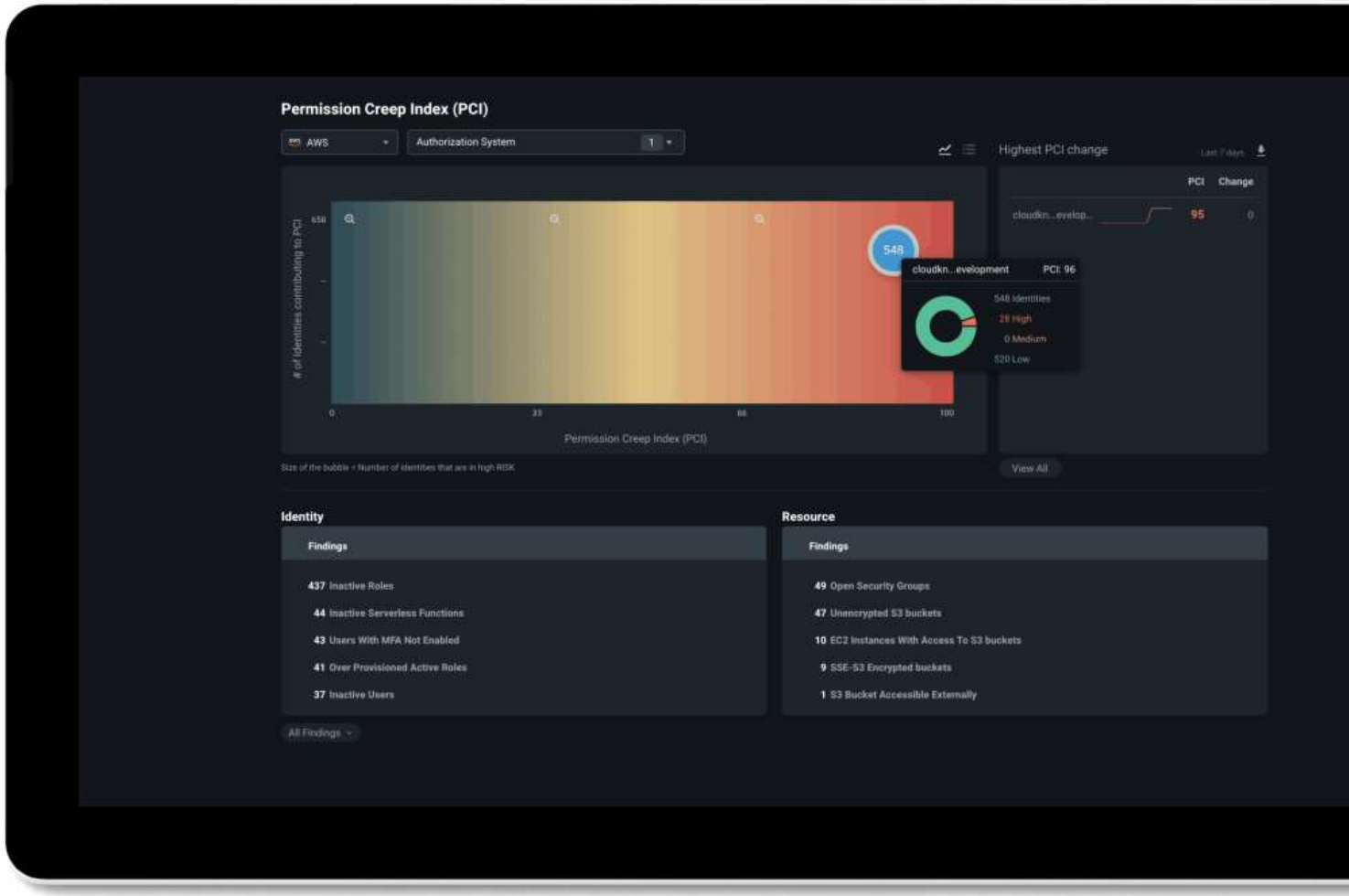
異常なパーミッションの使用を検出し、詳細な**フォレンジック レポート**を生成する。

発見と評価

パーミッション リスクを多次元的に把握する

- **Permission Creep Index** を使用して、リスク プロファイルを理解する。これは、付与されたパーミッションと使用されたパーミッション ギャップを評価する単一のメトリックです。

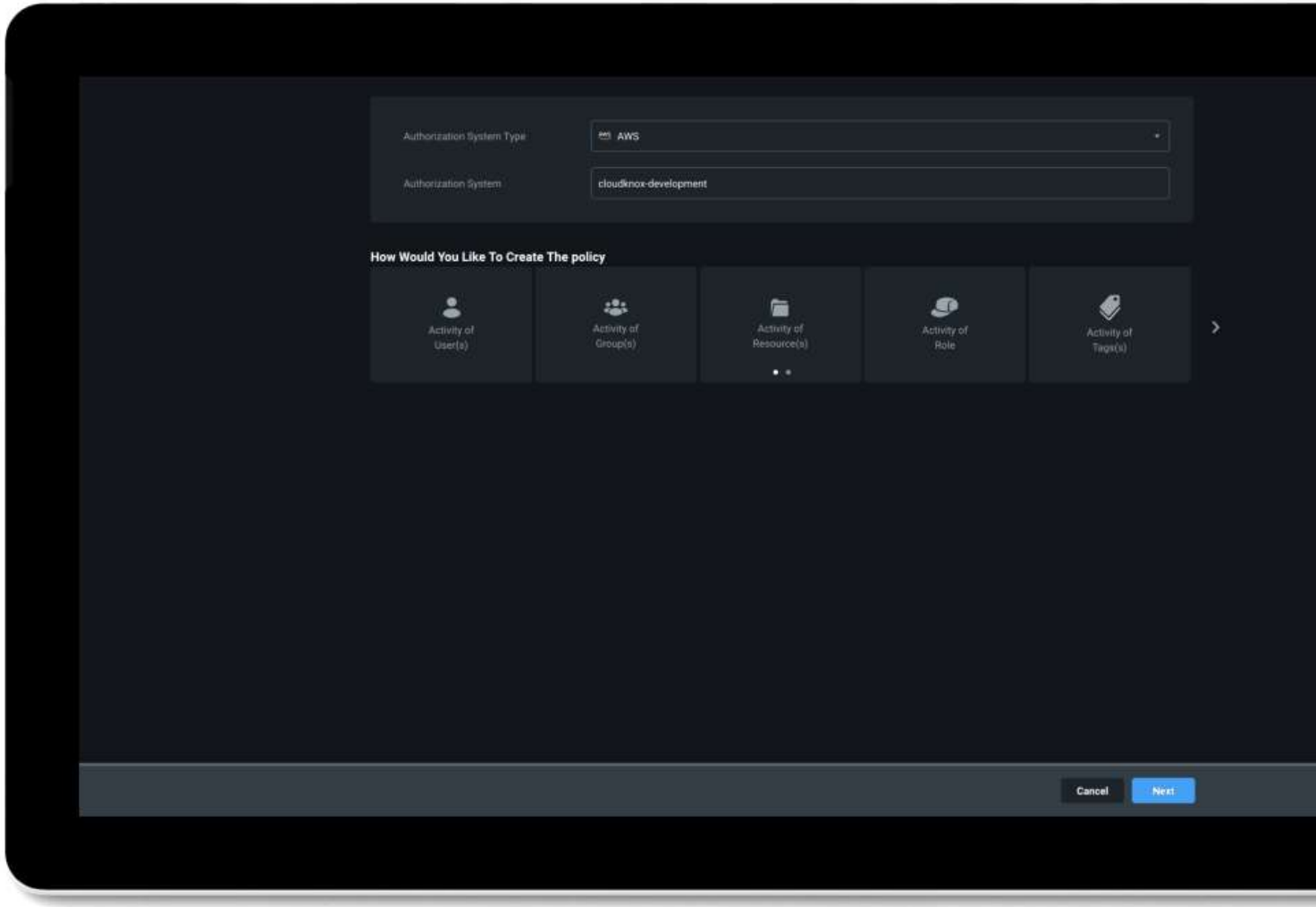
- 詳細な**使用状況を分析し**、あらゆるリソースであらゆる ID (ユーザー、アプリケーション、マネージド ID) によって実行されるすべてのアクションを明らかにする。



修復と管理

最小特権の原則を自動化する

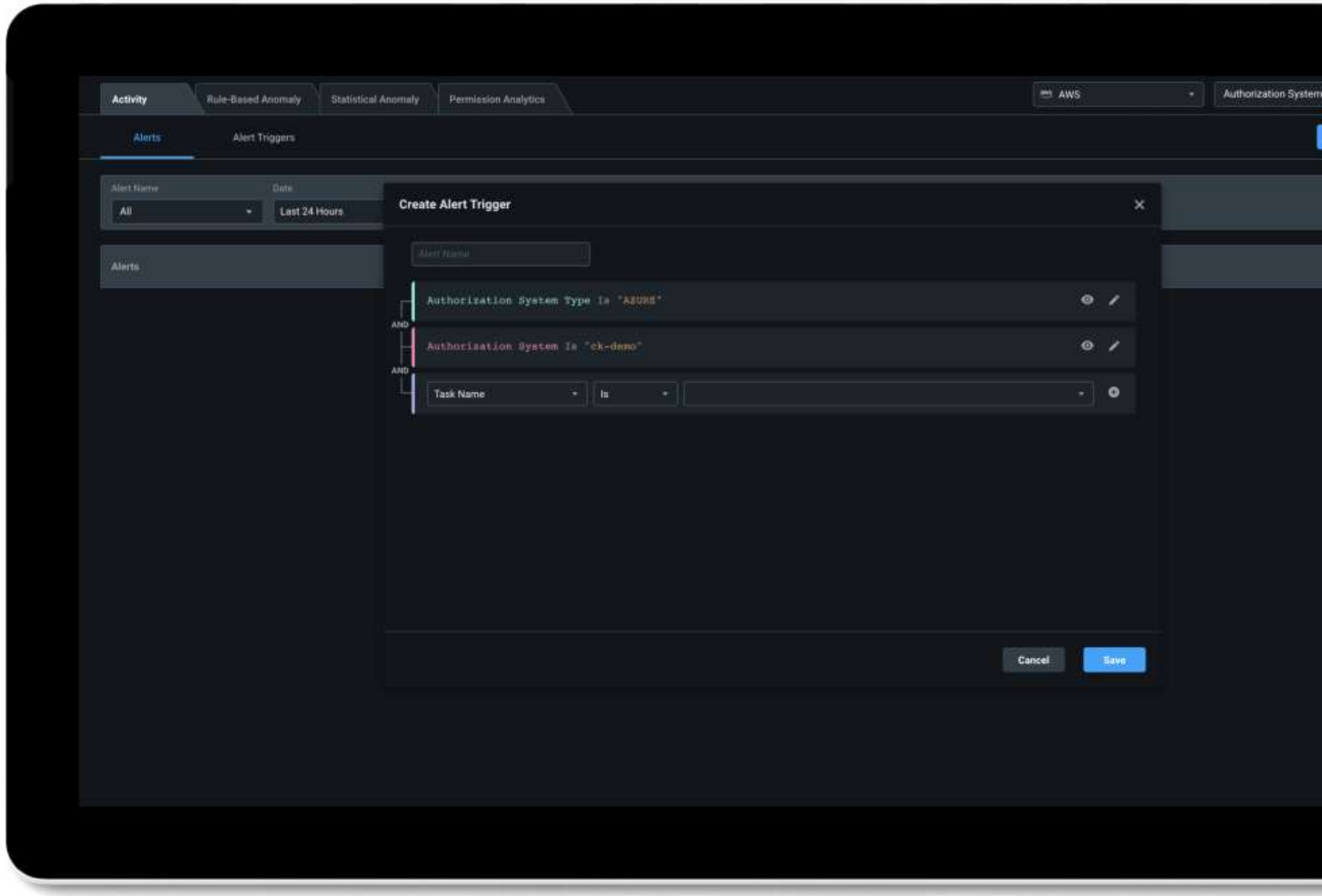
- 数回クリックするだけで新しいポリシー/ロールを作成し、最小特権のテンプレートを使用して Just-In-Time アクセスを適用することで、使用されていない過剰な権限を削除する。
- 期間限定、または必要に応じて、ID のパーミッションをオンデマンドで付与する。



監視とアラート

異常検出の合理化とインシデント レスポンスの迅速化

- パーミッションの使用パターンを追跡し、**カスタマイズ可能なアラートを使用する**。
- 高精度な**機械学習ベースの異常検出**で、セキュリティ ポスチャを強化する。
- **詳細なレポートとサイバー キル チェーン分析**を生成して、脅威の調査と修復を迅速化する。



ライセンス

Microsoft Entra 権限管理

無料で試す　価格を見る

Microsoft Entra Permissions Management

¥1,130 リソース/月

価格には消費税は含まれていません。

今すぐ購入

無料で試す >

Microsoft Entra 権限管理では、次のことができます。

- 組織内のリスクを多次元でとらえるために、ID、アクセス許可、リソースの評価を行います。
- 最小特権ポリシーの施行を自動化し、マルチクラウド インフラストラクチャ全体に一貫して適用します。
- アクセス許可の誤用や悪用から生じるデータ侵害を防ぐために、異常 (アノマリー) と外れ値を検出します。

サポートされるリソースには、コンピューティング リソース、コンテナー クラスター、サーバーレス関数、データベースがあり、アマゾン ウェブ サービス (AWS)、Microsoft Azure、Google Cloud Platform でサポートされます。

90 日間無料試用版をご用意しています。アクセス許可管理を無料で試して、リスク評価を実行してみてください。お客様のマルチクラウド インフラストラクチャ全体でアクセス許可の主なリスクを特定することができます。

[Microsoft Entra 権限管理 | Microsoft Security]

Permissions Management を今すぐ試す

Permissions Management を試し、
無料のリスク評価を実行して、マルチクラウド環境
全体での上位の権限リスクを特定します。
90 日間トライアルを今すぐ申し込む:
https://aka.ms/TryPermissionsManagement

詳しくはこちら
aka.ms/PermissionsManagement