すとなり
2025.02.12

Identity Migration Service (IMS)

オンプレミス AD 間の移行で ADMT が使われてきたが、それを大幅に拡張する IMS がリリースされる（名称が変更される）。

【ADMT の制限】
- サポートが切れており、セキュリティ上の懸念がある
- 機能のスコープがオンプレ AD のみ

【IMS の利点】
- サポートされ、セキュリティやコンプライアンスが考慮された新しいソリューション
- オンプレミス AD だけでなく Entra ID もサポート

- 1月末から 2 月にかけてブログが複数リリースされたが、Learn などにもまだ情報がない
- Entra Connect との関係が気になる
- 機能自体は今後リリースされるものっぽい？
- ライセンスも不明
- MIIS/FIM/ILM/MIM の系統？

【IMS が統合する機能】
- ADMS（Active Directory Migration Service）：AD 間のオブジェクト移行
- ADSS（Active Directory Synchronization Service）
  - ADDS for on-premises AD Synchronization：複数 AD からターゲット AD に同期
  - TSYNC（Tenant-to-Tenant Synchronization）：テナント間の単一の GAL を作成
- ADGMS（Active Directory Group Modification Service）：同期グループをクラウド グループに変換

https://techcommunity.microsoft.com/blog/microsoft-security-blog/why-identity-migration-service-ims-is-the-future-of-migration/4370335
https://techcommunity.microsoft.com/blog/microsoft-security-blog/exploring-the-use-cases-of-adxs-services/4373299
https://techcommunity.microsoft.com/blog/microsoft-security-blog/ims-project-success-story/4374844
https://techcommunity.microsoft.com/blog/microsoft-security-blog/whats-in-a-name/4371519
https://www.youtube.com/watch?v=wq4W6ZKfw4U

AD to AD Migration

Sync multiple ADs into one target AD domain, maintaining user and group SID history. Ensure continuous sync of users and groups with unidirectional password sync. The target AD is ready for cloud integration.

AD to Entra ID Migration

Complex many-domain or multi-tenant scenarios supported

Entra ID to Entra ID Sync

Sync and provision users and contacts between Entra ID tenants for collaboration, and provision guest accounts for Entra B2B to share resources. Operates indefinitely without on-premises connectivity

Entra Join 端末のプロファイルを維持

Group Modernization

Convert on-premises distribution groups synced to Entra ID via Entra ID Connect into cloud-only groups manageable in Office 365

Enabling Gal Generation

Email users, mail-enabled accounts, and contacts, including distribution lists as contacts, are supported in complex many-domain or multi-tenant scenarios

Unified Device Timeline Experience in Microsoft SIEM + XDR

現代のセキュリティチームは、複数のツールや断片化されたデータの操作の複雑さにより、大きな課題に直面しています。Microsoft Sentinel と Defender XDR のタイムライン エクスペリエンスを統合することで、次のことを目指します。

調査の簡素化: デバイスのアラート、異常、およびネットワークを含むデバイス アクティビティの統一されたビューを提供します
効率の向上: 別々のプラットフォームを切り替える必要がなくなり、より迅速な意思決定が可能になります

このイニシアチブは、Microsoft Sentinel を Defender XDR ポータルに統合し、ワークフローを合理化し、セキュリティの成果を向上させる統合 SIEM + XDR プラットフォームを作成するという Microsoft の取り組みにおける重要なマイルストーンです。

<セキュリティチームの主な利点>

統合ワークフロー: Sentinel と Defender XDR からすべてのデバイス アクティビティに 1 つのタイムラインでアクセスできます
包括的なインサイト: ドロップされたトラフィックやブロックされたトラフィックなど、重要なネットワーク アクティビティを可視化します
ユーザーエクスペリエンスの向上: Ibiza ポータルに移動することなく、Sentinel データをシームレスに統合します

https://techcommunity.microsoft.com/blog/microsoftsentinelblog/introducing-the-unified-device-timeline-experience-in-microsoft-siem--xdr/4372047

SQL2022CRM

Selected workspace: 'CyberSecuritySoc'

Guides & Feedback | Last 24 hours

SQL2022CRM

--
DNS Name

Identity

OS Type	OS Version
Windows	10.0
Is Domain Joined	**NetBios Name**
-	SQL2022CRM
Public IP Addresses	**Private IP Addresses**
-	172.27.2.4

Heartbeat (Last 30 days)

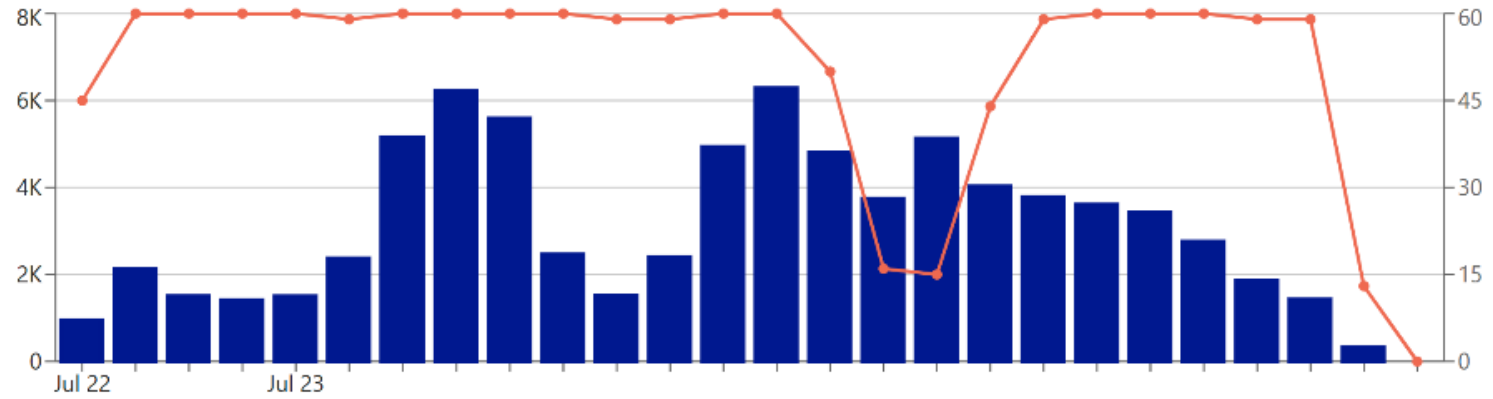
Earliest Heartbeat	Latest Heartbeat
24/04/2024, 20:16:22	23/07/2024, 20:14:31

Azure

Entity link
https://ms.portal.azure.com/#asset/Microsoft_Azu...

Investigate | Run playbook

Alerts, events and anomalies over time



SecurityAlert 1.3K | Anomalies 0 | SecurityEvent 79K

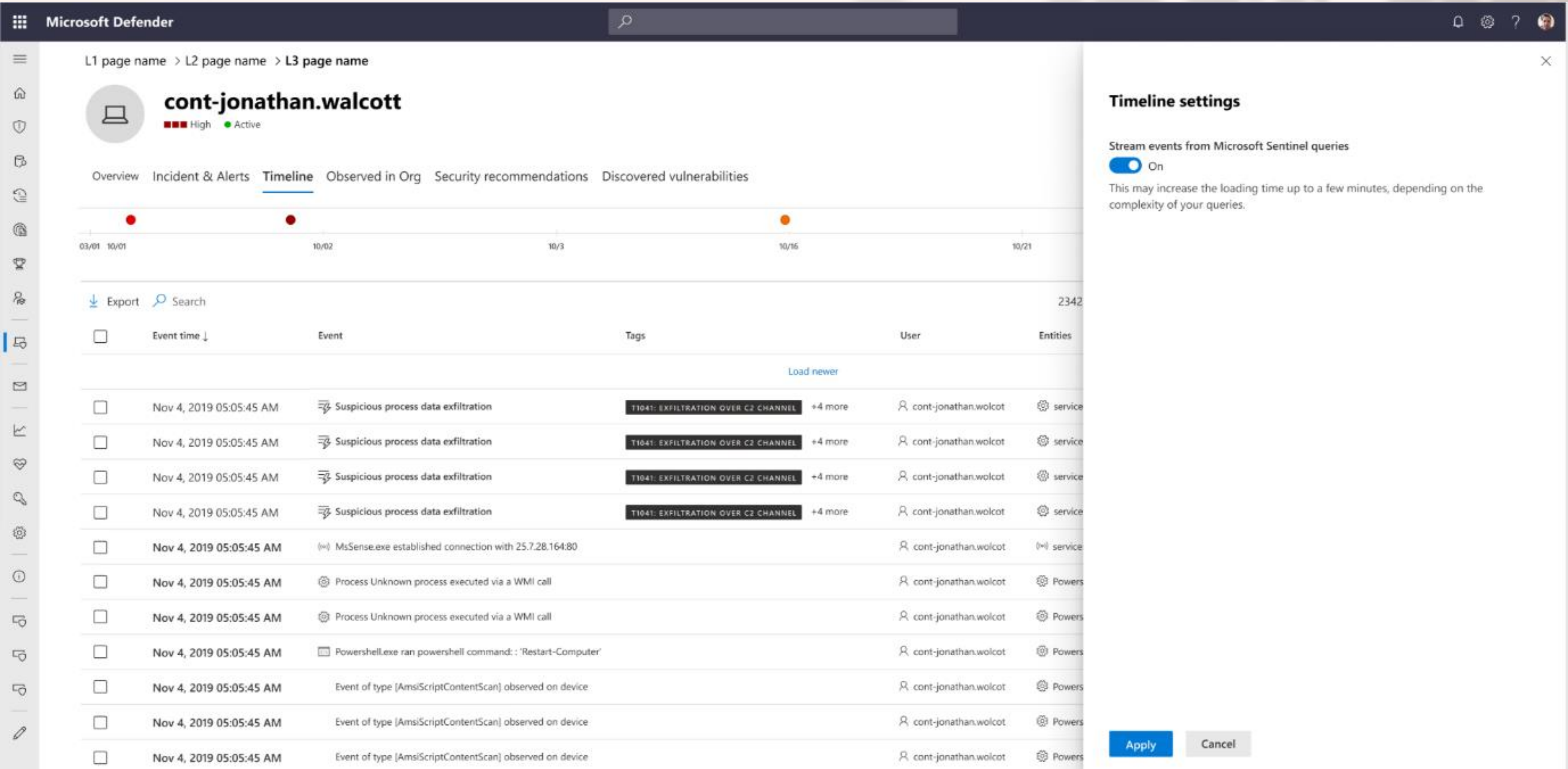
Entity timeline

Search | Timeline content : All | Tactics : All | Add filter

An 'Inbound' connection was made from '191.33.202.150' to '172.27.2.4' via port '3389'

Jul 23 19:37:55 — **A network connection is made to/from the device**
An 'Inbound' connection was made from '119.201.140.193' to '172.27.2.4' via port '3389'

Jul 23 19:35:27 — **A network connection is made to/from the device**
An 'Outbound' connection was made from '172.27.2.4' to '20.72.205.209' via port '443'


Microsoft Defender
L1 page name > L2 page name > L3 page name
cont-jonathan.walcott
High
Active
Overview
Incident & Alerts
Timeline
Observed in Org
Security recommendations
Discovered vulnerabilities
03/01
10/01
10/02
10/3
10/16
10/21
Export
Search
2342
Event time
Event
Tags
User
Entities
Load newer
Nov 4, 2019 05:05:45 AM
Suspicious process data exfiltration
T1041: EXFILTRATION OVER C2 CHANNEL
+4 more
cont-jonathan.wolcot
service
MsSense.exe established connection with 25.7.28.164:80
Process Unknown process executed via a WMI call
Powershell.exe ran powershell command: : 'Restart-Computer'
Event of type [AmsiScriptContentScan] observed on device
Timeline settings
Stream events from Microsoft Sentinel queries
On
This may increase the loading time up to a few minutes, depending on the complexity of your queries.
Apply
Cancel

Zero Trust Deployment Essentials for Digital Security

ゼロトラストはセキュリティ戦略です。これは製品やサービスではなく、次の一連のセキュリティ原則を設計および実装するためのアプローチです。
ゼロトラストは、その中核として、次の3つの基本原則に基づいて運用されています。

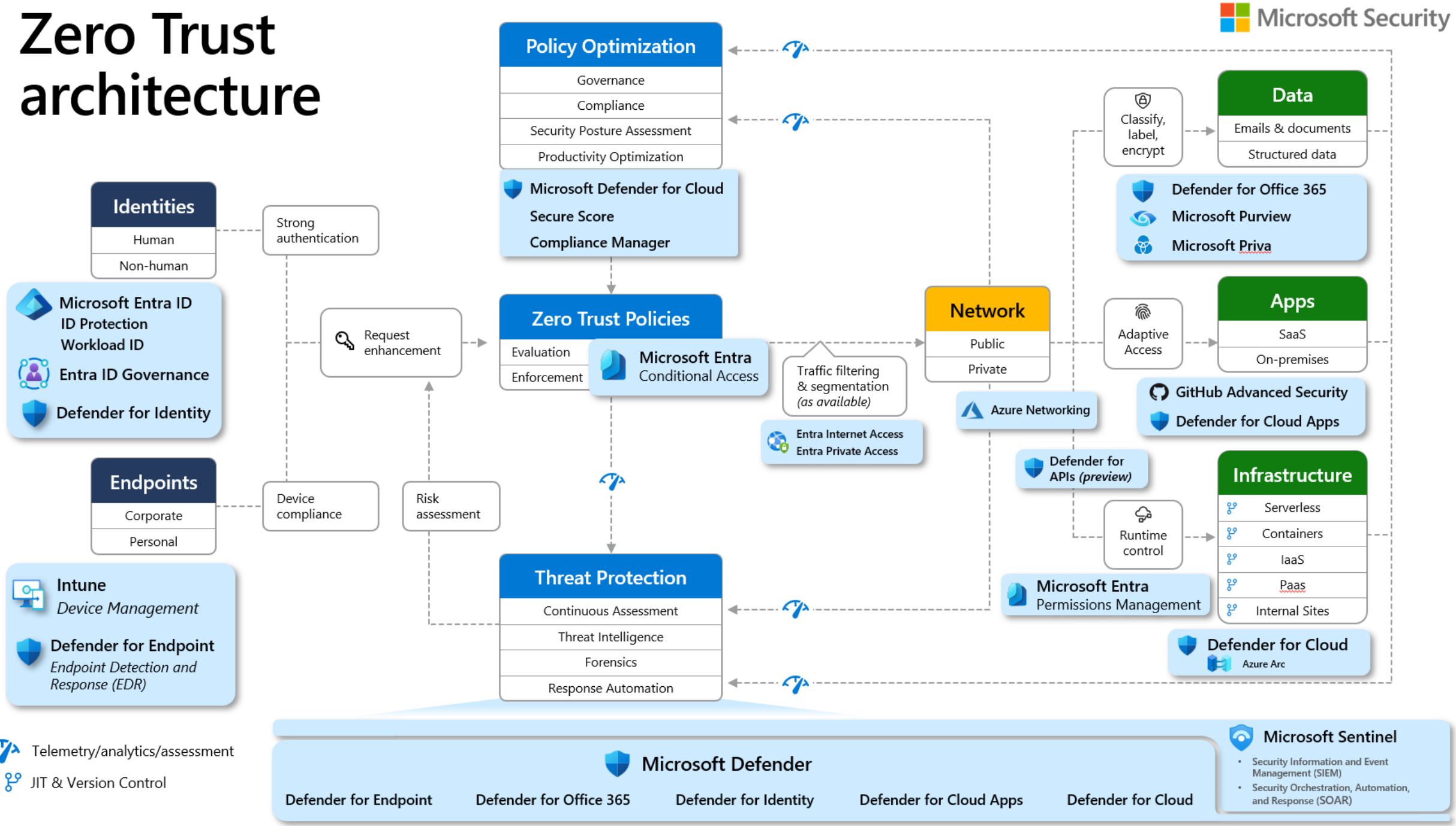
1. 侵害を前提とする（Assume Breach / Assume Compromise）
あらゆるもの（ID、ネットワーク、デバイス、アプリ、インフラなど）が攻撃され、それが成功する可能性があることを前提に対策を講じる。

2. 明示的に検証する（Verify Explicitly）
すべての信頼やセキュリティに関する判断は、利用可能なすべての情報やテレメトリを基に明確に検証し、攻撃者による不正な操作を防ぐ。

3. 最小特権アクセスを適用する（Use Least Privileged Access）
攻撃対象となる資産のアクセスを最小限に制限し、Just-In-Time（JIT）/ Just-Enough-Access（JEA） やリスクベースのポリシー（適応型アクセス制御など）を活用して制御する。

https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsoft-security-in-action-zero-trust-deployment-essentials-for-digital-securi/4372698
https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview

Zero Trust architecture



ありがとうございます

narisho