Microsoft
DIGITAL TRUST
Summit 2019

#digitaltrust

B-4

従業員に働く場所は自由に選ばせたい

-デバイスを社外に持ち出すときに考えなければいけないセキュリティのこと-

Microsoft Corporation
EEM Customer Acceleration Team
髙部 大佑

日本マイクロソフト株式会社
クラウド＆ソリューション事業本部
松井 大 CISSP

Microsoft

このセッションについて
従来(現在)の

ネットワーク境界防御から

ゼロトラストアーキテクチャへの

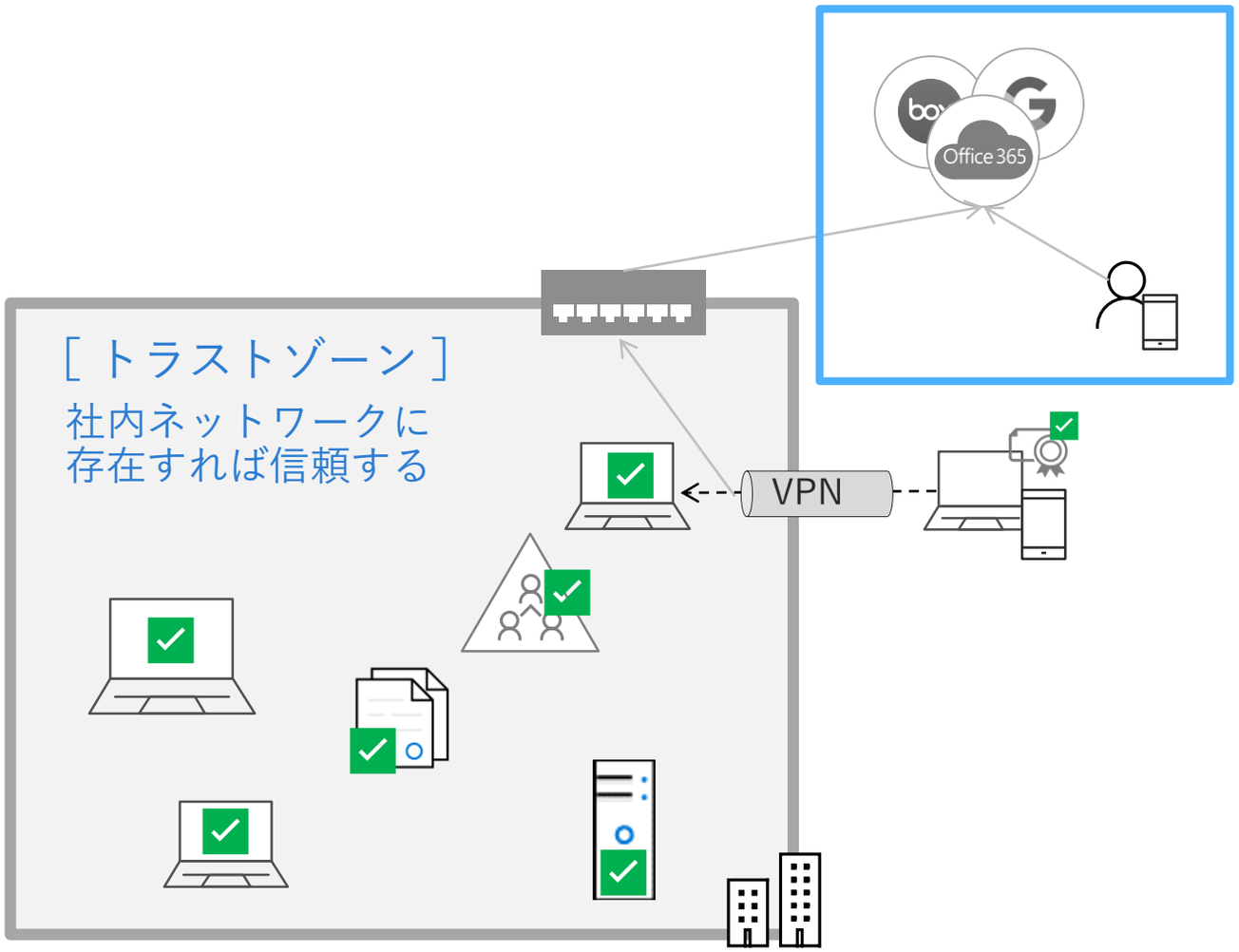
パラダイムシフトに対して必要なデバイス構成の
考え方と具体的な対策を検討できるようになって
いただくことを目的とします

なぜ、いま ゼロ トラスト の話をするのか？

今までは…
トラスト ＝ 信頼モデル

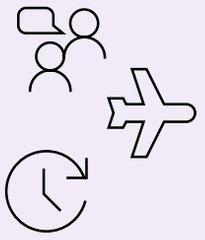
しかし!!
世界はトラストゾーンの外で動いている

信頼しているので、本物であることの確認はしない



IT 環境の変化

・アプリケーションのクラウド化
・インフラのクラウド化
・多様化するデバイス



働き方の変化

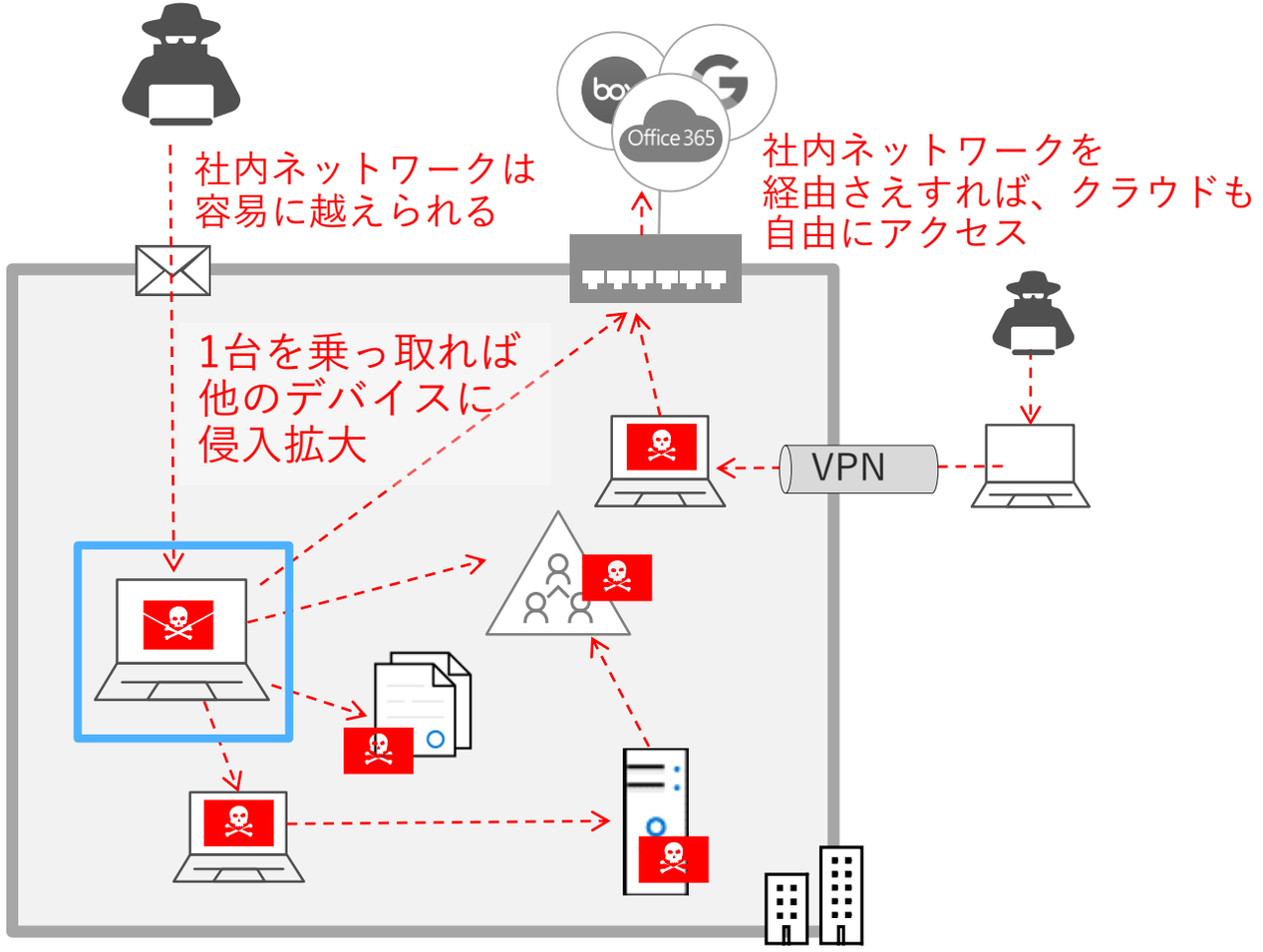
・多様化する働く場所、時間
・グローバル化
・B to B

なぜ、いま ゼロ トラスト の話をするのか？

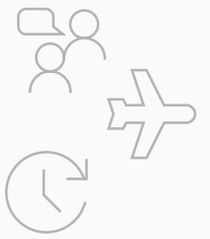
今までは…
トラスト ＝ 信頼モデル

しかし!!
世界はトラストゾーンの外で動いている

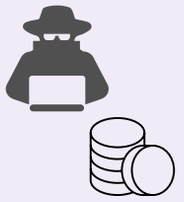
信頼しているので、本物であることの確認はしない
＝ 侵入済みの脅威に対して脆弱



IT 環境の変化
- アプリケーションのクラウド化
- インフラのクラウド化
- 多様化するデバイス



働き方の変化
- 多様化する働く場所、時間
- グローバル化
- B to B



脅威の変化
- 標的型攻撃
- 内部犯行
- ビジネスとしてのサイバー攻撃

“Zero Trust Model” というデザインの進化

2004
Jericho Forum
Formally Established

2014
Microsoft Advocates
“Assume Breach”

2016
Conditional
Access Released

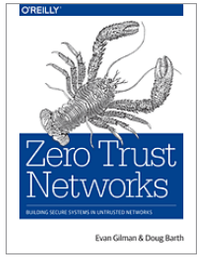
2019/9
NIST
SP 800-207 (DRAFT)

~2004
Network Access
Control (NAC)
Architectures

2010
Forrester coins
“Zero Trust” Term

2014
BeyondCorp
Published

2017



Slow mainstream adoption for both network identity models:

Network – Expensive and challenging to implement
Google’s BeyondTrust success is rarely replicated

Identity – Natural resistance to big changes
Security has a deep history/affinity with networking

ゼロトラスト = 信頼しないモデル

“Zero Trust Model” というデザインの進化

ついに NIST(アメリカ国立標準技術研究所)が標準化を考えはじめました

SP 800-207 (DRAFT)

NIST Zero Trust Architecture (ZTA)：
https://csrc.nist.gov/publications/detail/sp/800-207/draft

Zero Trust is the term for an evolving set of network security paradigms that move network defenses from wide network perimeters to narrowly focusing on individual or small groups of resources. A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established. ZTA is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA focuses on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of ZTA and gives general deployment models and use cases where ZTA could improve an enterprise’s overall IT security posture.

“Zero Trust Model” というデザインの進化

ついに NIST(アメリカ国立標準技術研究所)が標準化を考えはじめました

SP 800-207 (DRAFT)

NIST Zero Trust Architecture (ZTA)：
https://csrc.nist.gov/publications/detail/sp/800-207/draft

ゼロトラストはネットワーク防御を広範なネットワーク境界から、個々または小規模のリソース グループに絞り込む、進化するネットワーク セキュリティ パラダイムのセットの用語です。A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established. ZTA is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. ZTA focuses on protecting resources, not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of ZTA and gives general deployment models and use cases where ZTA could improve an enterprise’s overall IT security posture.

“Zero Trust Model” というデザインの進化

ついに NIST(アメリカ国立標準技術研究所)が標準化を考えはじめました

SP 800-207 (DRAFT)

NIST Zero Trust Architecture (ZTA)：
https://csrc.nist.gov/publications/detail/sp/800-207/draft

ゼロトラストは、ネットワーク防御を広範なネットワーク境界から、個々または小規模のリソース グループに絞り込む、進化するネットワーク セキュリティ パラダイムのセットの用語です。A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established. ZTA is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary.

ZTA は、ネットワークの場所がセキュリティの主要なコンポーネントと見なされなくなったため、ネットワーク セグメントではなくリソースの保護に重点を置いています。 This document contains an abstract definition of ZTA and gives general deployment models and use cases where ZTA could improve an enterprise’s overall IT security posture.

保護対象：ネットワーク から リソース

ネットワークベースのゼロトラスト		ID/"デバイス"ベースのゼロトラスト
ネットワーク接続のアクセス制御	対象	資産(リソース)単位でのアクセス制御
ネットワーク・セキュリティベンダー	ベンダー	IDaaSベンダー（Microsoftなど）
マイクロセグメンテーション	手法と効果	認証・認可、「信頼済み」の証明書
IPアドレスなどに紐づけられる資産だけが対象となり、SaaSやPaaS上の資産は対象外。ベンダー固有の技術を利用し、標準化された技術はない		標準化された技術を利用し、ベンダーを超えた信頼性を確保できる。資産の場所に関係なく、どこにあっても信頼性を維持できる

ID/"デバイス"ベースのゼロトラストによって、アプリケーションやデータレベルでの信頼性を構築

真に安全なデバイスであることを担保し、ユーザのふるまい検知をベースにした運用を行うことで、
少ないデータでより多くの信頼できるインテリジェンスを活用することができる

Intune is not only an MDM!

Microsoft Intune

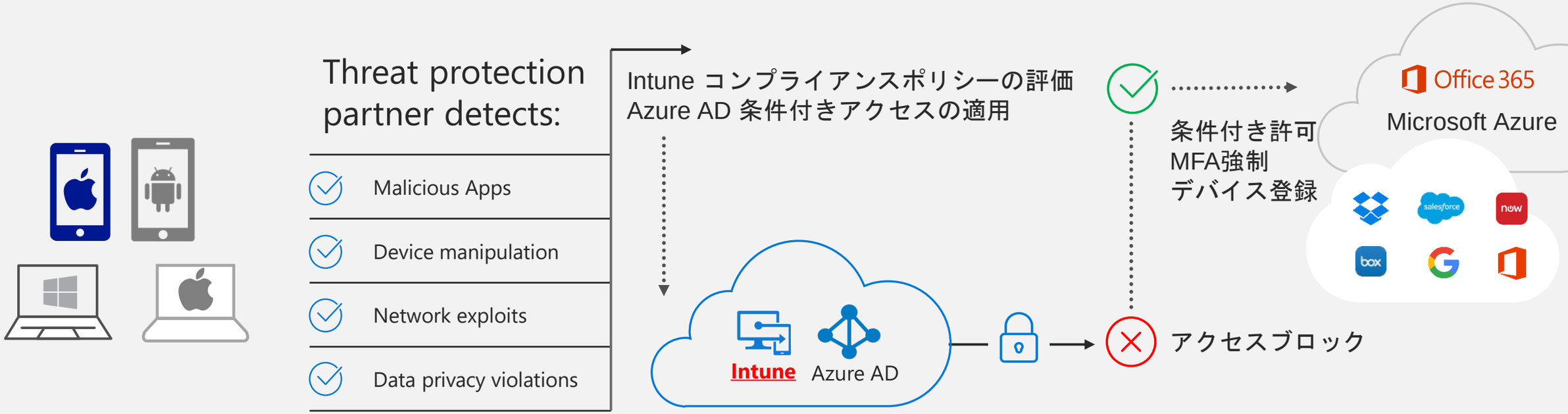
デバイスのモバイル利用でよくある要件・要望

クラウド移行に伴い、**場所を問わず**、**ストレスフリー**な
会社データへのアクセスを**セキュアなデバイス**に許可

- Windows 10
  - ADドメイン グループポリシー + VPN (ADFS+証明書) がセキュアな状態で動作？
- iOS, Android
  - 社給シナリオ (VPN + 証明書) ≠ セキュリティ

デバイスの状態を継続して評価、状態に応じたアクセス制御、
アクションおよび管理者へレポートが必要

デバイスの状態とリスクに基づくアクセスコントロール



Microsoft Defender ATP 連携

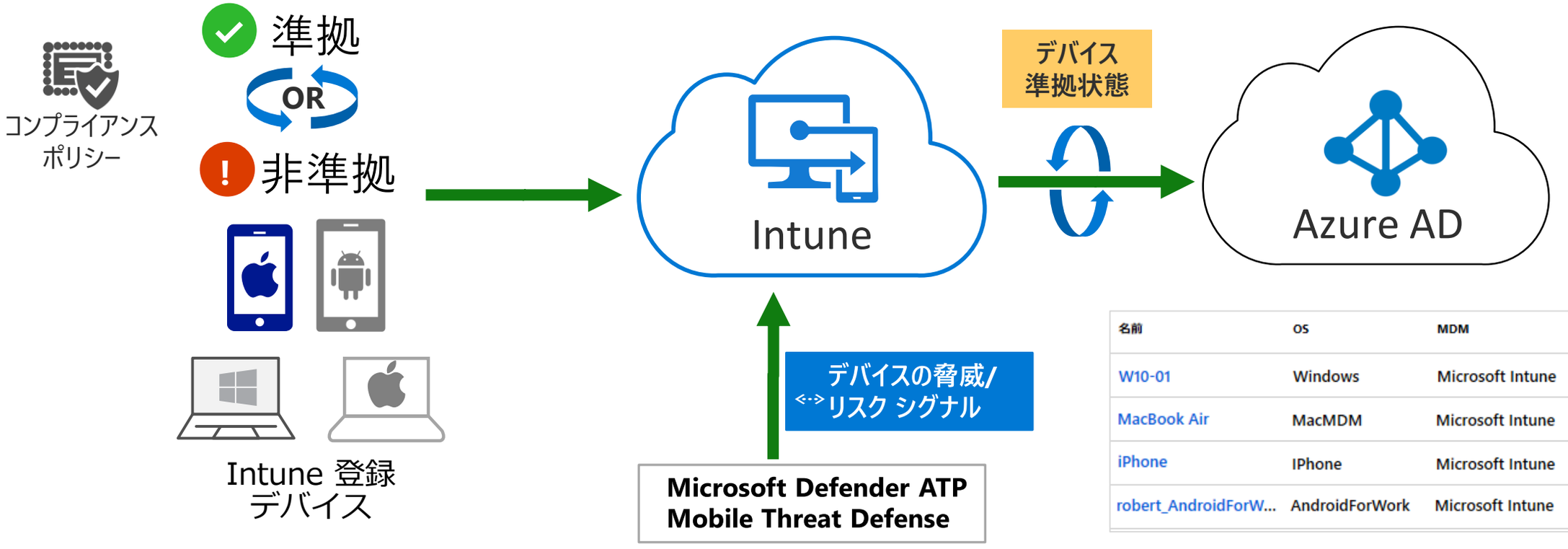
Mobile threat defense (MTD) パートナー (iOS, Android)

Microsoft
Lookout
Symantec
ZIMPERIUM
pradeo
Google Play Protect
Check Point SOFTWARE TECHNOLOGIES LTD

デバイス状態
＋ リスクの評価
（MDATP/MTD連携）

デバイス準拠状態の評価と更新

デバイスの準拠状態に応じて デバイス情報を動的に更新



名前	OS	MDM	準拠している
W10-01	Windows	Microsoft Intune	いいえ
MacBook Air	MacMDM	Microsoft Intune	いいえ
iPhone	IPhone	Microsoft Intune	はい
robert_AndroidForW...	AndroidForWork	Microsoft Intune	はい

iOS, Android の ポリシー準拠 デバイスとは

デバイスの状態を継続して監視、正常性を評価

組み込みデバイス
コンプライアンスポリシー
（グローバル設定）

- **コンプライアンスポリシー割り当てなしのデバイス**
  - **非準拠 (既定) or 準拠**
- **コンプライアンス状態の有効期間**
  - **既定３０日**
- 脱獄の高度な検出（iOS）
  - iOS で位置情報サービス有効化が必要
  - バッテリー使用量に影響

＋

コンプライアンスポリシー
(iOS, Android)

- **脱獄、ルート化**
- OS の最大/最小バージョン
- **デバイスPINおよび構成**
- 制限アプリ
- Android
  - **Google Play Protect**
  - **デバイス暗号化**
  - **提供不明のアプリブロック**
  - **USBデバッグ**
  - セキュリティパッチレベル
  - 場所 (Network fencing)
- **デバイス脅威レベル（MTD連携, リスクベースCA）**

コンプライアンス非対応に対するアクション

AADデバイス状態更新

準拠

OR

非準拠

メール通知

リモートロック (iOS, Android)

Windows 10 の コンプライアンス ポリシー

ポリシーカテゴリ	ポリシー設定
デバイスの正常性	Windows 正常性構成証明サービスの評価規則 • **BitLocker を必須とする** • **デバイス上でセキュアブートの有効化が必要** • **コードの整合性が必要**
デバイスのプロパティ	オペレーティングシステムのバージョン • 最小 OS バージョン • 最大 OS バージョン • 有効なオペレーティングシステムのビルド
Configuration Manager の コンプライアンス	System Center Configuration Manager からデバイス コンプライアンスが必要 *Co-Management 構成のみ
システムセキュリティ	• パスワード • **暗号化** • **デバイスのセキュリティ（Defender Firewall, TPM, ウイルス対策, スパイウェア対策の有効化 ）** • **Microsoft Defender（エンジン、定義が最新、リアルタイム保護の有効化 ）**
Microsoft Defender ATP (リスクベース CA)	**Microsoft Defender Advanced Threat Protection 規則**

紛失対策

静的な脅威対策

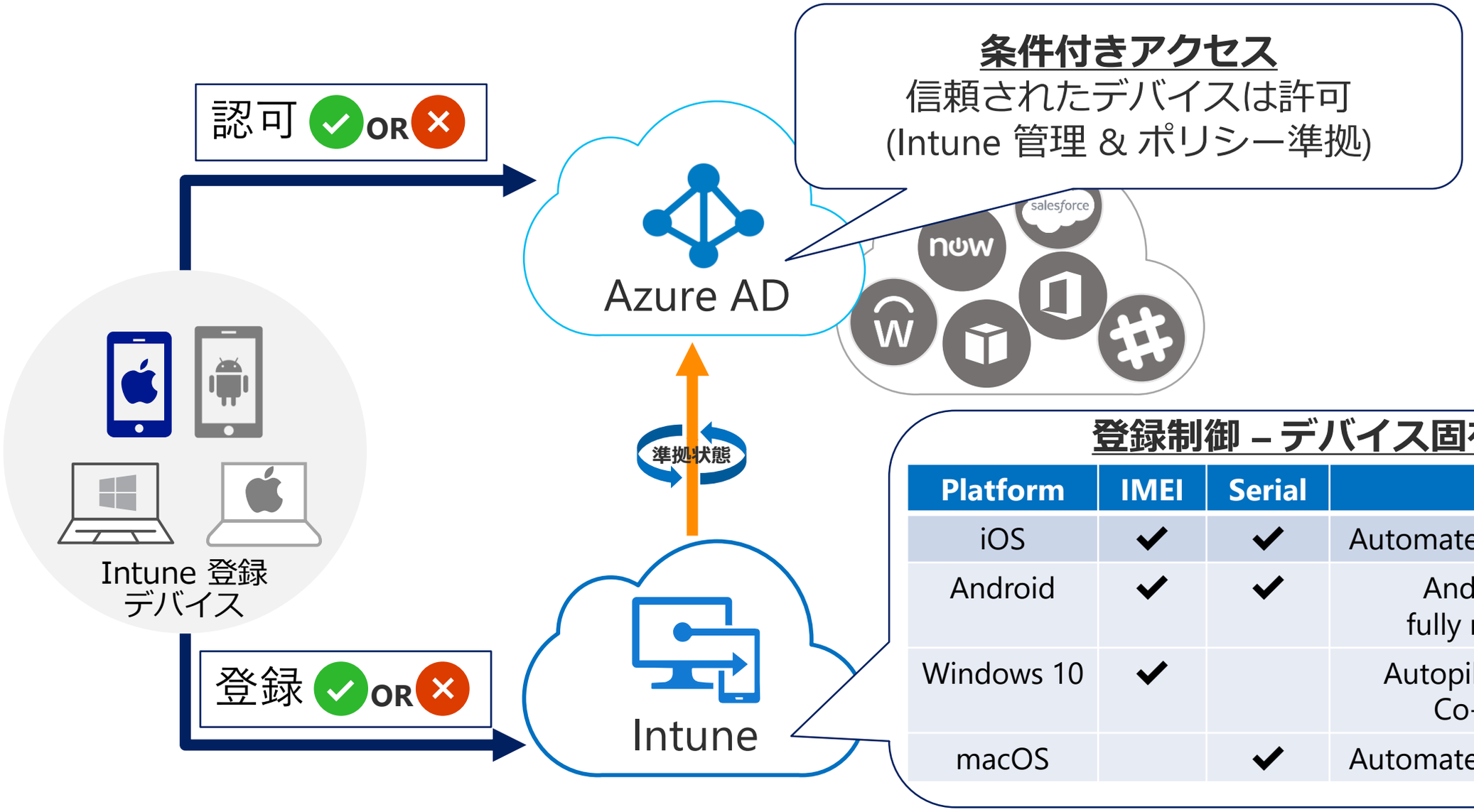
動的な脅威対策

Microsoft

Demo
Intune ポリシー準拠, 状態の確認

DIGITAL TRUST
Summit 2019

ゼロトラストモデルの デバイス ベース アクセス制御



登録制御 – デバイス固有情報

Platform	IMEI	Serial	社給展開
iOS	✔	✔	Automated Device Enrollment
Android	✔	✔	Android Enterprise fully managed device
Windows 10	✔		Autopilot, GPO自動登録, Co-Management
macOS		✔	Automated Device Enrollment

Windows 10 OS、アプリ脆弱性の対策（MDATP連携）

Microsoft

Demo
Intune + MDATP連携による
アプリ脆弱性の対応

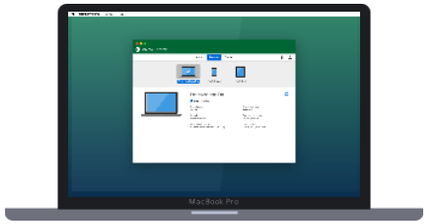
DIGITAL TRUST
Summit 2019

デバイス登録の
モダンなプロビジョニング

ゼロタッチ デバイス プロビジョニング

Apple iOS

Automated Device Enrollment



macOS

Automated Device Enrollment

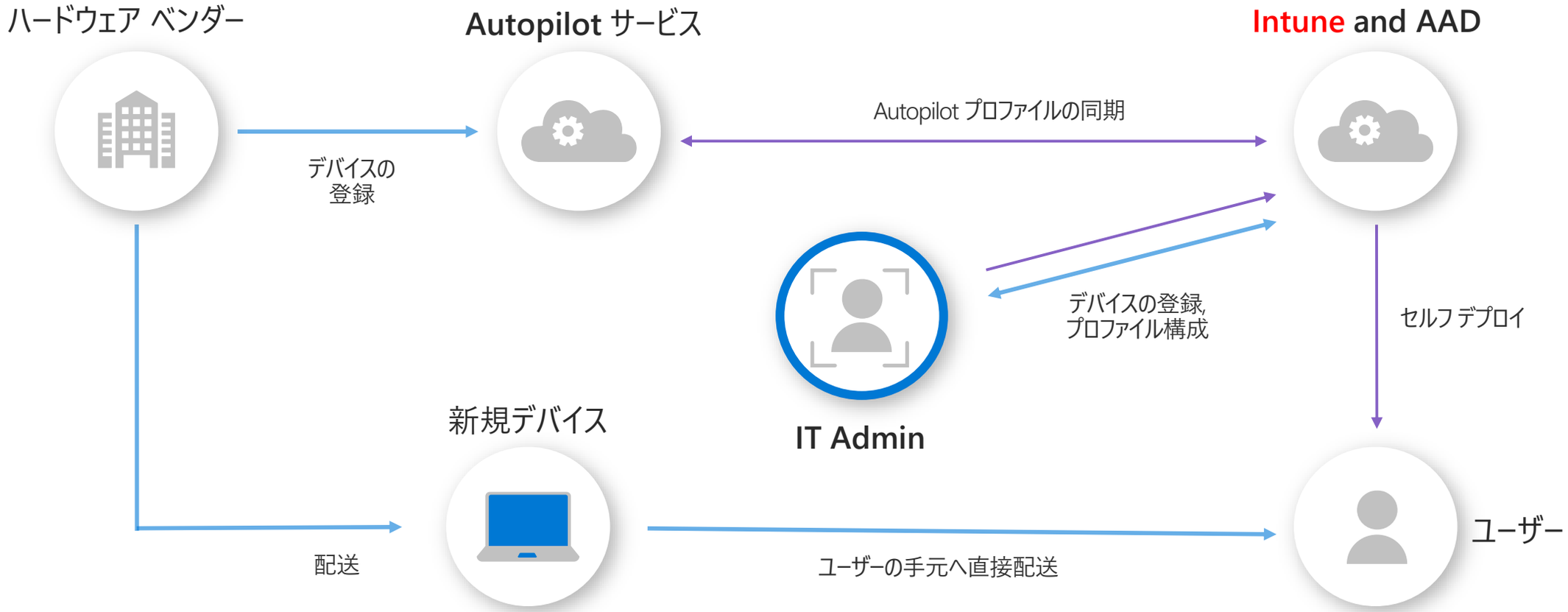
Android

Android Enterprise
Zero Touch Enrollment

Windows 10

Windows Autopilot

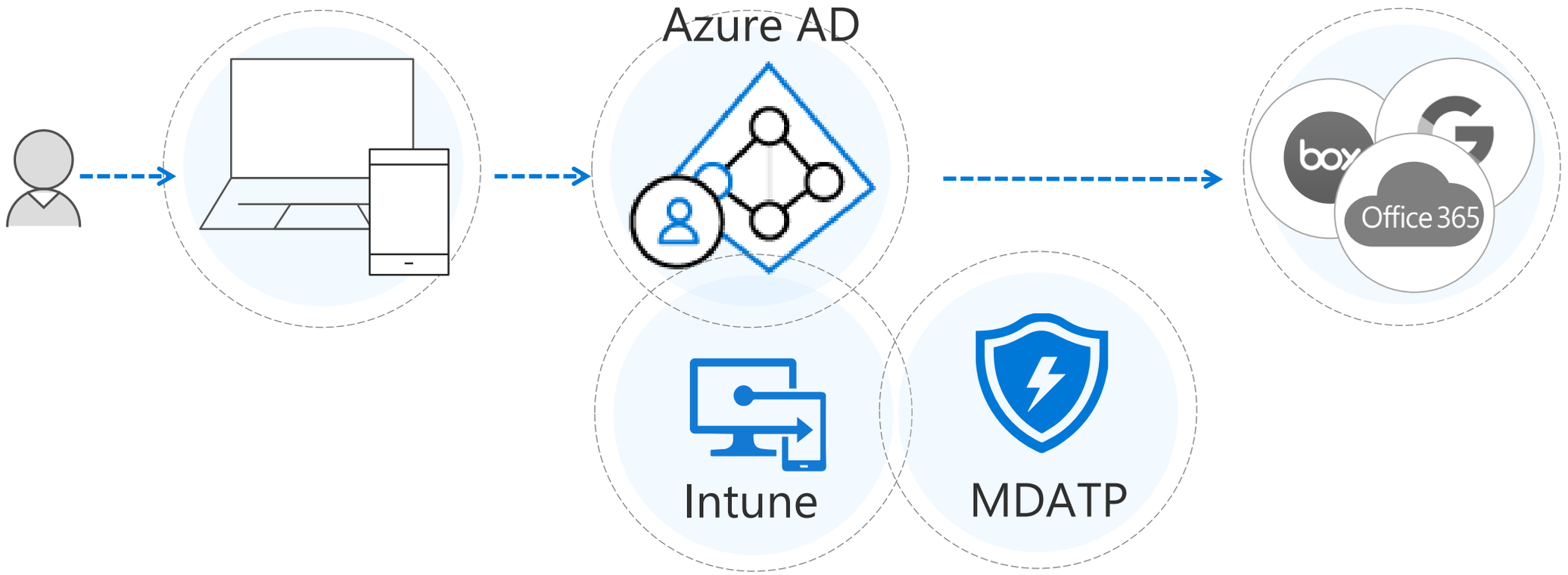
モダン プロビジョニング – Windows Autopilot



- 場所を問わずに、ユーザー セルフで業務に必要なデバイスを展開
- デバイス展開にかかる時間を削減
- イメージの作成、更新にかかる工数を削減

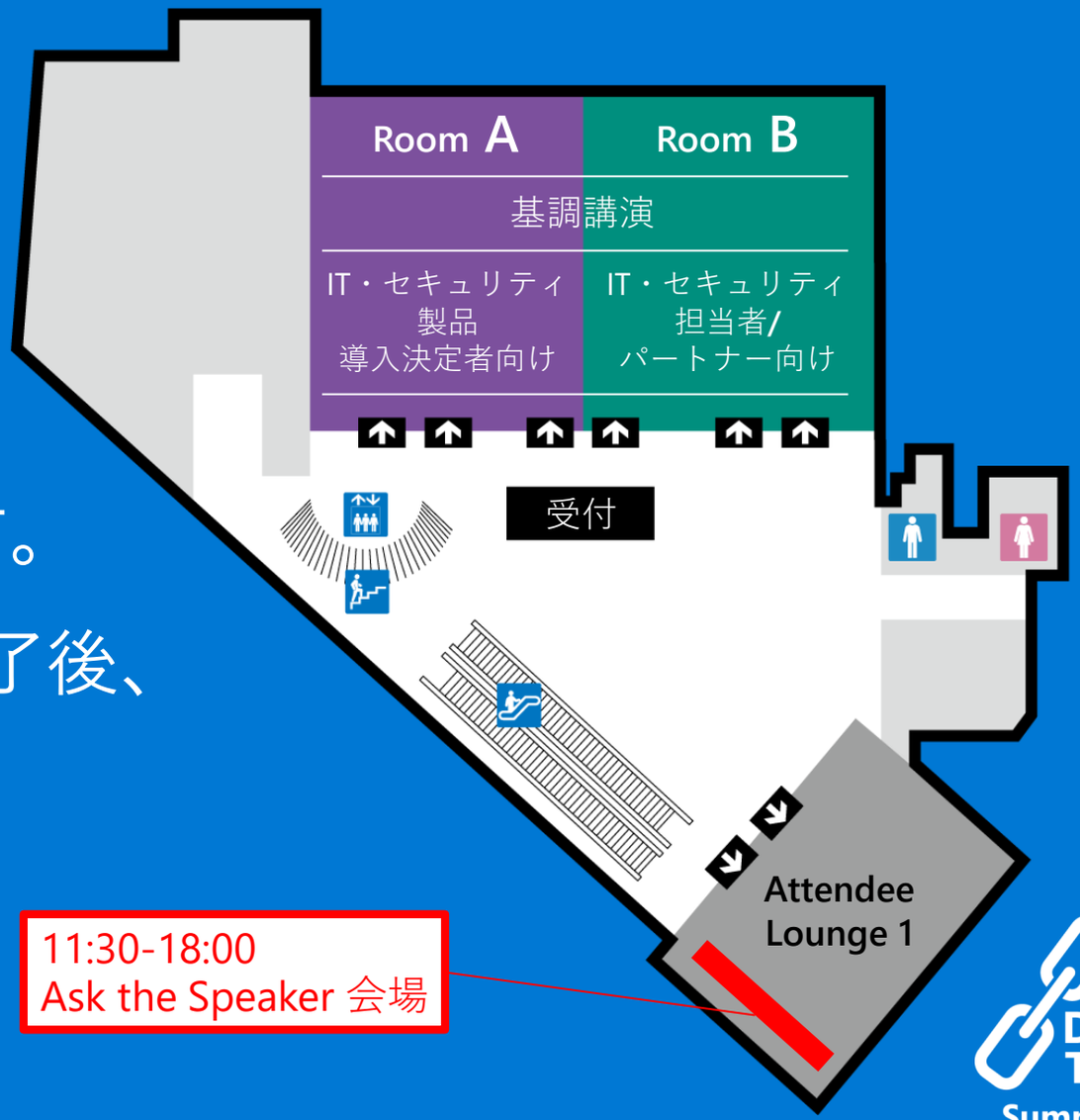
まとめ

- ✓ ネットワーク境界防御→ゼロトラストへの変革の時期
- ✓ 厳密な デバイス+ID の状態を常に確認することが重要
- ✓ Azure AD + Intune + Microsoft Defender ATP



Ask the Speaker について

Attendee Lounge 1 内に、
各ブレイクアウト セッション終了後、
Ask the Speaker をご用意しております。
※Ask the Speaker は各セッション終了後、
30 分程度実施する予定です。



DIGITAL TRUST
Summit 2019

アンケートにご協力ください

本イベントおよびセッションへのアンケートに
ぜひご協力ください。
お帰りの際は、イベント アンケートにお答えいただき、
日本マイクロソフトからの連絡が可能な方には
Yubico セキュリティキーを差し上げております。

Yubico セキュリティキー
(U2F と FIDO2 に対応)

DIGITAL TRUST
Summit 2019

Microsoft

#digitaltrust