
Microsoft
DIGITAL TRUST
Summit 2019
Microsoft

DIGITAL TRUST
Summit 2019

山崎 善寛

Yoshihiro Yamasaki

日本マイクロソフト株式会社
Microsoft 365 ビジネス本部
本部長


デジタルな世界の広がり

増え続ける
エンドポイント

把握できない
ITやサービス

次々に変わる
攻撃手法

データの保護と
生産性のトレードオフ

捨てられない
セキュリティソリューション

慢性的な
セキュリティ人材不足

増え続ける
エンドポイント

データ
生産性の

慢性的な
セキュリティ人材不足

統合化されたシンプルな
IT基盤の構築

人材の育成の
負担軽減

統合化されたシンプルな
IT基盤の構築

ネットに点在しているものはなにか

重複した資産はないか

権限管理は一元化されているか

クラウド上のID管理サービス

	ネットワークベースのゼロトラスト	IDベースのゼロトラスト
対象	ネットワーク接続のアクセス制御	資産単位でのアクセス制御
ベンダー	ネットワーク・セキュリティベンダー	IDaaSベンダー（Microsoftなど）
手法と効果	マイクロセグメンテーション 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	認証・認可、「信頼済み」の証明書 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

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

新しいITを扱う知識？

新しい攻撃に対応するスキル？

正しい判断力？

AIやインテリジェンスの活用

人材の育成の
負担軽減

DIGITAL TRUST

Summit 2019

DIGITAL TRUST
Summit 2019

Siân John MBE

シアン・ジョーン

EMEA/APJ
Cybersecurity Strategy

Microsoft

The power of people; amplifying our human capacity through technology and community

Siân John MBE
EMEA/APJ Cybersecurity Strategy
Cybersecurity Solutions Group

$8 TRILLION

2022年までの世界経済に
対するサイバー犯罪のコスト

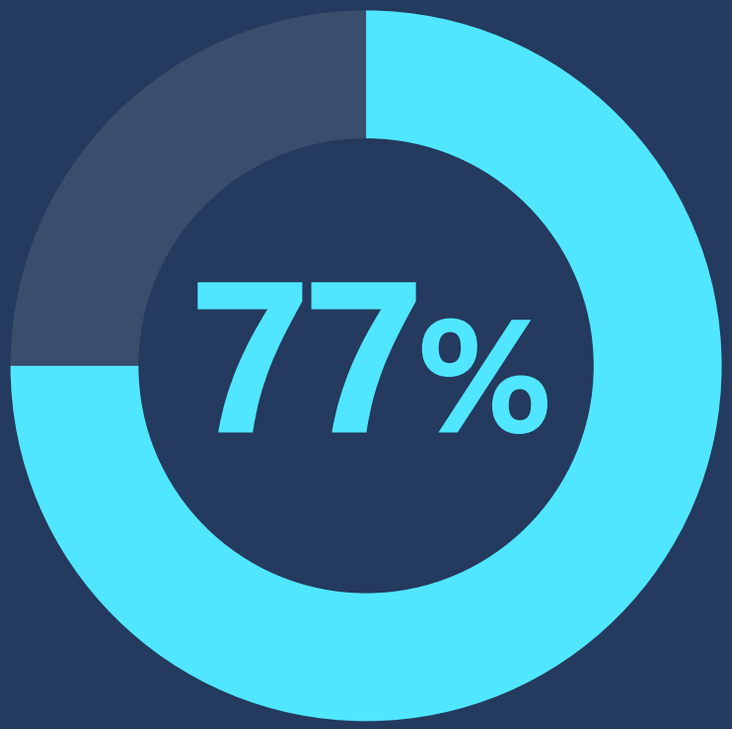
¥400 BILLION

1つのデータ侵害の平均コスト

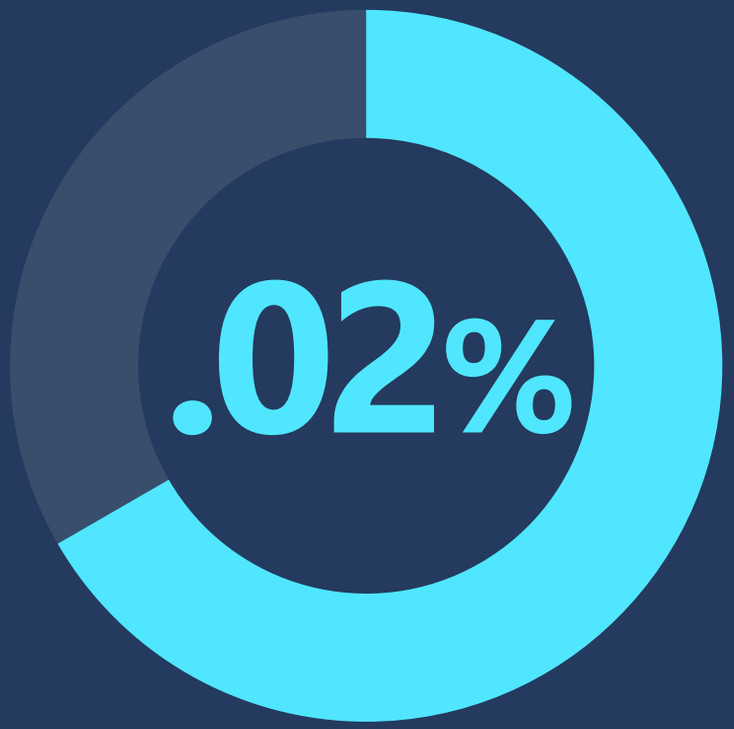
1 in 5

サイバー攻撃により
1/5 の組織が顧客を失う

マルウェア発生率は世界平均より
60% 低い



ランサムウェアの発生率が
75% に低下

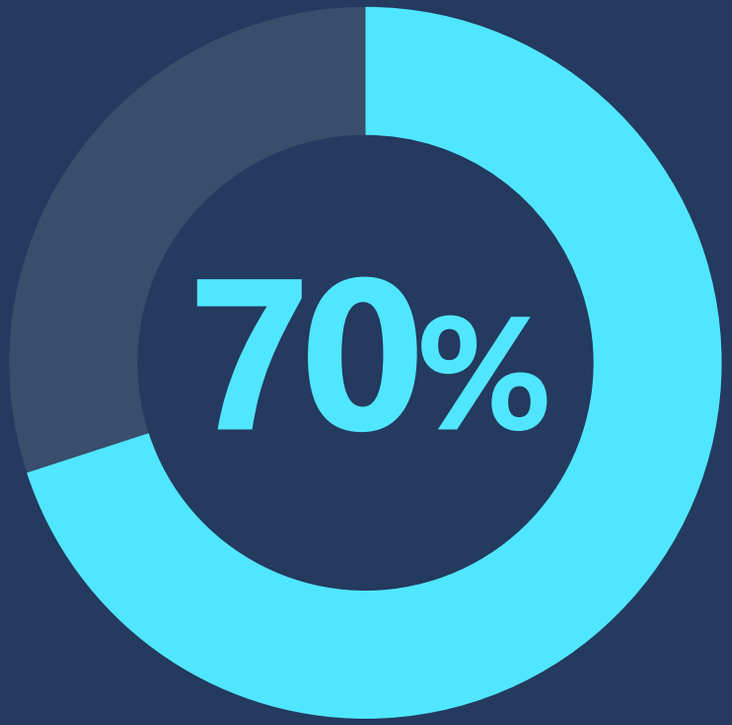


0.02%
仮想通貨の採掘率

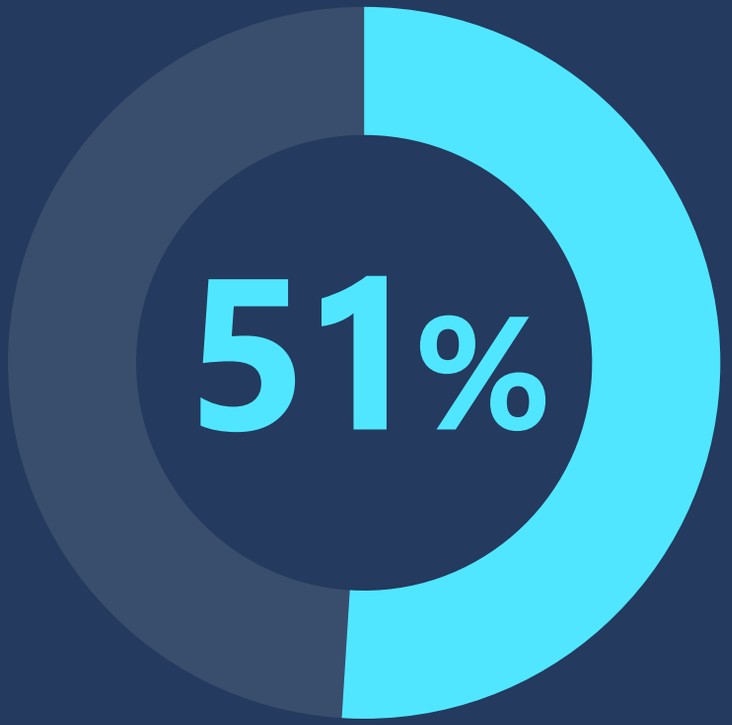

PROTECT
DETECT
RESPOND


soil temperature
71°

セキュリティ専門家の
今後 2 年間の推定不足数



IT雇用者の多くは、ITプロフェッショナルの中程度から極端なスキル不足に直面していると述べている



51% はストレスの少ない
低賃金の仕事を引き受ける









mawingu







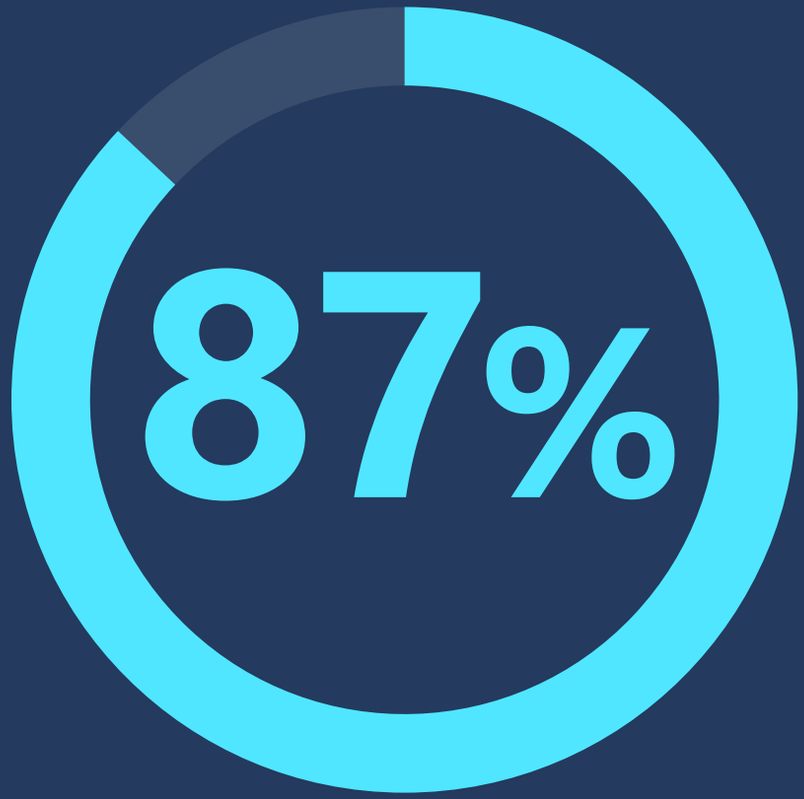
398円



LEAD

DIVERSE TEAMS

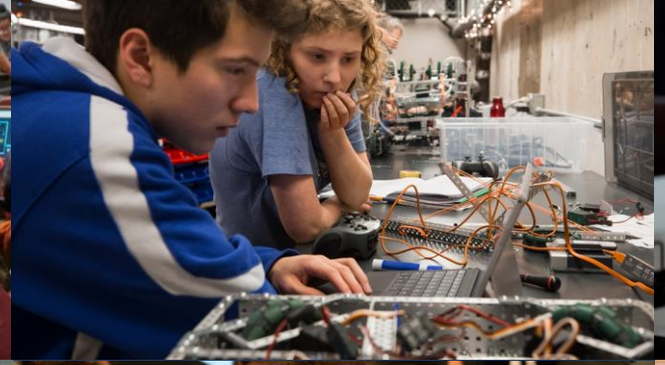
MAKE BETTER DECISIONS UP TO



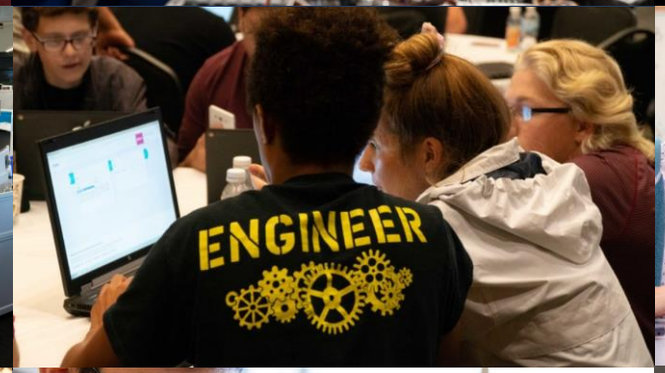
OF THE TIME







PROTECT
DETECT
RESPOND

ENGINEER










PENNSTATE


Microsoft
ThinkPad

At Microsoft, our mission is to empower every person and every organization on the planet to achieve more

DIGITAL TRUST

Summit 2019

DIGITAL TRUST
Summit 2019

河野 省二

Shoji Kawano

日本マイクロソフト株式会社

Chief Security Officer

セキュリティ人材の雇用や教育が困難

- 2020年までにセキュリティ人材は1800万人不足すると言われています
- 社内のセキュリティ人材のトレーニングに投資することと、従業員間でセキュリティを意識した文化を構築することが重要です

複雑な攻撃、判断の難しさ

- 信頼できるアラートを手に入れるために、大規模なクラウドプロバイダーが持つインテリジェンスや専門知識を活用する
- 自動化されたソフトウェアベースの処理で分析や対応をリアルタイムに行うことが可能です


情報収集
インテリジェンス
レポート
人口知能
判断
自動化
対応

M365

https://security.microsoft.com

Microsoft 365 Security Center

Share | Comments and history | Actions and assistance

Dashboard > **Incident**

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

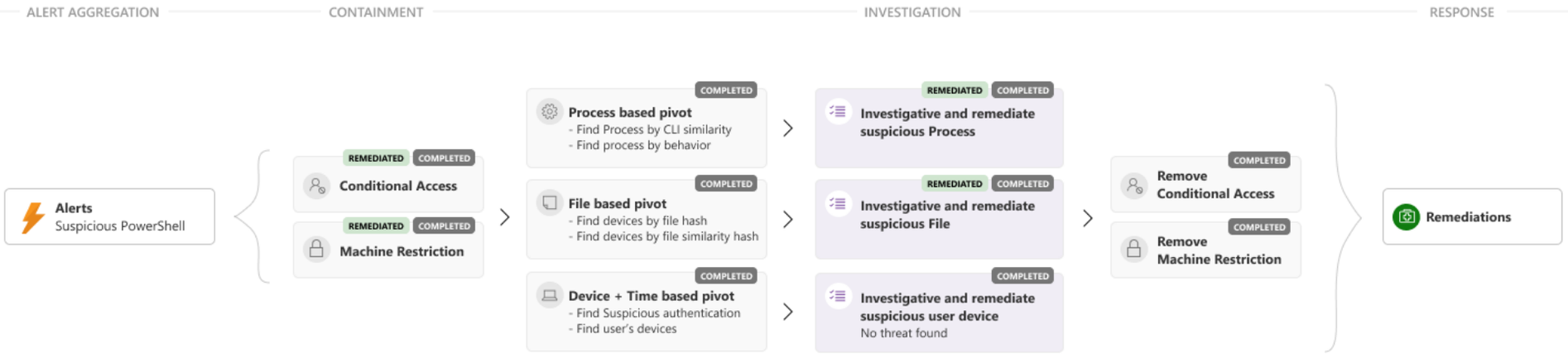
Duration
00H : 03M : 23S

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Collapse table

Export | Customize columns | Filters

Triggering alert	Investigation state	Investigated entities	Start date	Duration
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso	Jul 03, 2018 09:26 AM	00:00:23
Suspicious PowerShell	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:23
Golden ticket compromised	Running	JW Jonathan Wolcott	Jul 03, 2018 09:26 AM	00:00:23
Spear-phishing attack	Remediated	cont-jonawolcot	Jul 03, 2018 09:26 AM	00:00:20



M365

https://security.microsoft.com

Microsoft 365 Security Center

Dashboard > Incident

Alerts | Devices | Identities | **Investigations** | Incident graph | Action center

Incident #496

Edit incident name

High

Conditional access applied

INCIDENT DETAILS

Status
Active

Classification
True positive
Set status and classification

Assigned to
Dan Smith
Unassign

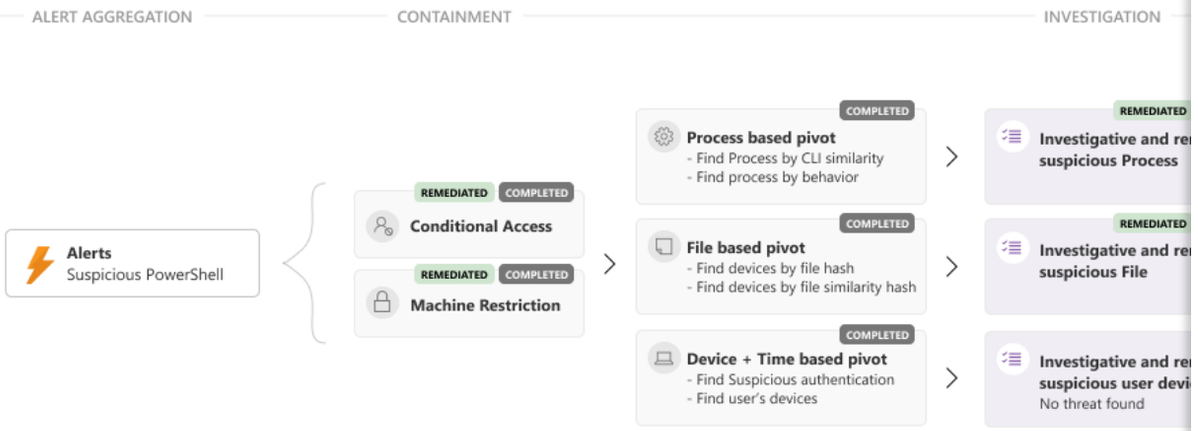
Category
Compromised mailbox | Suspicius activity | Persistence | Credential Theft | Compromised account | Suspicius activity

ACTIVE

Activity time
First - Jul 03, 2018 9:26:18 AM
Last - Jul 03, 2018 9:28:54 AM

Duration
00H : 03M : 23S

Triggering alert	Investigation state	Investigated entities
Email reported as phishing	Remediated	cont-jonawolcot, Jonathan.wolcott@contoso
Suspicious PowerShell	Remediated	cont-jonawolcot
Golden ticket compromised	Running	JW Jonathan Wolcott
Spear-phishing attack	Remediated	cont-jonawolcot



Suspicious PowerShell

Remediated

Investigation details

Severity
Medium

Threats found
#Malwear

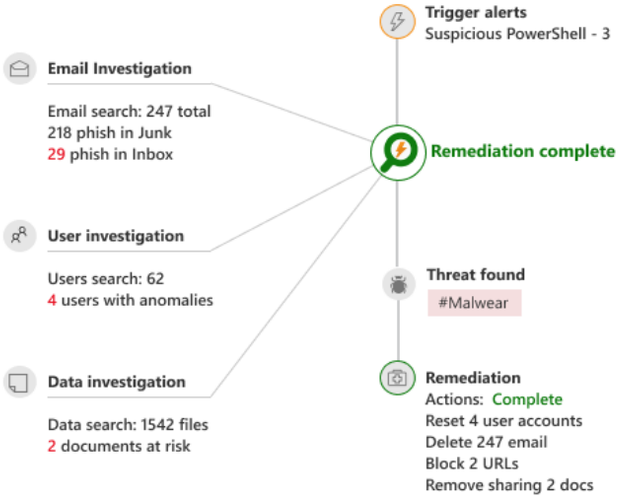
Status
Running

Category
Suspicious activity

First activity
Jul 03,2018 9:29:42 AM

Last activity
Jul 03,2018 9:32:42 AM

Investigation chart

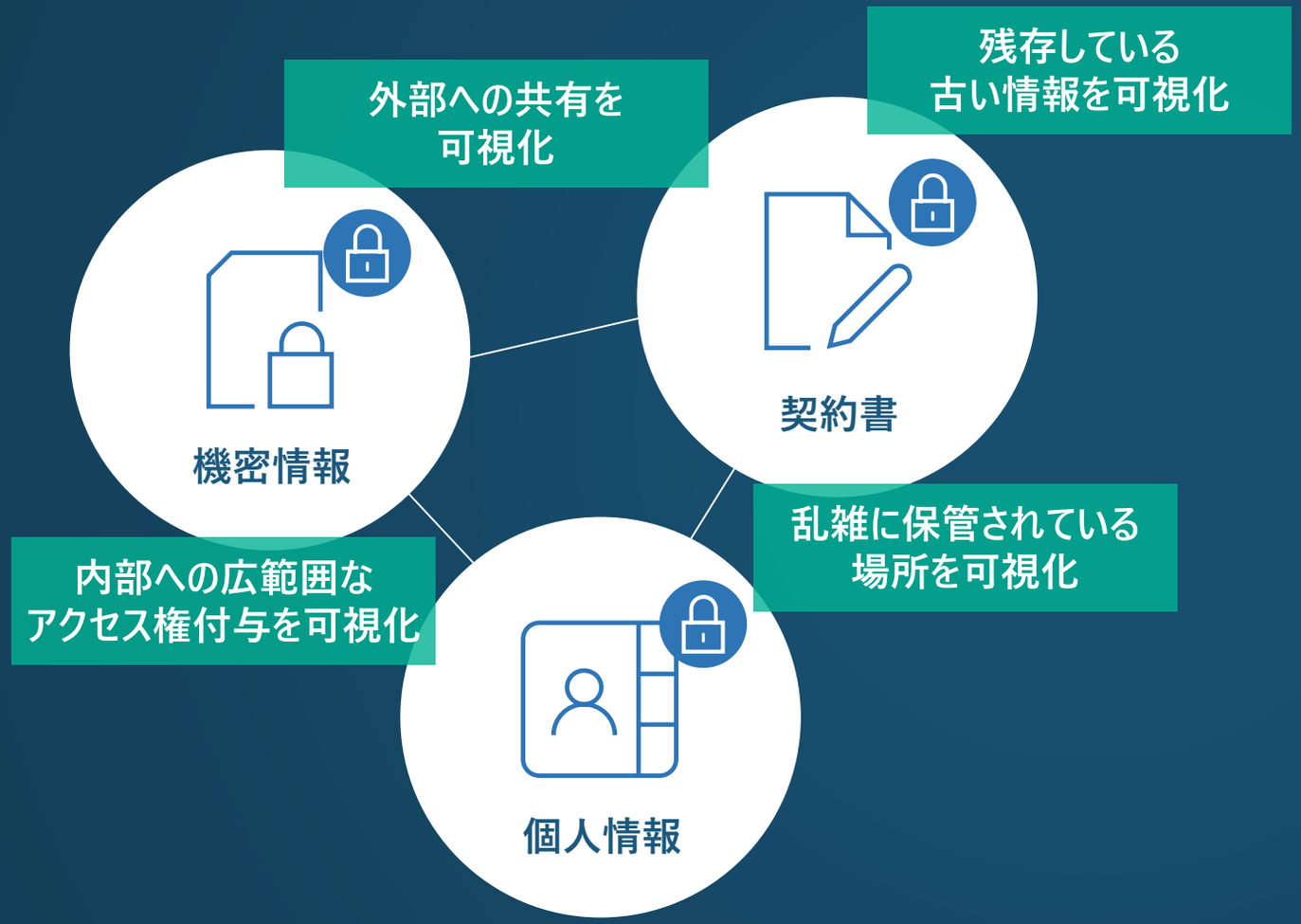


Open playbook log | Close

最短 2 週間!《限定 100 社》無料
脅威可視化アセスメントサービス

https://www.microsoft.com/ja-jp/biz/security/digital-trust-check.aspx

機密情報可視化アセスメントサービス



11月以降提供開始予定

Microsoft
DIGITAL TRUST
Summit 2019

株式会社NHKテクノロジーズ

穂積 律宇 様

2020 年に向けたサイバーセキュリティ戦略

株式会社NHKテクノロジーズ
穂積 律宇

NHK テクノロジーズのセキュリティ戦略・方針

経営理念：

“公共メディア”ＮＨＫを支える総合技術会社として、創造性に富む企業文化を構築するとともに、
多様な専門性と確かな技術力により社会に貢献します“

1 ＮＨＫへの貢献

ＮＨＫ業務を高度かつ効率的に担う役割を果たし、“公共メディア”ＮＨＫを支えます

2 ＮＨＫグループへの貢献

先進性や独自性を大切に、技術の変革・スピードを意識した対応で、ＮＨＫグループからの期待に応えます

3 社会への貢献

ＮＨＫグループとして期待される高度な専門性や技術力により、文化の創造と社会の発展に貢献します

高度な専門性が要求される情報セキュリティ強化により、公共メディアのITガバナンスを支える

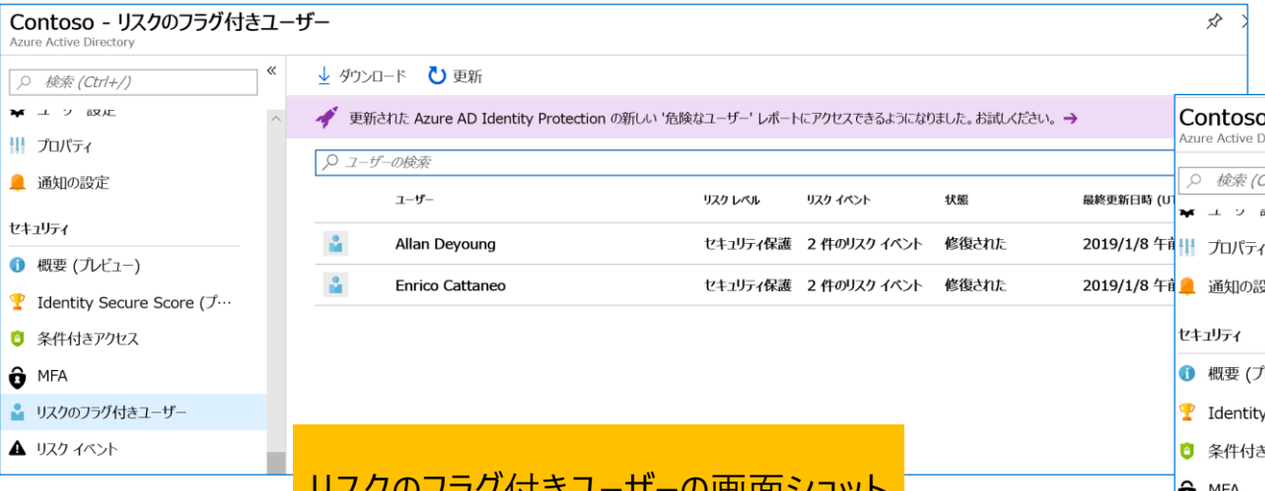
近年の被害動向を受け、マイクロソフトの脅威可視化アセスメントを実施

運用中の Office365 テナント上で、脅威の可視化を実施

① ID + パスワードがブラックマーケットに流出していた
② 大量のファイルがダウンロードされていた (正当な理由ではない可能性)

	結果	危険度
Office 365 振る舞い	大量のファイル削除アクティビティのみ Cyber Kill Chain の観点で、ID 盗用まで行われているため、データの監視は継続を推奨	中

	結果	危険度
ID/認証	以下の不正アクセスが成功されている状態 ・漏洩した資格情報からの不正アクセス ・接続元を偽装したアクセス (Tor ブラウザなど)	高



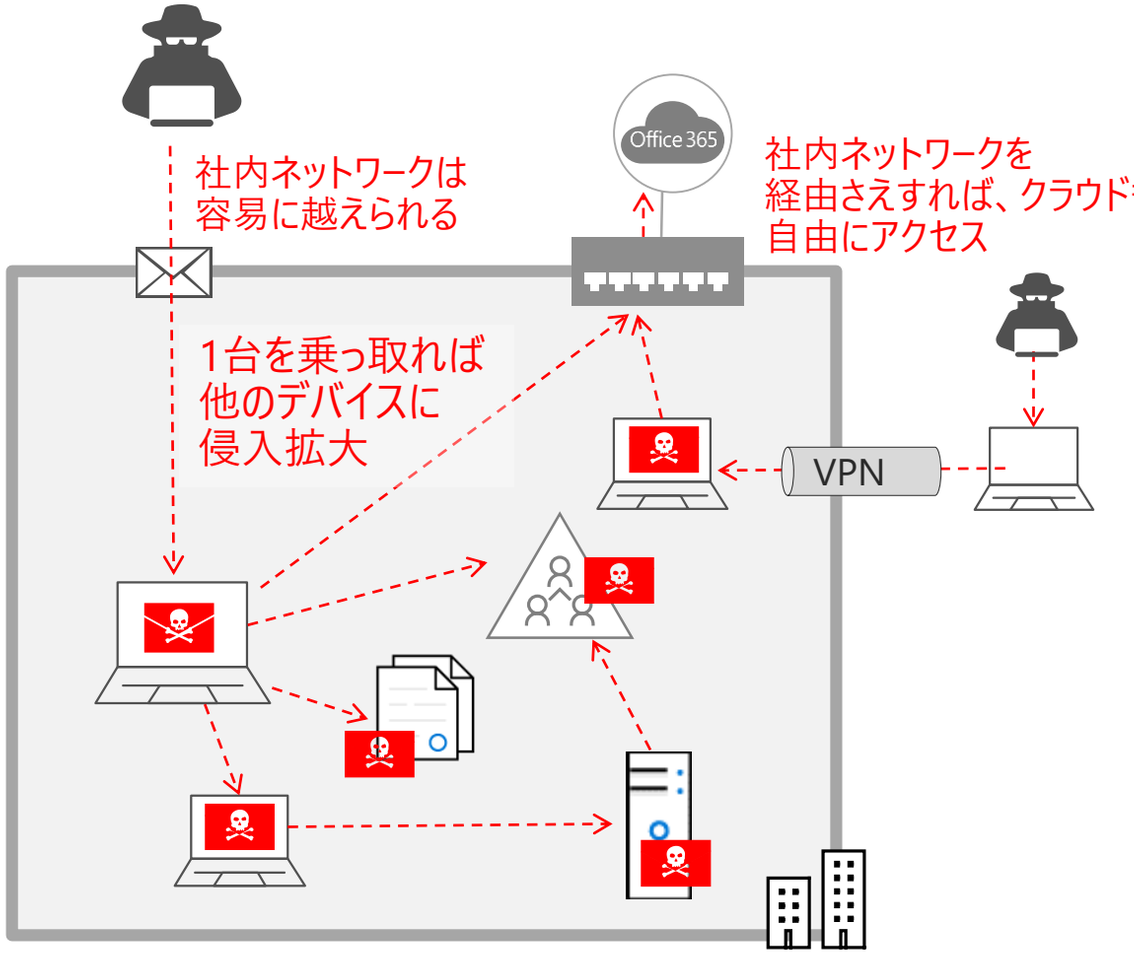
リスクのフラグ付きユーザーの画面ショット

リスク イベントの画面ショット

脅威可視化アセスメントの結果により、従来の対策の限界を認識

従来のセキュリティ対策は...

ネットワークを境界とした信頼モデル
= 侵入済みの脅威に対して脆弱

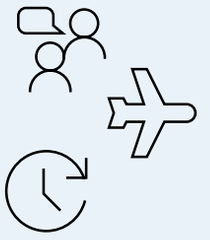


しかし!!

世界は会社の外で動いている

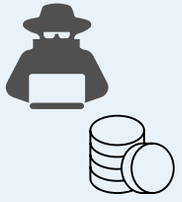
IT 環境の変化

- 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

ゼロトラストの考え方がもっともマッチ

Achieve Zero Trust with Azure AD conditional access
https://www.microsoft.com/en-ww/security/technology/identity-access-management/zero-trust

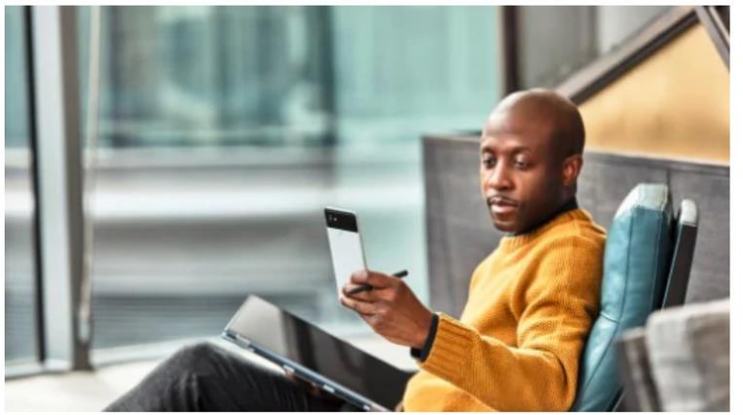
From perimeter security to Zero Trust

Establish identity as the control plane

Today, users work anywhere with multiple devices and apps. The only constant is user identity. That's why the first step to Zero Trust is making identity your security control plane.

Assume every resource is on the open internet

To ensure the security of your corporate data, the second step is to connect all your on-premises and cloud apps along with your user identities and their devices to the cloud.



Never trust—always verify

Finally, every access must be verified. Azure AD conditional access provides you the ability to verify identity, device, app, data, and risk signals before allowing access.

何をすべきか？

1. NHK グループにおけるテクノロジーリーダー企業として
グループ全体を脅威から守るためにできることは何か

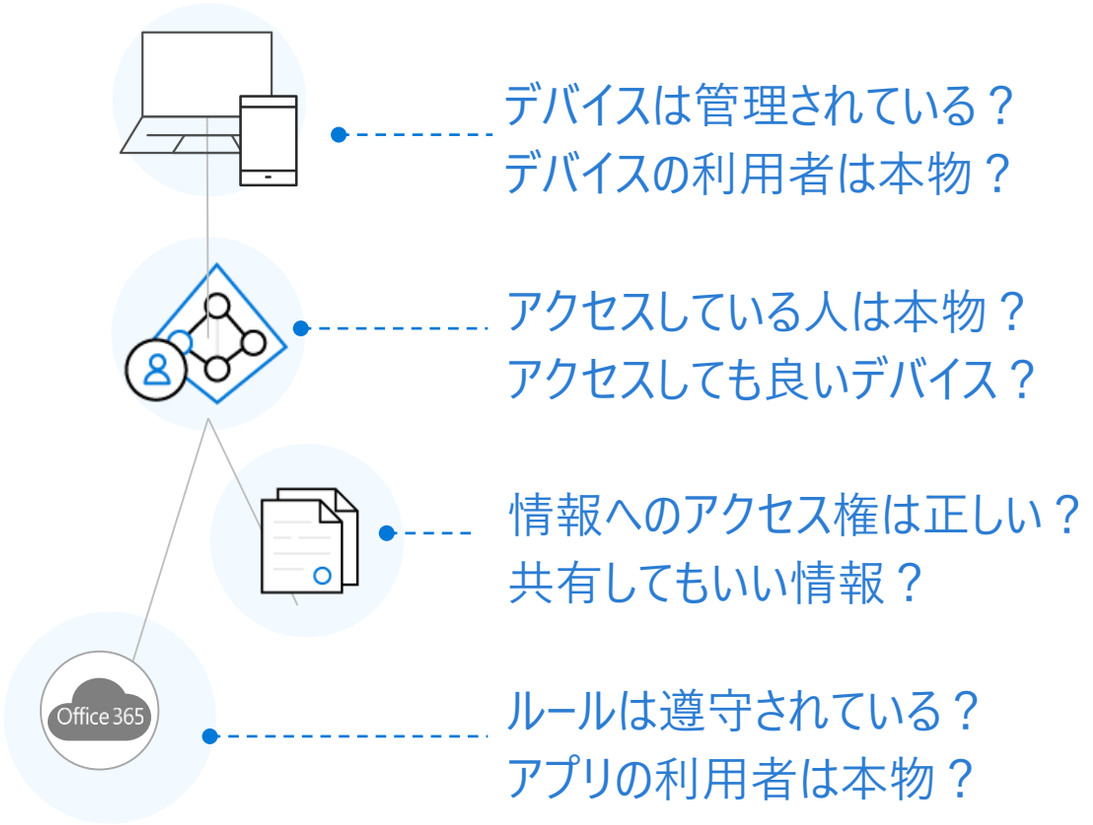
2. 2020 年に向けて
高まるサイバー攻撃リスク

3. 脅威可視化アセスメントで発覚した
既にサイバー攻撃を受けている事実

ゼロトラストを最も迅速に実現できる Microsoft 365 E5 の導入を決定

今後、必要とされる考え方

ゼロトラスト = 信頼しないモデル
信頼しないので、本物であることをイチイチ確認する



デバイスは管理されている？
デバイスの利用者は本物？

アクセスしている人は本物？
アクセスしても良いデバイス？

情報へのアクセス権は正しい？
共有してもいい情報？

ルールは遵守されている？
アプリの利用者は本物？

今後、必要とされる考え方

ゼロトラスト = 信頼しないモデル
信頼しないので、本物であることをイチイチ確認する

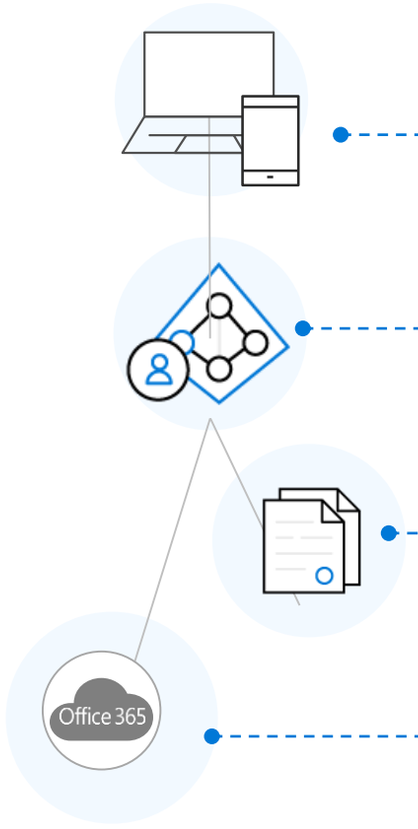
防御
- ☐ デバイスのセキュリテレベルを継続的に正しく維持する
- ☐ 不正な侵入を検出し拡大を阻止する

制御
- ☐ ID のなりすましを検出しアクセスを制限する
- ☐ セキュリティリスクの高いデバイスからのアクセスを防ぐ

保護
- ☐ 保存場所に依存せず、機密情報を分類して保護 (暗号化) する
- ☐ 内部からの情報漏洩を防ぐ

監視
- ☐ 機密情報の保存場所や公開範囲、アクセス状況を可視化する
- ☐ アプリに対する不正な操作を検出する

現状できていることをチェックし、今後の対策を検討



	現状できていることをチェック	必要な対策
防御	☑ デバイスのセキュリテレベルを継続的に正しく維持する ☐ 不正な侵入を検出し拡大を阻止する	➡ デバイスのセキュリティ管理 (モバイル) ➡ デバイスへの脅威検出と自動修復
制御	☐ ID のなりすましを検出しアクセスを制限する ☐ セキュリティリスクの高いデバイスからのアクセスを防ぐ	➡ リスクベース認証 ➡ 危険なデバイスのアクセス制限
保護	☐ 保存場所に依存せず、機密情報を分類して保護 (暗号化) する ☐ 内部からの情報漏洩を防ぐ	➡ ファイルの分類・保護 ➡ 機密情報の投稿や共有を防止
監視	☐ 機密情報の保存場所や公開範囲、アクセス状況を可視化する ☐ アプリに対する不正な操作を検出する	➡ 機密情報の可視化と自動修復 ➡ 内部・外部犯行の可視化と防止

現状できていることをチェックし、今後の対策を検討

➡ Microsoft 365 E5 の導入を決定

E5 に決定した理由：

- ゼロトラストの実現に必要なサービスがすべて含まれている
- コンセプトが共通している
(圧倒的な脅威情報から得る高度な脅威検出、対応の自動化)
- クラウドなので短期間で導入可能

必要な対策

Microsoft 365 E5 で対応可能

- ➡ デバイスのセキュリティ管理 (モバイル)
- ➡ デバイスへの脅威検出と自動修復
- ➡ リスクベース認証
- ➡ 危険なデバイスのアクセス制限
- ➡ ファイルの分類・保護
- ➡ 機密情報の投稿や共有を防止
- ➡ 機密情報の可視化と自動修復
- ➡ 内部・外部犯行の可視化と防止

＋

今後評価したい (Azure Sentinel)

- ➡ クラウド型 SIEM / SOAR (将来)

まとめ

- NHK グループにおけるテクノロジーリーダー企業として、セキュリティ分野においても、リーダシップを発揮する。

- 高度な専門性や技術力をもって、NHKグループのみならず、社会に貢献する。

NHK Technologies

DIGITAL TRUST

Summit 2019

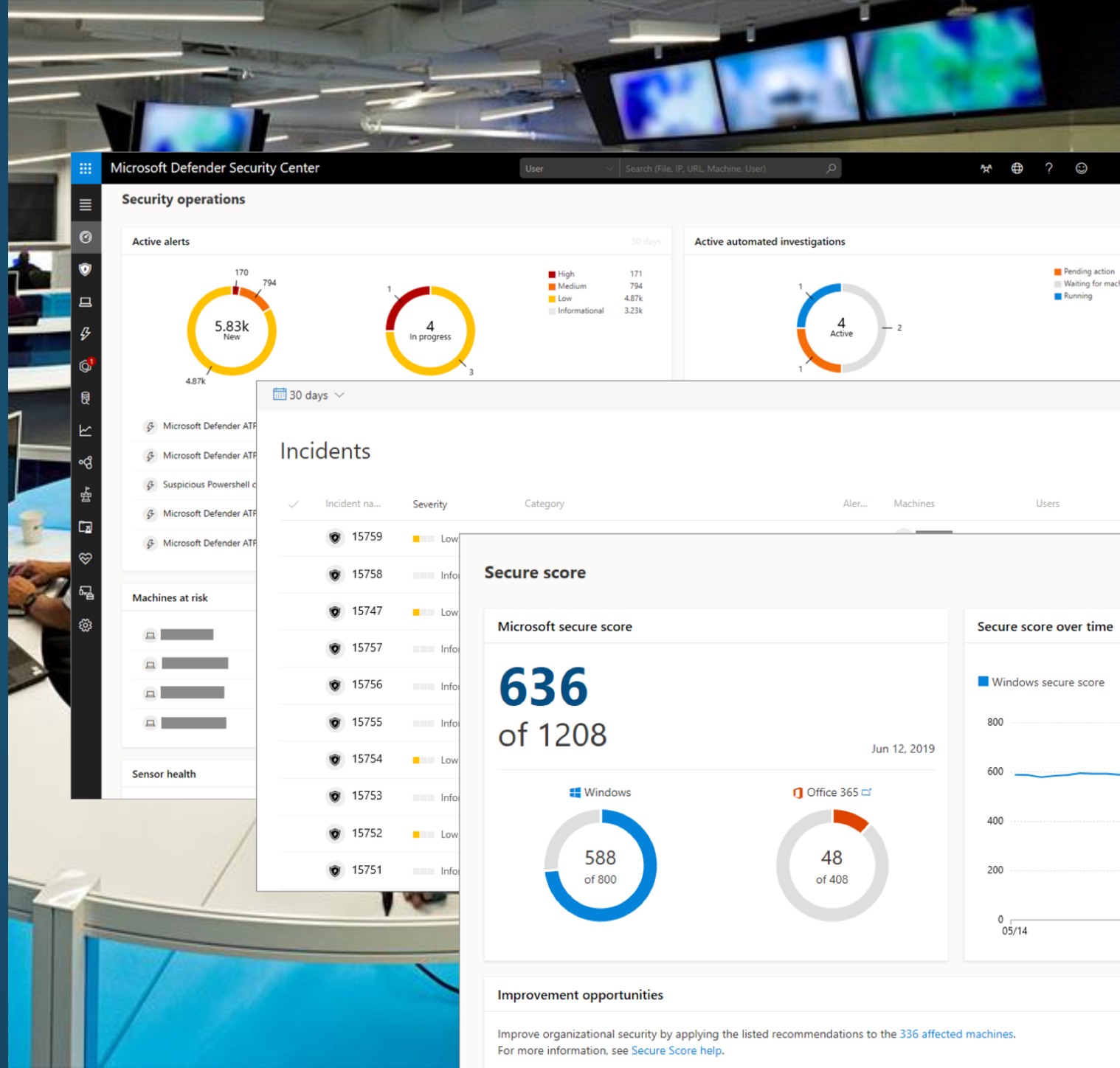
Microsoft

Demo:

Microsoft Defender Security Center

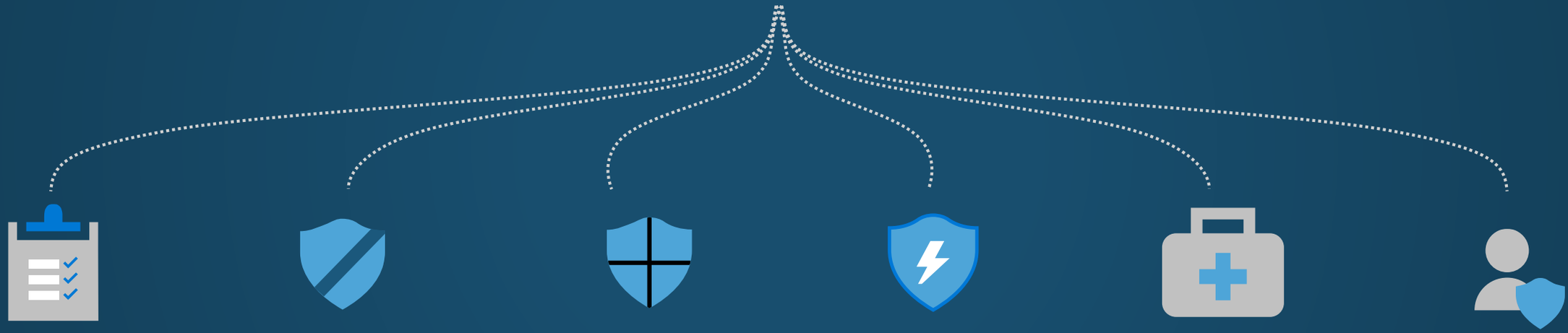
脅威と脆弱性の管理 (TVM)

DIGITAL TRUST Summit 2019



Microsoft Defender
Advanced Threat Protection

ビルトイン・クラウドパワー



脅威と脆弱性情報の管理

攻撃対象の削減

次世代保護

EDR

自動調査と修復

MICROSOFT
THREAT EXPERTS

設定と構成の集中管理、APIによる制御

DIGITAL TRUST

Summit 2019

IDベースの
統合型
セキュリティ

スケジュールされた
監査機能

脅威
インテリジェンス

データ
ガバナンス

APIを活用した
自動化ツール

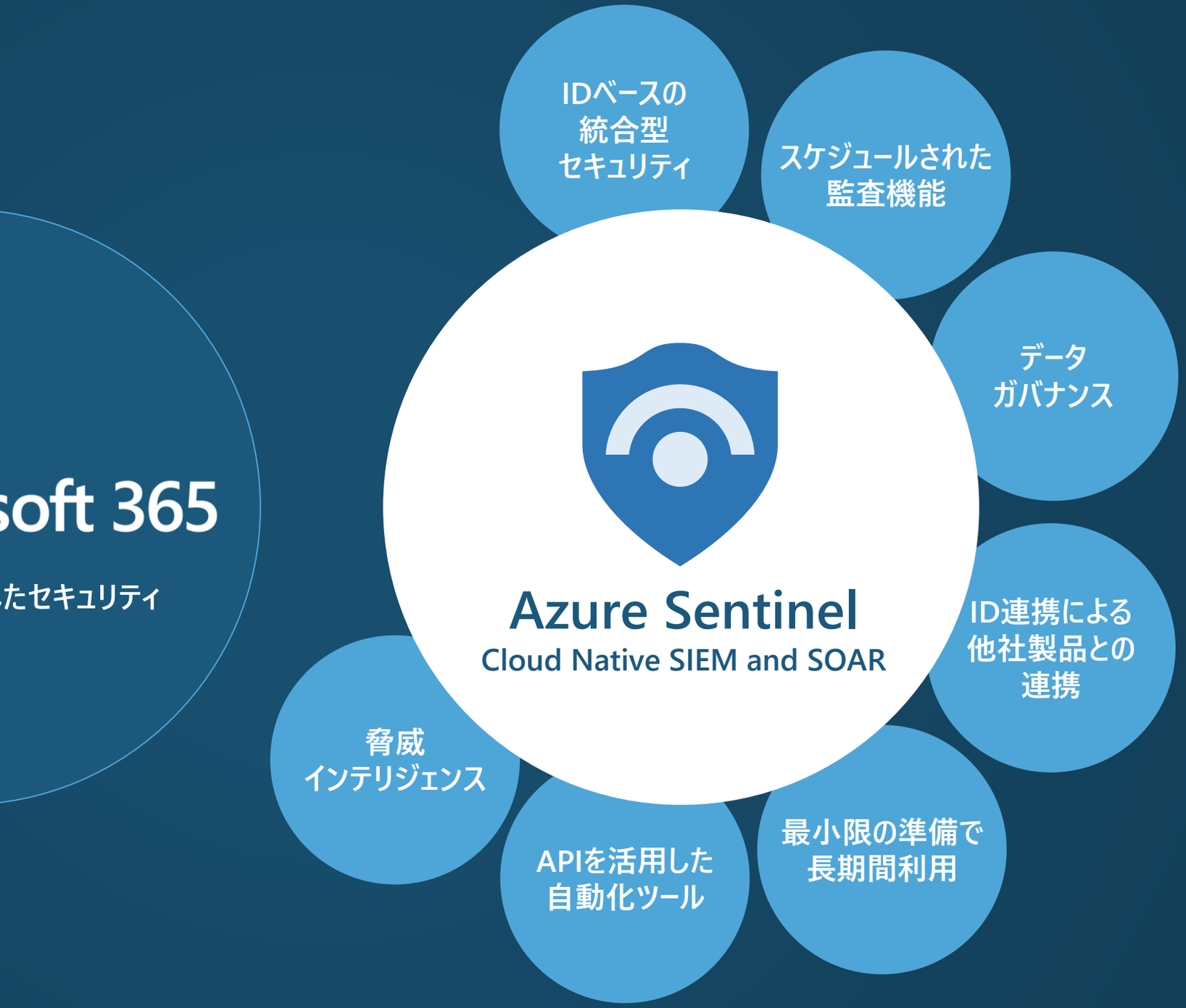
最小限の準備で
長期間利用

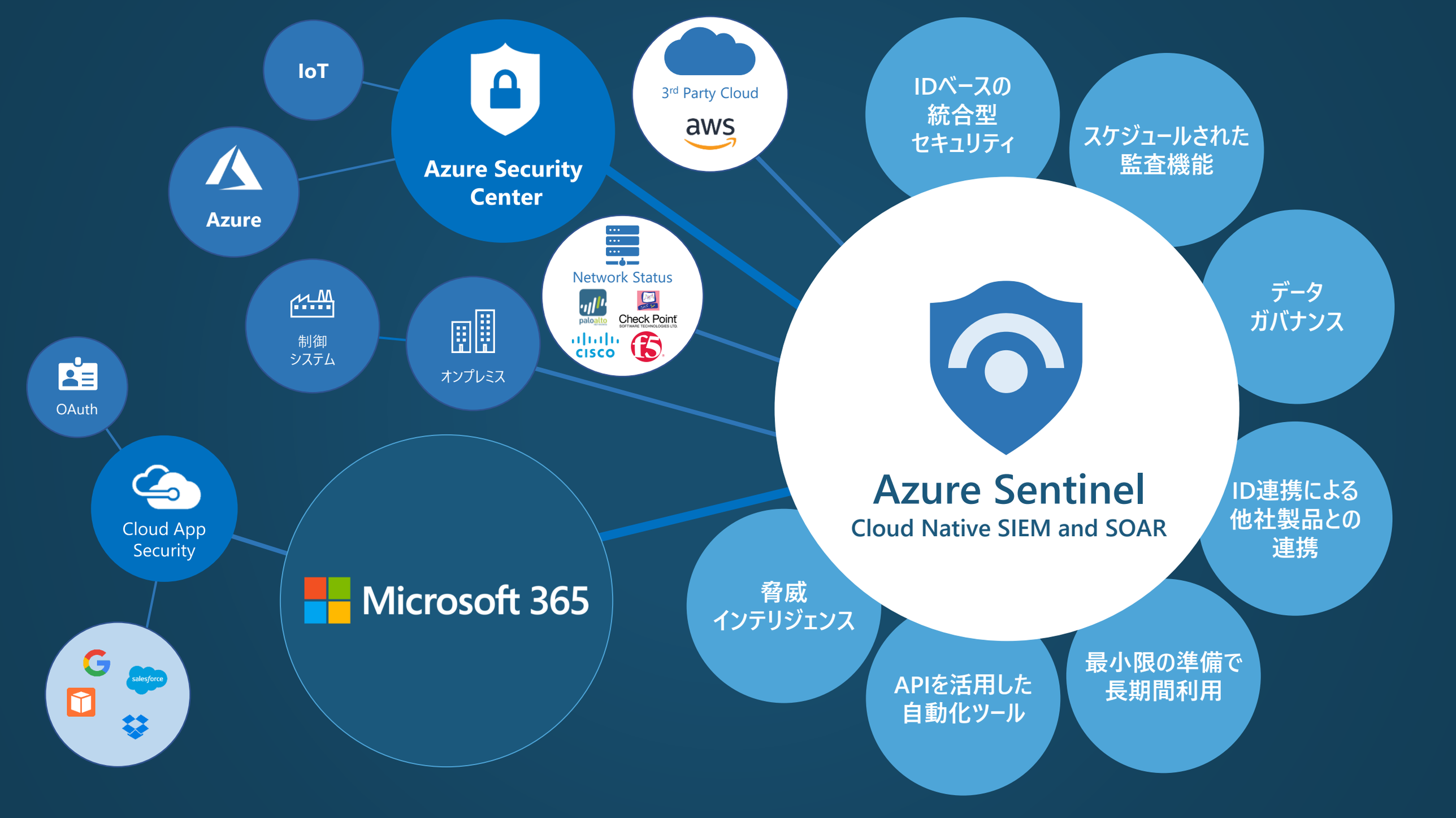
ID連携による
他社製品との
連携

Microsoft 365

シンプルで統合されたセキュリティ


Microsoft 365
シンプルで統合されたセキュリティ


IDベースの
統合型
セキュリティ
スケジュールされた
監査機能
データ
ガバナンス
ID連携による
他社製品との
連携
最小限の準備で
長期間利用
APIを活用した
自動化ツール
脅威
インテリジェンス
Azure Sentinel
Cloud Native SIEM and SOAR


IoT
Azure
Azure Security Center
3rd Party Cloud
aws
IDベースの
統合型
セキュリティ
スケジュールされた
監査機能
データ
ガバナンス
Network Status
paloalto
Check Point
SOFTWARE TECHNOLOGIES LTD.
cisco
f5
制御
システム
オンプレミス
OAuth
Cloud App
Security
Microsoft 365
Azure Sentinel
Cloud Native SIEM and SOAR
ID連携による
他社製品との
連携
脅威
インテリジェンス
APIを活用した
自動化ツール
最小限の準備で
長期間利用
salesforce

DIGITAL TRUST

Summit 2019

Microsoft
DIGITAL TRUST
Summit 2019

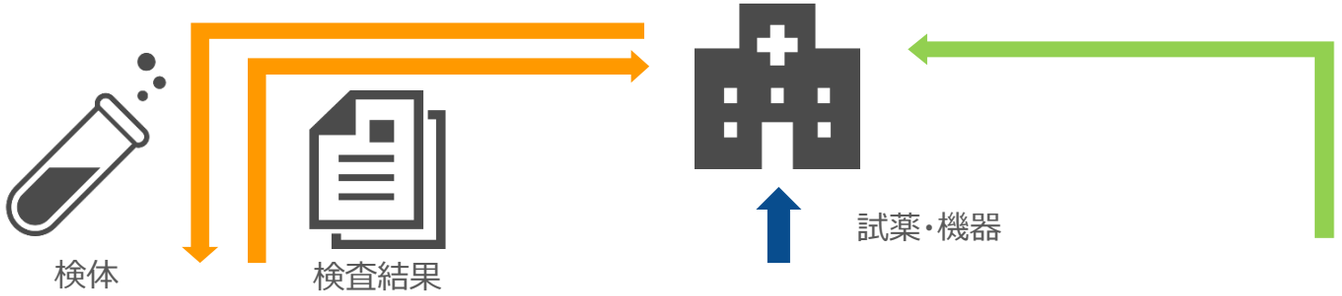
みらかホールディングス株式会社
ITインフラサービス部 部長
茂手木 達男 様

みらかホールディングス 会社概要

会社名	みらかホールディングス株式会社
設立	1950年12月18日 (2005年7月1日(旧)富士レビオ株式会社より社名変更、会社分割により持株会社化)
本店所在地	東京都新宿区
代表者	代表執行役社長兼グループCEO竹内成和
資本金	9,113百万円(2019年3月末現在)
経営体制	指名委員会等設置会社

- 2016年10月に代表執行役社長が交代(エンタテインメント業界出身)
- 2017年度を「第2の創業」と位置付け、グループ全体の変革を推進

みらかグループの事業



臨床検査の受託サービス事業

臨床検査に使用する
試薬・機器の製造販売事業

滅菌等の医療関連サービス事業
（医療行為を除く）

受託臨床検査事業

SRL Communication for Health 株式会社 エスアールエル

臨床検査薬事業

富士レビオ株式会社

滅菌関連事業

NS Nihon Stery 日本ステリ株式会社

新規育成事業

食品・環境・
化粧品検査

在宅・福祉用具

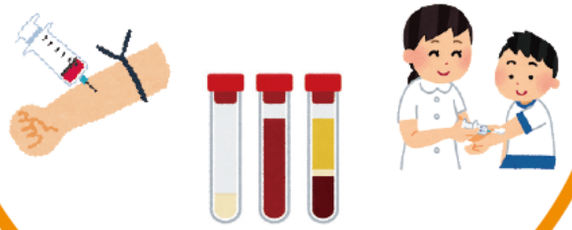
CRO

セルフメディケーション・
健保ビジネス

「検体検査」はこんな形で役に立っています

検体検査では患者さまの
血液や尿などを調べます

臨床検査って
（検体検査）
何に役立つの？



Miraca
みらかグループ

正しい診断

ポイント!!

自分がどんな病気なのかが分かります。

治療と薬

ポイント!!

自分に合った治療や投薬が可能になります。

健康診断

ポイント!!

病気の早期発見が可能になります。

手術

ポイント!!

術後の確認や再発の早期発見が可能になります。

みらかグループが提供するサービスは、
（実は・・）皆さんの生活の近くにいます。

ITインフラサービス部のミッション

◆ **サービス対象：2019年10月現在**

- みらかグループ国内20社以上
- 約120拠点
- 約8,000ユーザー

◆ **目的：ITインフラ環境を統合しグループ内に以下の事業価値を提供する**

- **統一されたセキュリティ環境**
- 環境集約によるコスト削減
- どの拠点でも通常通りの業務ができる環境

我々の取り組み

◆ **経験や知識による変革設計**

- 現状調査
- 新IT標準・制度の設計

環境構築

＋

◆ **マンパワーによる変革導入**

- 新規運用のスタート
- 既存環境の廃止

環境集約

新しいIT風土

◆ **変革に対応できるIT環境**

- 組織目標の共有
- 付加価値の提供
- 自己啓発

気持ちの変革の後押し！

これまでのインフラ統合計画

2017年度				2018年度				2019年度			
1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q

- シェアードIT組織開始
- Microsoft 365 E3 7,000 ユーザーに展開開始
- Microsoft 365 E5 Security 9,000 ユーザーに展開開始
- **Azure Sentinel 検討・導入**
- DC運用設計、500台DC移設計画、500台オンプレサーバ運用統合、新規サーバ構築
- 国内グループ120拠点のネットワーク統合と無線化
- グループ標準PC MeW 配布 6,800台

みらか統合ITインフラ環境

Azure Sentinel の導入背景

ログの統合基盤およびセキュリティチームの運用効率実現に向けて Azure Sentinel を採用

課題

- IT 基盤のログ統合の実装
- ログの相関分析の実装

Azure Sentinel の優位性

低コストでログの一元管理が可能

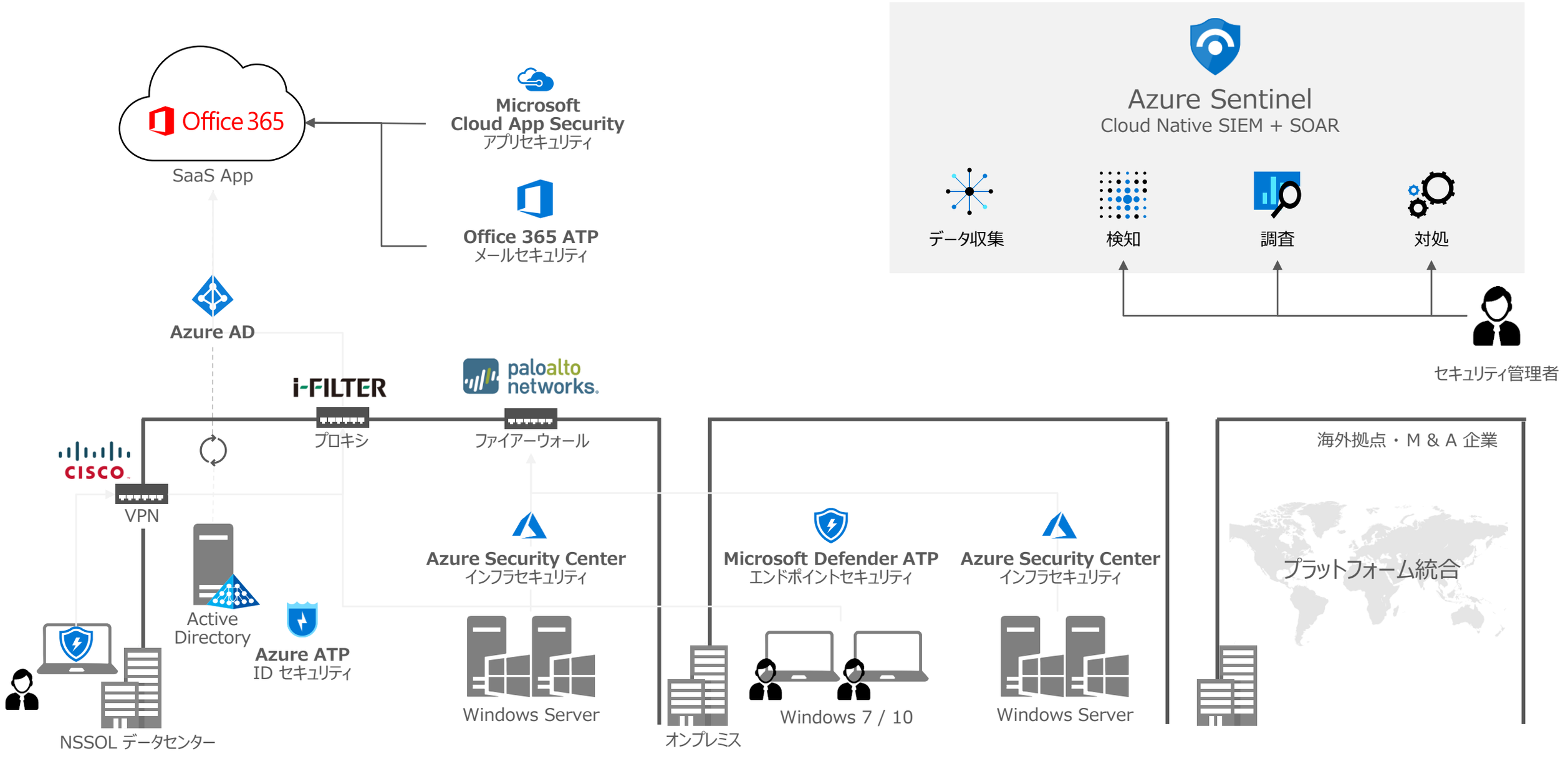
導入から運用するまでのスピードが早い

マイクロソフトの脅威インテリジェンスを活用可能

外部委託がしやすい

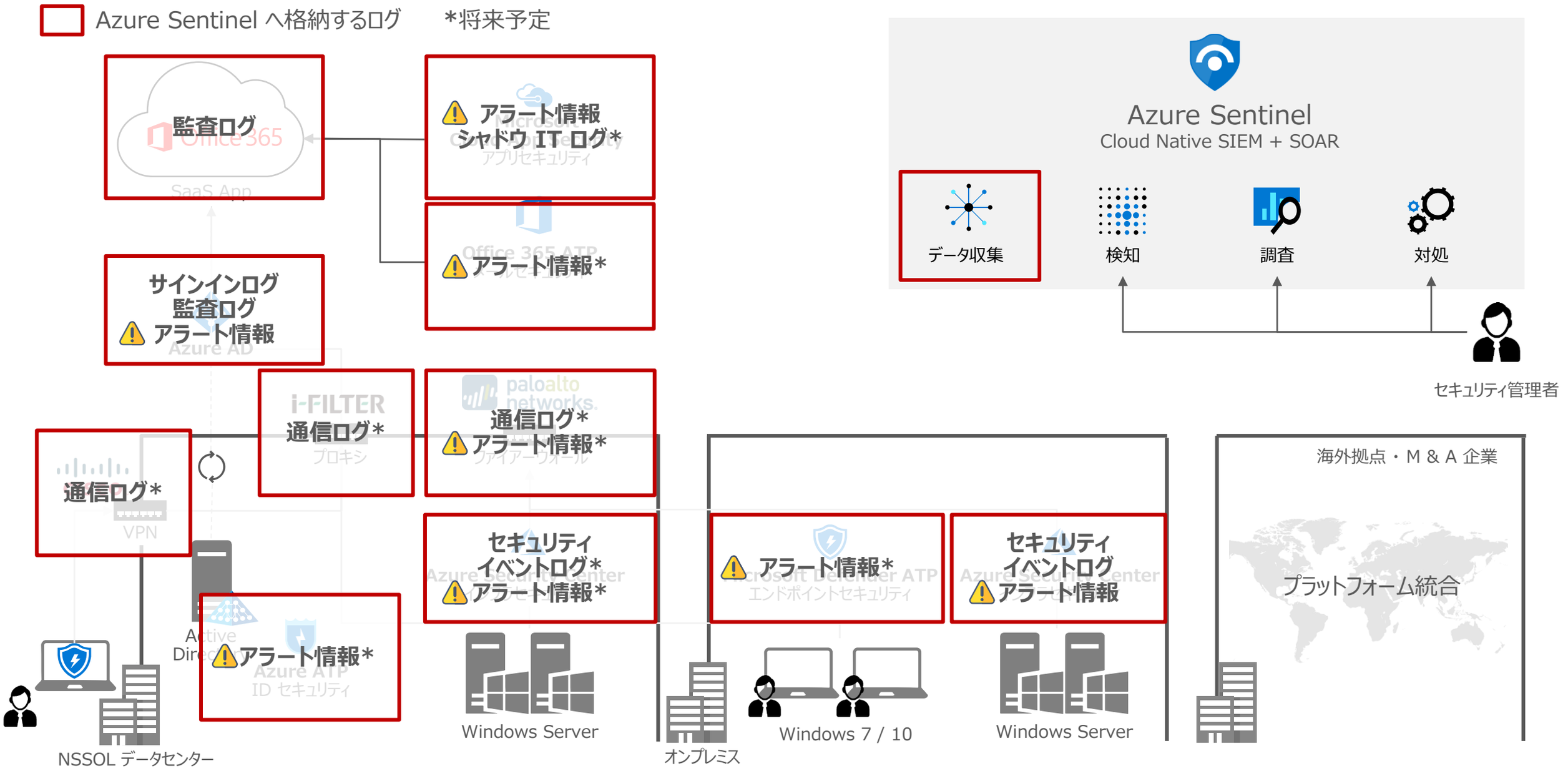
容易な脅威の調査 & 対処

アーキテクチャ図


Office 365
SaaS App
Microsoft
Cloud App Security
アプリセキュリティ
Office 365 ATP
メールセキュリティ
Azure Sentinel
Cloud Native SIEM + SOAR
データ収集
検知
調査
対処
セキュリティ管理者
Azure AD
i-FILTER
paloalto networks.
プロキシ
ファイアーウォール
CISCO
VPN
Active Directory
Azure ATP
ID セキュリティ
Azure Security Center
インフラセキュリティ
Microsoft Defender ATP
エンドポイントセキュリティ
Azure Security Center
インフラセキュリティ
海外拠点・M & A 企業
プラットフォーム統合
Windows Server
Windows 7 / 10
Windows Server
NSSOL データセンター
オンプレミス

アーキテクチャ図

Azure Sentinel へ格納するログ　　*将来予定




Miraca

DIGITAL TRUST

Summit 2019

Microsoft

Demo:

Microsoft Azure Sentinel

Cloud native SIEM and SOAR

DIGITAL TRUST
Summit 2019

DIGITAL TRUST

Summit 2019

Microsoft Graph を活用した開発の一元化

https://graph.microsoft.com

全てのものに

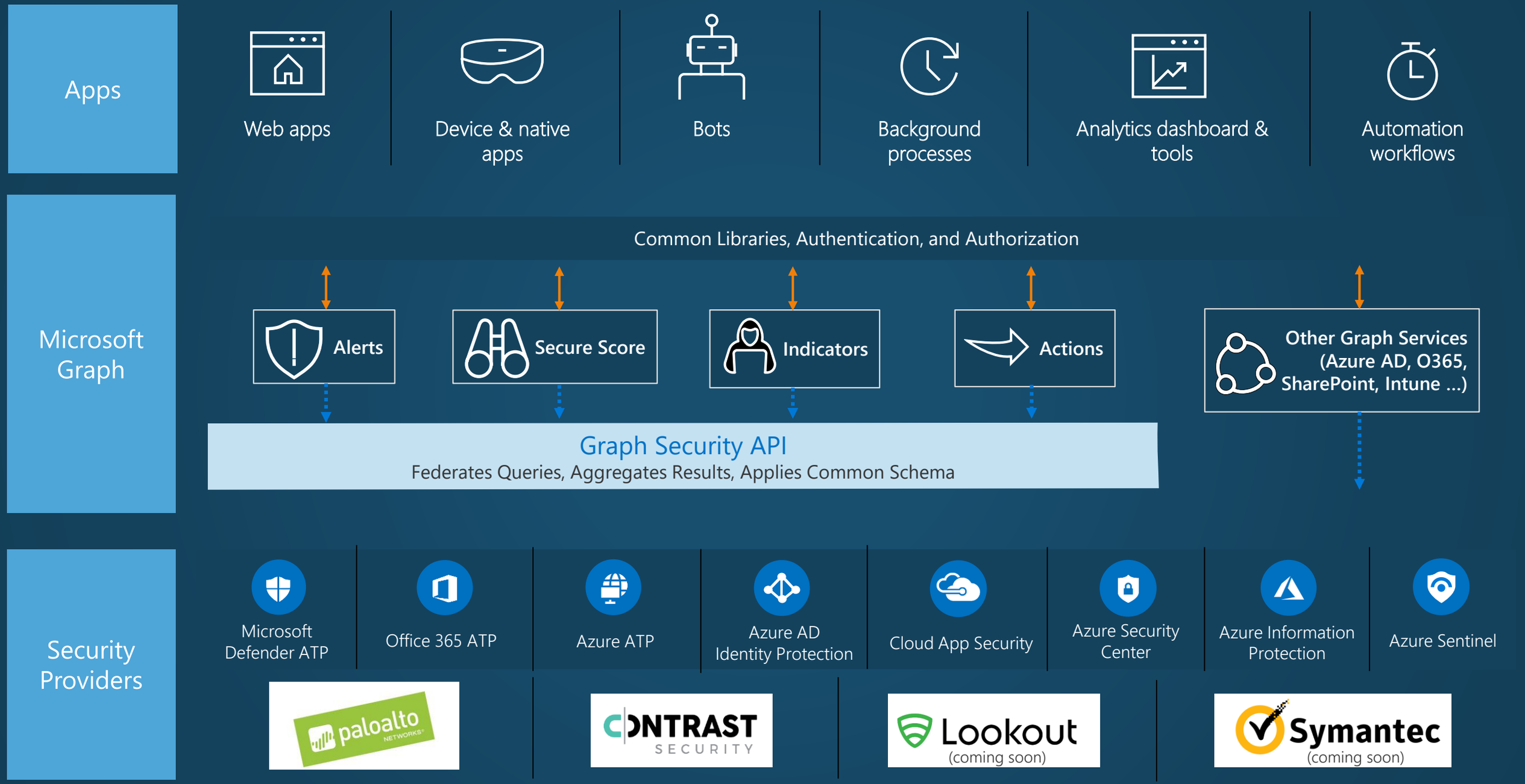
ユーザと組織のデータ

- Microsoft 365
- Azure
- Microsoft Partners

一つのインタフェースで

アクセスできる

- 一つのエンドポイントから
- 1つの認証キーで全てにアクセス
- 共通のSDKで開発できる


Apps
Web apps
Device & native apps
Bots
Background processes
Analytics dashboard & tools
Automation workflows
Microsoft Graph
Common Libraries, Authentication, and Authorization
Alerts
Secure Score
Indicators
Actions
Other Graph Services (Azure AD, O365, SharePoint, Intune ...)
Graph Security API
Federates Queries, Aggregates Results, Applies Common Schema
Security Providers
Microsoft Defender ATP
Office 365 ATP
Azure ATP
Azure AD Identity Protection
Cloud App Security
Azure Security Center
Azure Information Protection
Azure Sentinel
paloalto NETWORKS
CONTRAST SECURITY
Lookout (coming soon)
Symantec (coming soon)


Microsoft
Digital Trust
Security Alliance


NTT Communications

KPMG

SB Technology

JBS

PERSOL
パーソル プロセス＆テクノロジー

FUJITSU

M B S D

LAC

Microsoft
Digital Trust
Security Alliance

EY
Building a better working world

isr

isao

株式会社 大塚商会

クラウドネイティブ
CLOUD NATIVE INC.

GSX
GLOBAL SECURITY EXPERTS

KDDI

KDDI
KDDI まとめてオフィス

CompTIA

SYNNEX
JAPAN

SOFT CREATE

Sophia Network

TIS
TIS INTEC Group

DIS
ダイワボウ情報システム株式会社

DXC.technology

TOSYS

"Your Best Partner"
NISSHO ELECTRONICS

NS Solutions
NIPPON STEEL

PSC

BBSystem
Big Bang System Corporation

FUJISOFT

yubico

YOKOGAWA
横河レンタ・リース株式会社

Microsoft Digital Trust Security Alliance

5000人
ユーザー向けセキュリティ
勉強会実施予定

50社
パートナ設立

5000人
学生向けセキュリティ
教育実施予定


Microsoft
DIGITAL TRUST
Summit 2019
Microsoft