Microsoft
DIGITAL TRUST
Summit 2019

#digitaltrust

B-1

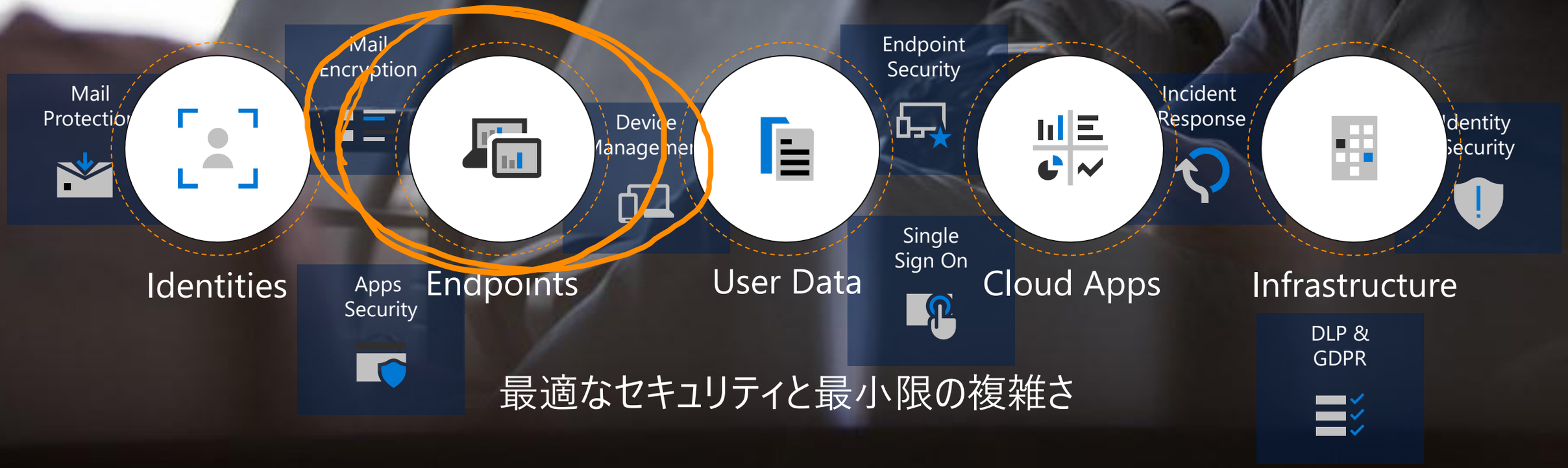
エンドポイントの保護に Windows Defender を検討すべき 5 つの理由

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
太田 卓也, CISSP

Microsoft

Microsoft Threat Protection solves your challenges

今のセキュリティ製品は多数あり、まとめるのが困難で複雑です。



最適なセキュリティと最小限の複雑さ

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

Microsoft Threat Experts

Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt

MSSP

Cloud App Security

Azure Security Center

Microsoft Defender

Office 365

Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Information Protection

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score

Threat Analytics

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

Extranet

NGFW

Edge DLP

SSL Proxy

IPS/IDS

Azure Firewall

Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs

Azure Stack

VMs

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Application & Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

Intelligent Security Graph

Microsoft

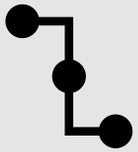
Windows Defender を検討すべき理由

Trust - 信頼

Technology - 技術

Operation - 運用

Connection - 連携



どんな基準でセキュリティ製品を選んでいますか？

理由その 1
パートナーとしての信頼性

CYBERscape: The Cybersecurity Landscape

The Security Sector Is Dynamic And Vast. We Are Ceaseless & Vigilant In Our Coverage.

セキュリティ製品は一年半で勝負がつく

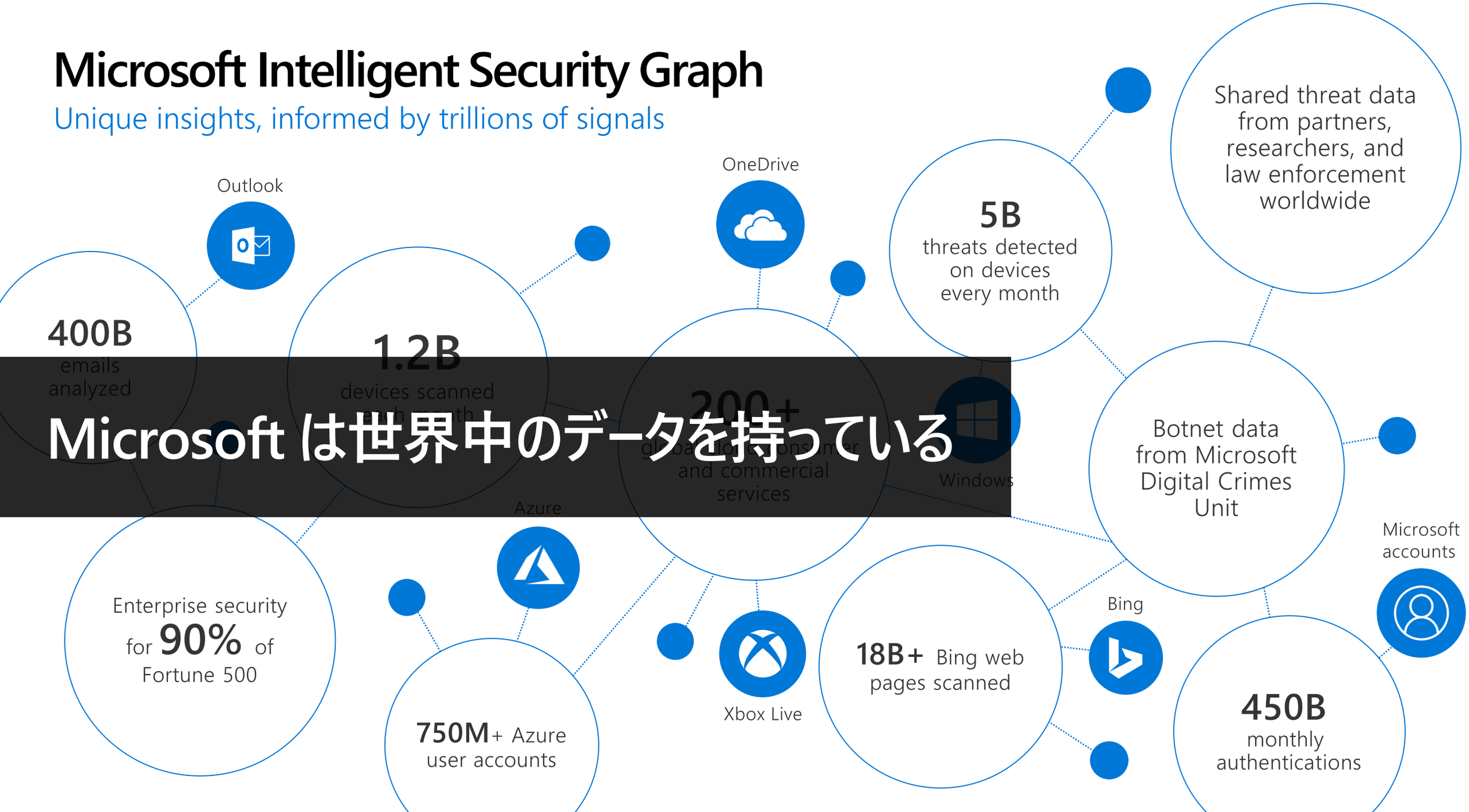
Source: Momentum Partners.

Cybersecurity is the #1 priority

Microsoft は毎年 1000 億円を
セキュリティに投資しています。

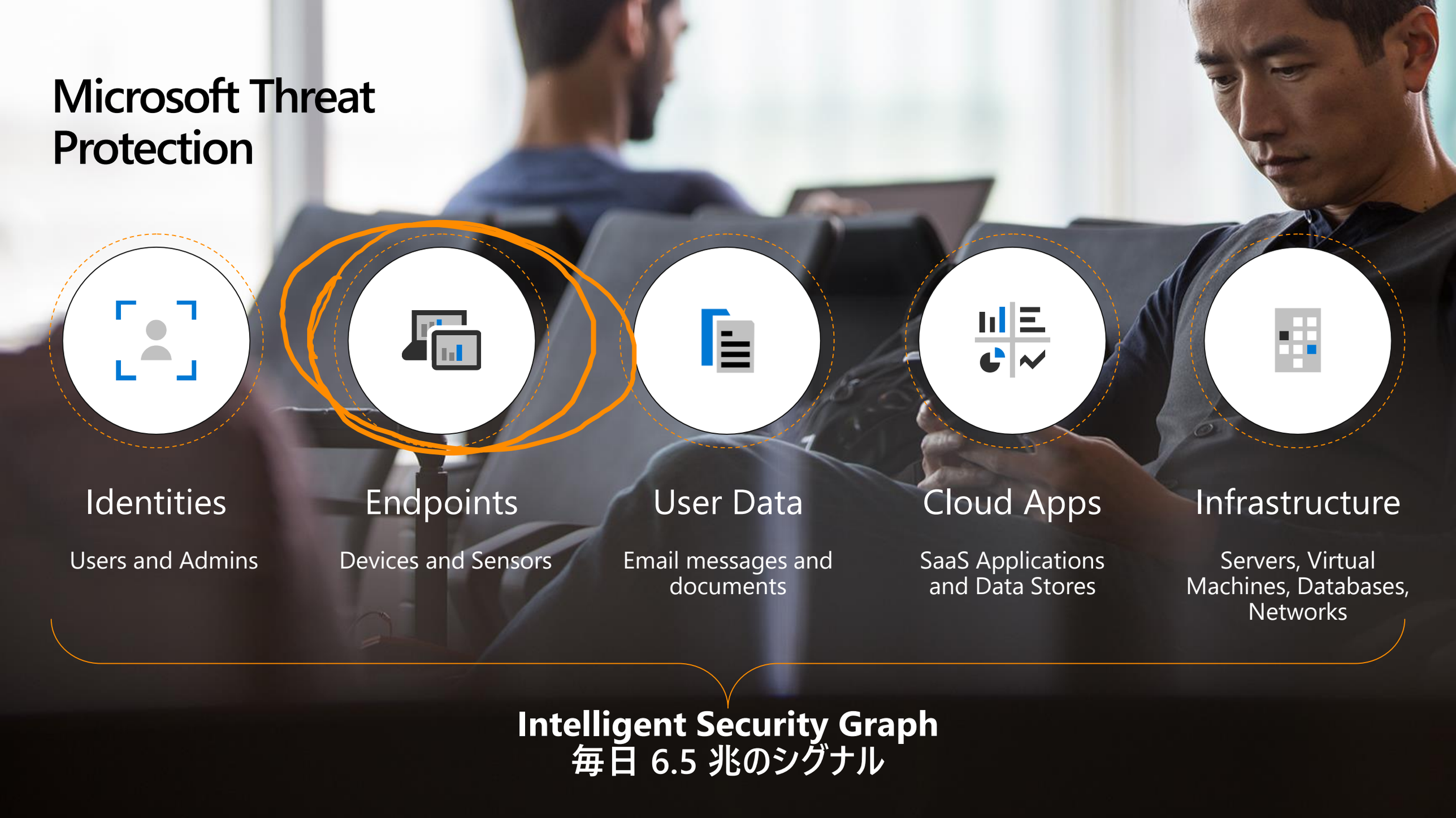
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Microsoft は世界中のデータを持っている

Microsoft Threat Protection



Identities

Users and Admins

Endpoints

Devices and Sensors

User Data

Email messages and documents

Cloud Apps

SaaS Applications and Data Stores

Infrastructure

Servers, Virtual Machines, Databases, Networks

Intelligent Security Graph
毎日 6.5 兆のシグナル

Microsoft / Story Labs

Windows 10

世界で

9 億台

Windows Defender ウイルス対策

法人だけでも

50%+

August 23, 2019

Gartner names Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant

Rob Lefferts Corporate Vice President, Microsoft Security

2019 年 ガートナー マジック クアドラント エンドポイント保護プラットフォーム部門「リーダー」評価を獲得

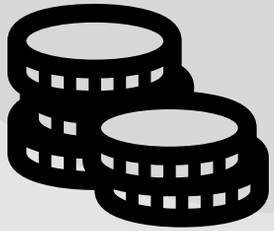
customers leading endpoint protection so they can defend against increasingly sophisticated attacks across a variety of devices, which is why we are so proud to have placed in the Leaders quadrant for this year's 2019 Gartner EPP Magic Quadrant and positioned highest in execution!

management capabilities for large enterprise accounts." Our latest product offerings prove that we've risen to the challenge that today's threat landscape presents. This achievement represents our ability to provide best-in-class protection and deliver on innovations that learn and evolve just as attackers change their tactics.

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Windows Defender を検討すべき理由その 1



莫大な投資

豊富なデータ

トップの評価

パートナーとしての信頼性

Windows Defender を検討すべき理由

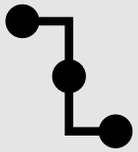
Trust - 信頼

パートナーとしての信頼性

Technology - 技術

Operation - 運用

Connection - 連携




PC にセキュリティ製品は
何製品くらい入れていますか？

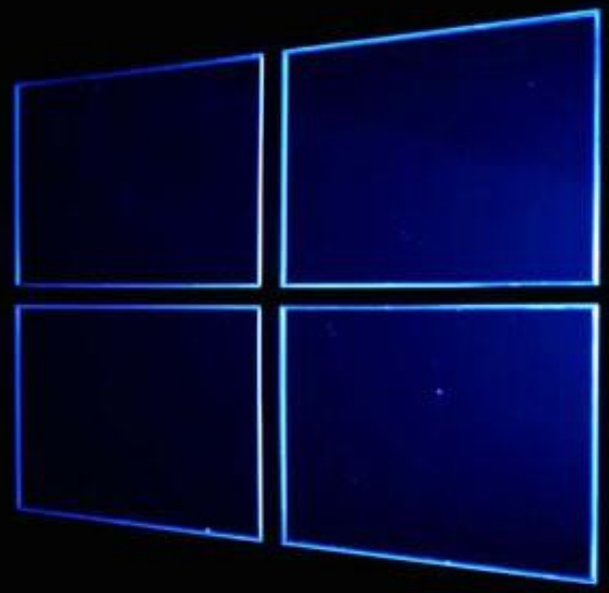
エンドポイントの多層防御

Enterprise E3
Enterprise E5

必要な対策例	とある構成例	Windows 10
不審な挙動の検知 (EDR for IOA)	- なし –	Windows Defender ATP
高度な攻撃の検知 (EDR for IOC)	C 社	Windows Defender ATP
脆弱性/マクロ悪用対策/ ネットワーク保護	- なし -	Windows Defender Exploit Guard
未知のマルウェア検知 (CI)	B 社	Windows Defender ウイルス対策 Windows Defender Smart Screen
既知のマルウェア検知 (Antivirus Scan)	A 社	Windows Defender ウイルス対策
資格情報の保護	- なし -	Windows Defender Credential Guard
HDD 暗号化	D 社	BitLocker
ブートレコード保護	- なし -	Windows Defender Device Guard

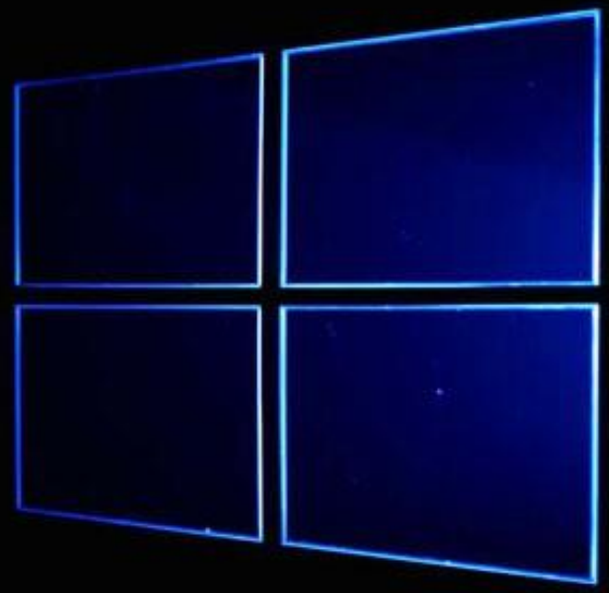
Windows 搭載機能で守れるようになった！

理由その 2
OS を作っている会社の
OS を守るための技術



Windows Defender はシリーズに！

Windows Defender ウイルス対策	Windows Defender Device Guard
Windows Defender ファイアウォール	Windows Defender Application Control
Windows Defender SmartScreen	Windows Defender Credential Guard
Windows Defender Exploit Guard	Windows Defender Application Guard
Windows Defender System Guard	Microsoft Defender ATP



最新のクラウド型セキュリティ
Microsoft Defender ATP

Windows E5
ライセンス

＋

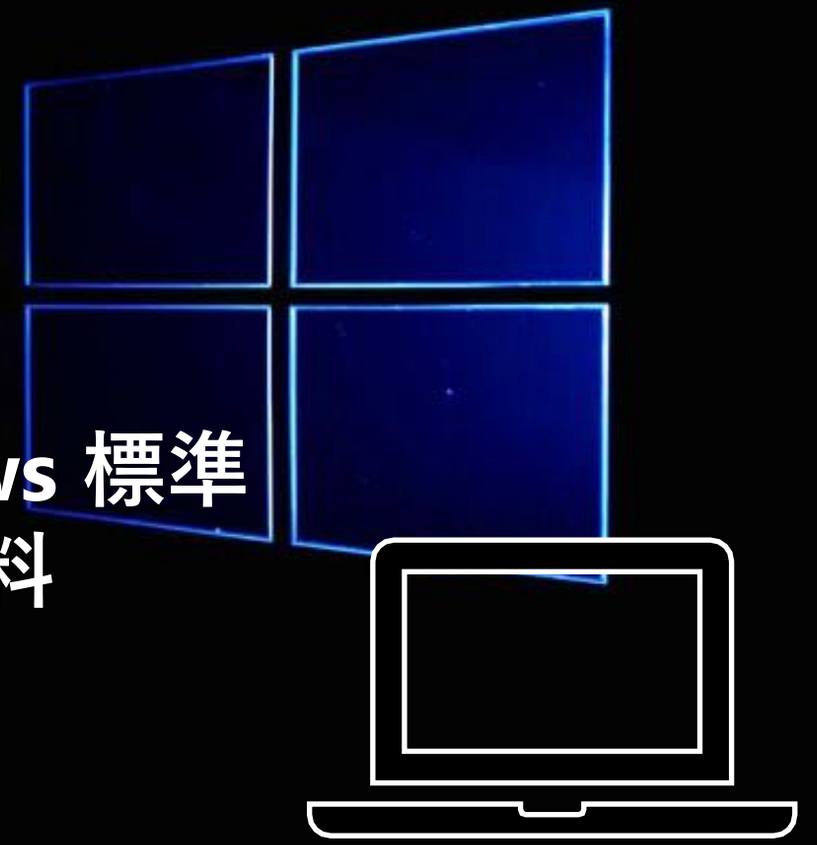
ウイルス対策
Windows Defender AV

ファイアーウォール
Windows ファイアウォール

Web セキュリティ
SmartScreen

ハードディスク 暗号化
BitLocker

Windows 標準
無料



ウイルス対策
Windows Defender AV

＋

最新のクラウド型セキュリティ
Microsoft Defender ATP

Windows Defender AV (ウイルス対策)

OS 標準の無料のウイルス対策ソフト

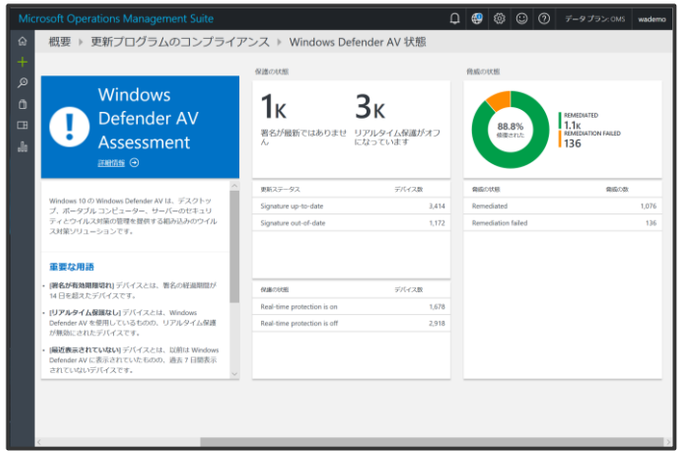
高度な機械学習による検知

クラウド型保護機能も搭載

Windows 10 に標準・無料

Defender ウイルス対策は性能が良くて無料
ただし企業向けの監視は有償ソリューションが必要

Microsoft Defender ウイルス対策
レポートや通知のソリューション



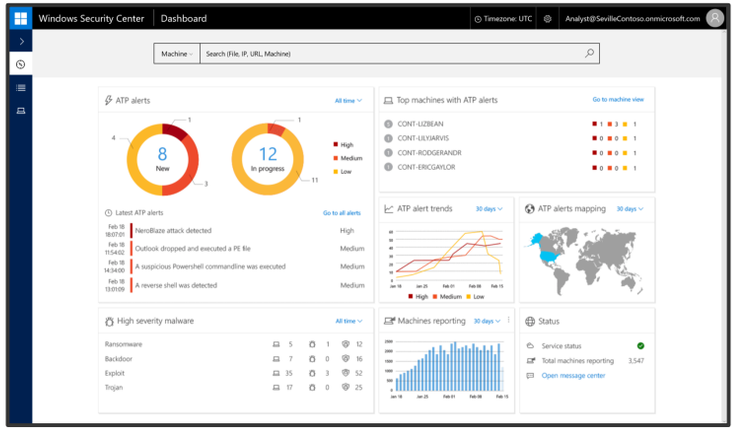
Update Compliance

メリット

Windows E3 ライセンス
クラウド サービス

注意点

レポートのみ
アラート通知不可



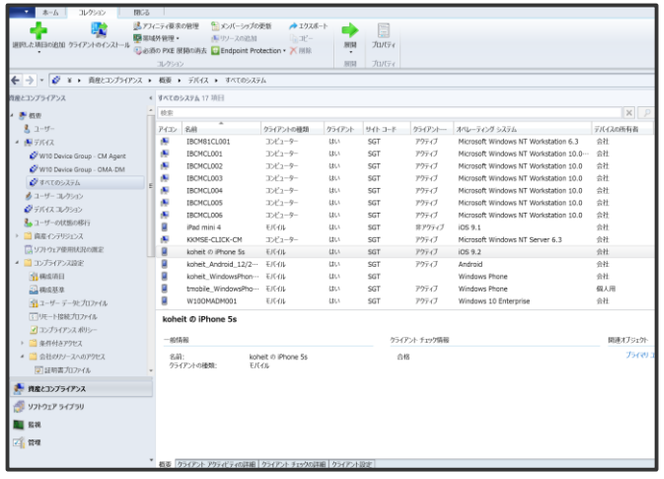
Windows Defender ATP

メリット

セキュリティ統合監視
クラウド サービス
アラート通知

注意点

ライセンスコスト



SCCM

メリット

クライアント統合管理
アラート通知

注意点

インフラの構築
ライセンス・運用コスト

ウイルス対策
Windows Defender AV

＋

最新のクラウド型セキュリティ
Microsoft Defender ATP

セキュリティ ゲート

Windows Defender AV

監視モニター

Microsoft Defender ATP

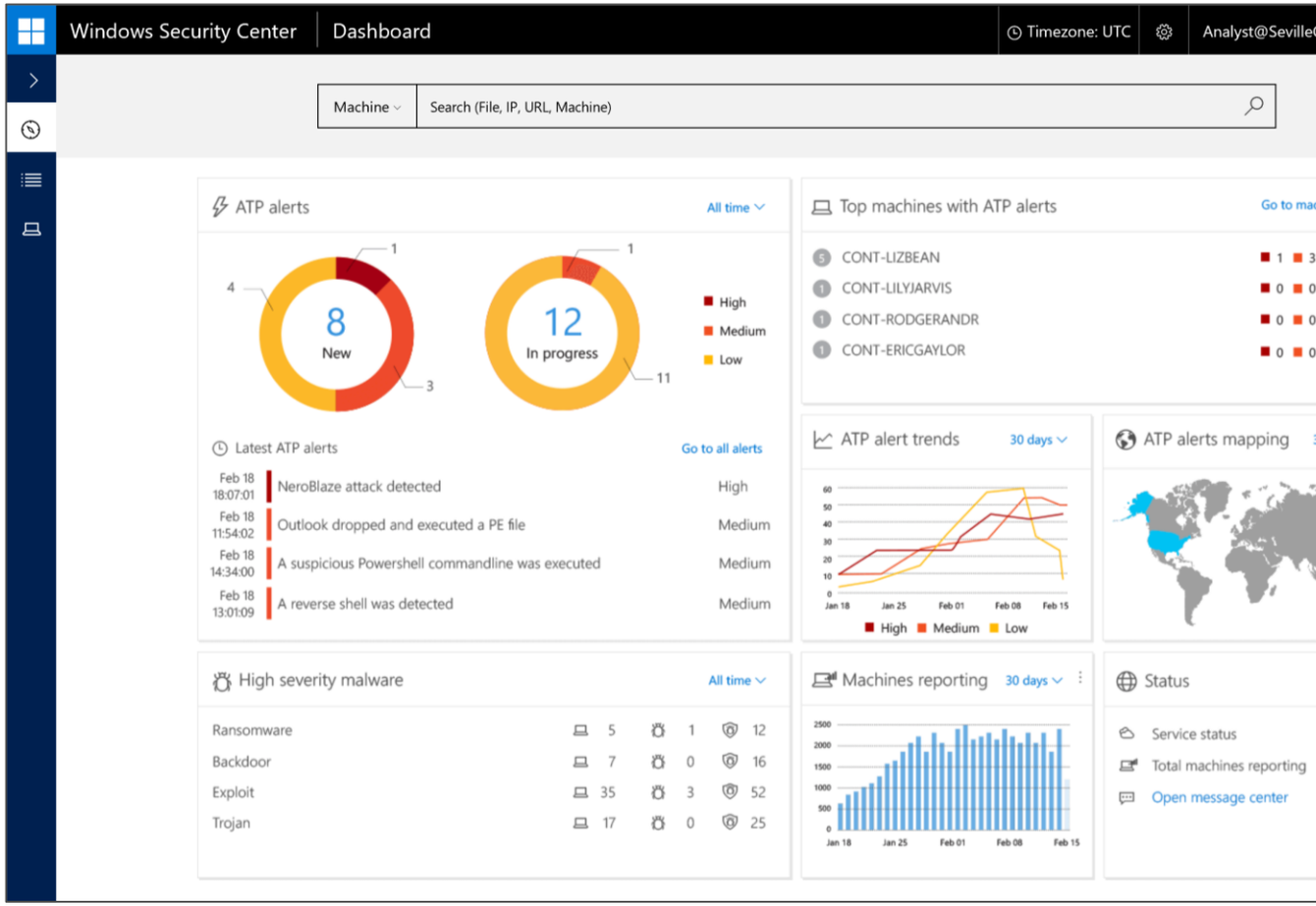
Microsoft Defender ATP

OS 組み込み型 クラウドベース EDR セキュリティ

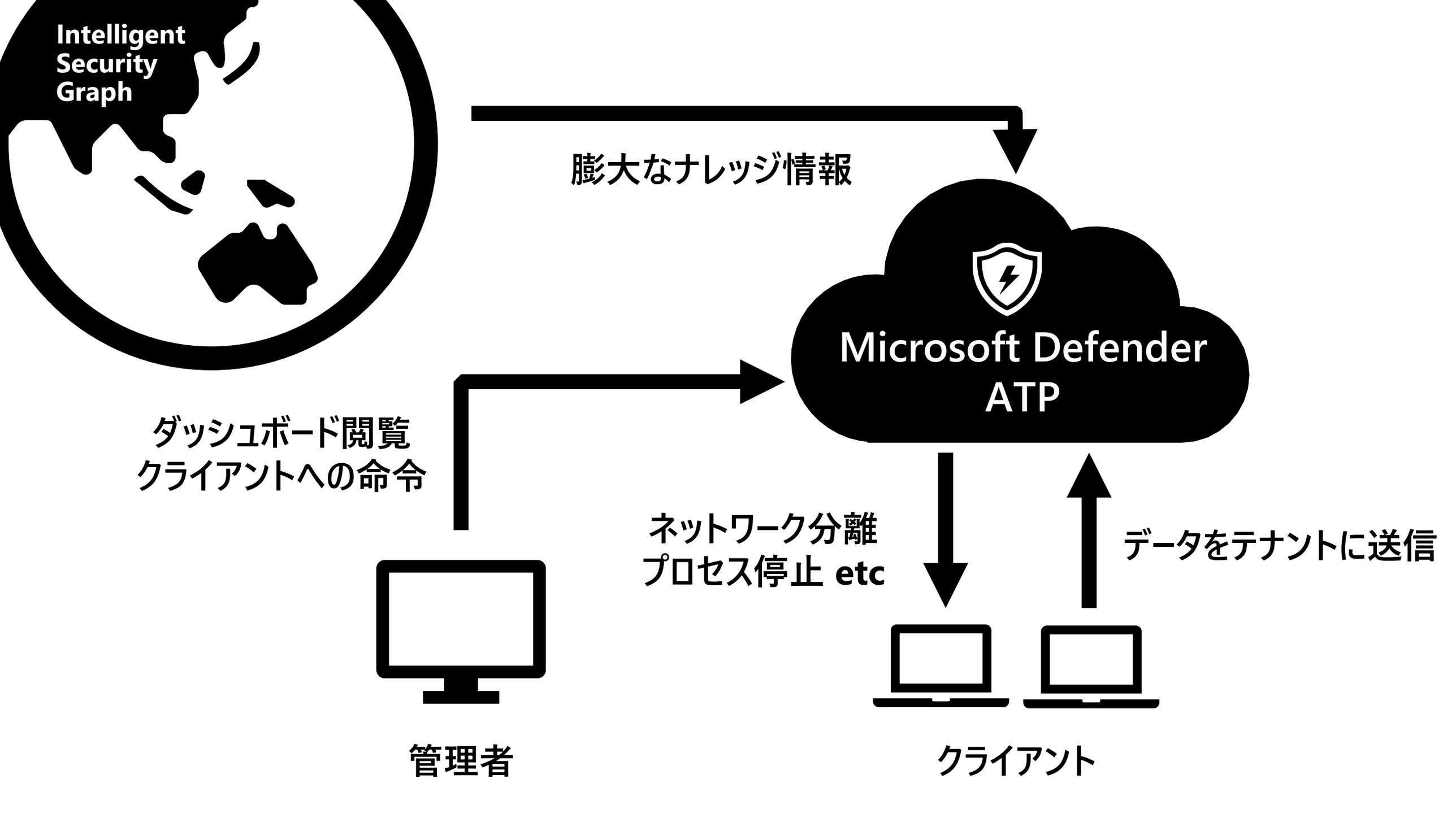
OS 標準搭載のクライアント

クラウド ベースの
セキュリティ分析サービス

マイクロソフトとコミュニティの
脅威インテリジェンス

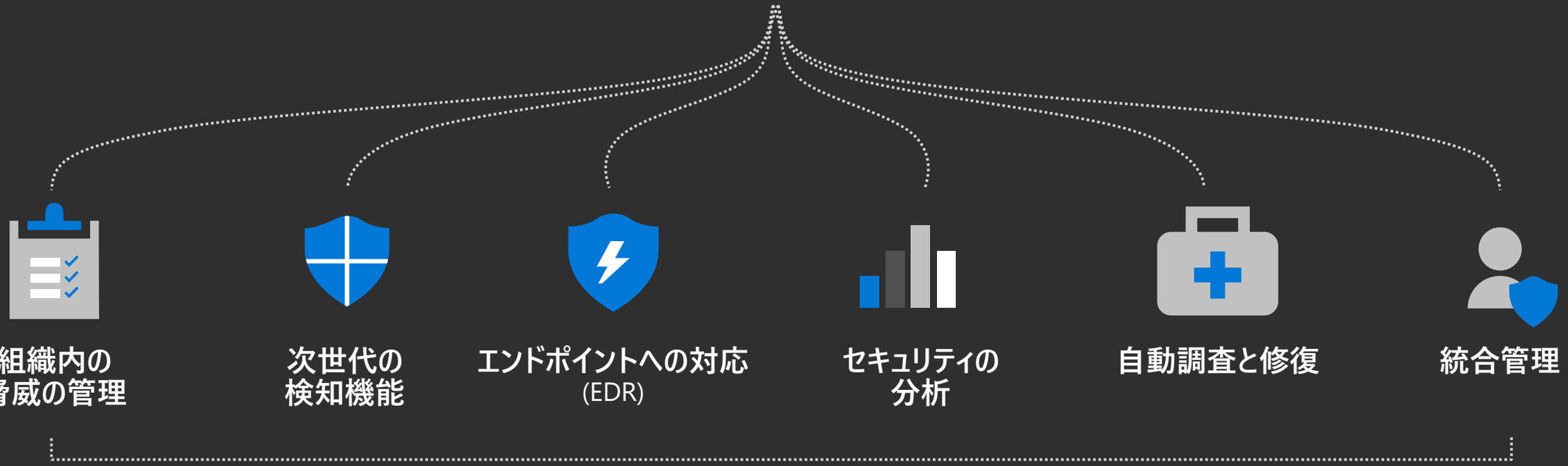


Windows Defender ATP の管理画面


Intelligent
Security
Graph
膨大なナレッジ情報
Microsoft Defender
ATP
ダッシュボード閲覧
クライアントへの命令
ネットワーク分離
プロセス停止 etc
データをテナントに送信
管理者
クライアント

Microsoft Defender
Advanced Threat Protection

組み込み型クラウドベースのセキュリティ

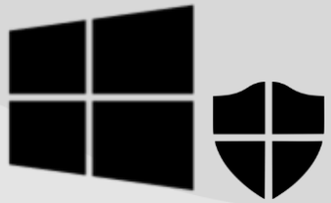


エンドポイント セキュリティ管理の一元化

Windows Defender ATP は OS 組み込み型

- エージェント管理不要 (ビルトイン)
- 負荷が少ない
- 高い耐タンパー性能 (改ざん防止)

Windows Defender を検討すべき理由その 2



OS 標準
無償セキュリティ

＋

OS 標準
有償セキュリティ
(Defender ATP)

＝

軽量かつ強力
管理も簡単

OS を作るベンダーの OS のためのセキュリティ

Windows Defender を検討すべき理由

Trust - 信頼

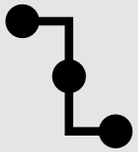
パートナーとしての信頼性

Technology - 技術

OS を作るベンダーの
OS のためのセキュリティ

Operation - 運用

Connection - 連携




運用保守にどれくらい
コストをかけていますか？

理由その 3
運用の手間が減る

エンドポイントの多層防御

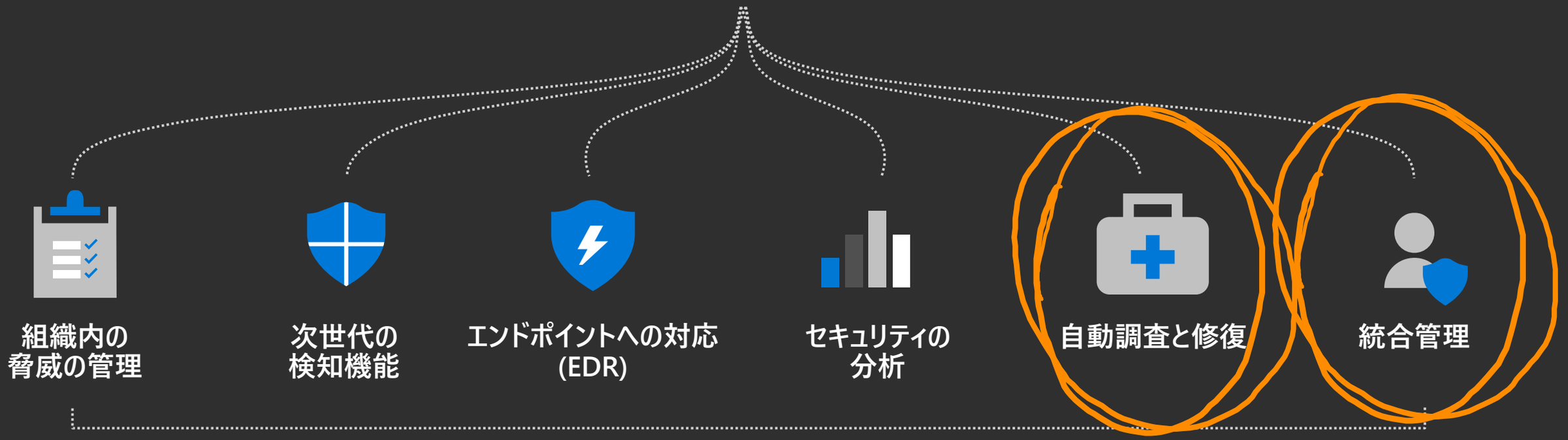
Enterprise E3
Enterprise E5

必要な対策例	とある構成例	Windows 10
不審な挙動の検知 (EDR for IOA)	- なし –	Windows Defender ATP
高度な攻撃の検知 (EDR for IOC)	C 社 (8,000円前後*)	Windows Defender ATP
脆弱性/マクロ悪用対策/ ネットワーク保護	- なし -	Windows Defender Exploit Guard
未知のマルウェア検知 (Reputation Check)	B 社 (約2,500～12,000円*)	Windows Defender ウイルス対策 Windows Defender Smart Screen
既知のマルウェア検知 (Signature)	A 社 (3,000円前後*)	Windows Defender ウイルス対策
資格情報の保護	- なし -	Windows Defender Credential Guard
HDD 暗号化	D 社 (3,000円前後*)	BitLocker
ブートレコード保護	- なし -	Windows Defender Device Guard

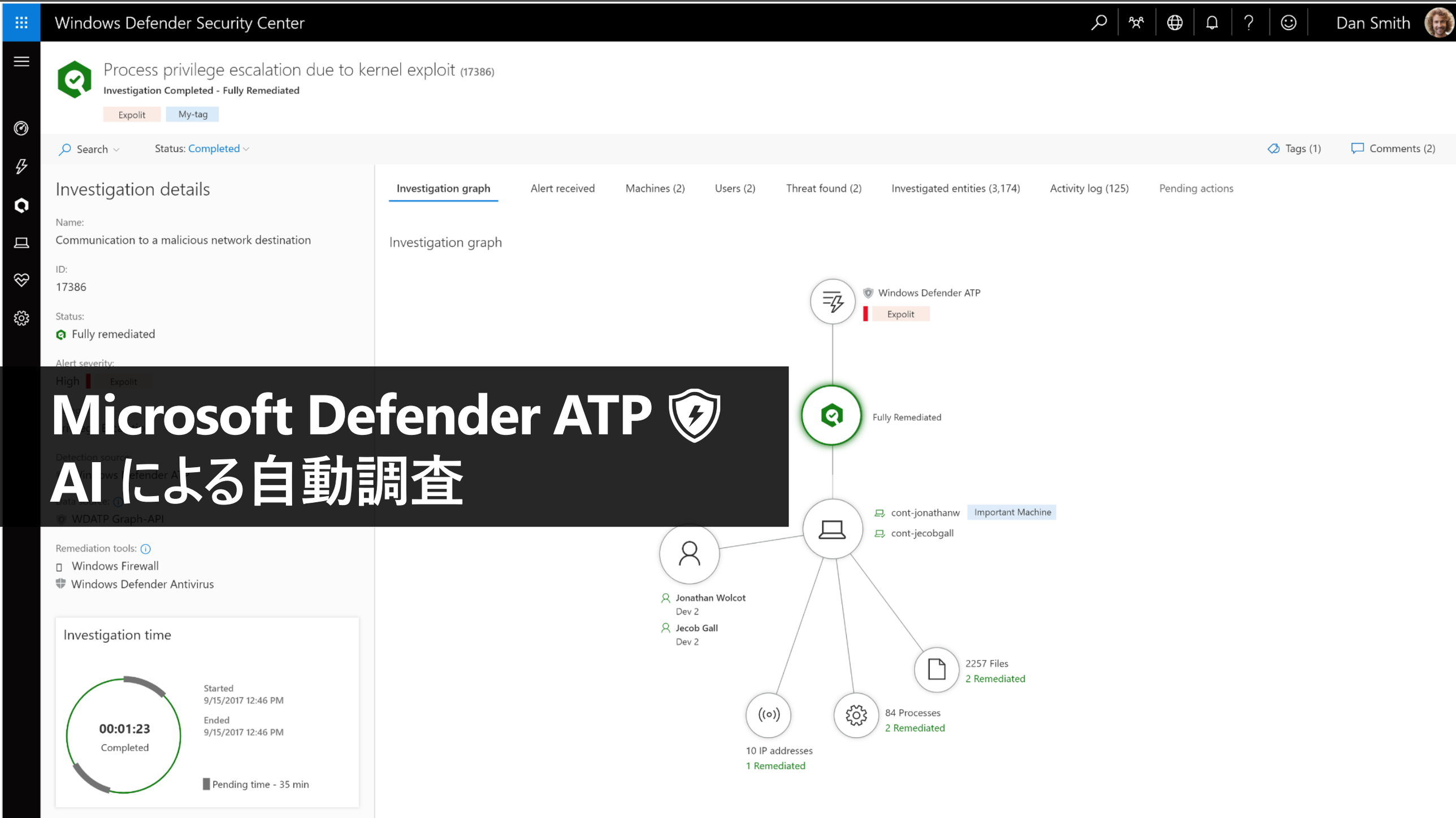
色々な製品の管理コンソールを見るのは大変

Microsoft Defender
Advanced Threat Protection

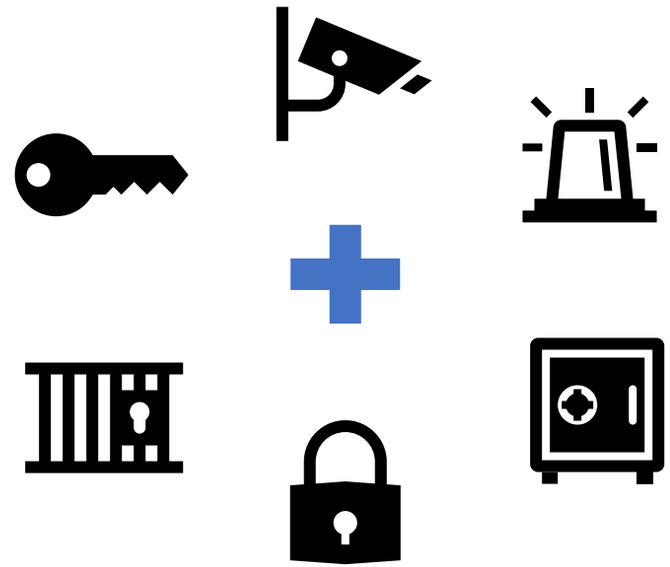
組み込み型クラウドベースのセキュリティ



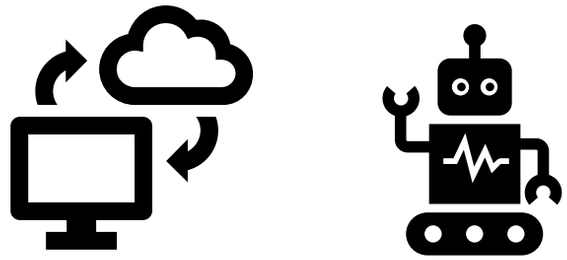
エンドポイント セキュリティ管理の一元化


Windows Defender Security Center
Dan Smith
Process privilege escalation due to kernel exploit (17386)
Investigation Completed - Fully Remediated
Expolit
My-tag
Search
Status: Completed
Tags (1)
Comments (2)
Investigation details
Name:
Communication to a malicious network destination
ID:
17386
Status:
Fully remediated
Alert severity:
High
Expolit
Detection source:
WDATP Graph-API
Remediation tools:
Windows Firewall
Windows Defender Antivirus
Investigation time
00:01:23
Completed
Started
9/15/2017 12:46 PM
Ended
9/15/2017 12:46 PM
Pending time - 35 min
Investigation graph
Alert received
Machines (2)
Users (2)
Threat found (2)
Investigated entities (3,174)
Activity log (125)
Pending actions
Investigation graph
Windows Defender ATP
Expolit
Fully Remediated
cont-jonathanw
Important Machine
cont-jecobgall
Jonathan Wolcot
Dev 2
Jecob Gall
Dev 2
2257 Files
2 Remediated
84 Processes
2 Remediated
10 IP addresses
1 Remediated
Microsoft Defender ATP
AI による自動調査

お金を払うならどっち？



A. 足し算のセキュリティ



B. やらないためのセキュリティ

理由その 3
もっと運用の手間が減る

各リリースによる Windows 10 の進化

IT と エンドユーザーの生産性向上のための
強化されたセキュリティとツール

1511

Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

1607

Windows Information Protection
Windows Hello for Business
Windows Analytics Upgrade Readiness
App-V, UE-V
Hybrid Azure Active Directory Join
Windows Ink
Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

1703

Windows Autopilot
Windows Defender ATP
Windows Defender Security Center
Express update delivery
Hyper-V
Windows 10 Subscription Activation
Windows Insider Program for Business
Paint 3D
Cortana at work
Night light, mini view
Windows Information Protection
Windows Hello for Business
Windows Analytics Upgrade Readiness
App-V, UE-V
Hybrid Azure Active Directory Join
Windows Ink
Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

1709

Windows Defender Exploit Guard, System Guard, Application Guard, Application Control
Mobile Device Management
Windows Analytics Update Compliance
Windows Analytics Device Health
Co-management
Enterprise search in Windows
Continue on PC
OneDrive Files On-Demand
Narrator
Mixed Reality Viewer
Windows Autopilot
Windows Defender ATP
Windows Defender Security Center
Express update delivery
Hyper-V
Windows 10 Subscription Activation
Windows Insider Program for Business
Paint 3D
Cortana at work
Night light, mini view
Windows Information Protection
Windows Hello for Business
Windows Analytics Upgrade Readiness
App-V, UE-V
Hybrid Azure Active Directory Join
Windows Ink
Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

1803

Windows Analytics – Spectre & Meltdown, Delivery Optimization, Application Reliability
Logon Health
WDATP Automated Remediation
Conditional Access based on WDATP device risk
Threat Analytics
Emergency Outbreak Updates
Advanced hunting
Cloud Credential Guard
Diagnostic data viewer
Windows Autopilot enrollment status page
Windows 10 Enterprise in S mode
Shared Windows Devices
Nearby Sharing
Dictation
Timeline
Windows Defender Exploit Guard, System Guard, Application Guard, Application Control
Mobile Device Management
Windows Analytics Update Compliance
Windows Analytics Device Health
Co-management
Enterprise search in Windows
Continue on PC
OneDrive Files On-Demand
Narrator
Mixed Reality Viewer
Windows Autopilot
Windows Defender ATP
Windows Defender Security Center
Express update delivery
Hyper-V
Windows 10 Subscription Activation
Windows Insider Program for Business
Paint 3D
Cortana at work
Night light, mini view
Windows Information Protection
Windows Hello for Business
Windows Analytics Upgrade Readiness
App-V, UE-V
Hybrid Azure Active Directory Join
Windows Ink
Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

1809

Windows Defender ATP new attack surface area reduction controls
Investigation and remediation across Office 365 ATP and Windows Defender ATP
Web Authentication in Microsoft Edge
Windows Hello with FIDO 2.0
30 months of support for September releases
Windows Autopilot Self-deploying mode
Windows Autopilot Hybrid Azure AD join
S Mode Block Switch
Microsoft Edge kiosk mode
Desktop Analytics (Preview) – Intelligent Pilot Selection and ConfigMgr Integration
ReadyforMicrosoft365.com
Microsoft Edge experience improvements
Accessibility enhancements
Access the clipboard across devices
Your Phone
Windows Analytics – Spectre & Meltdown, Delivery Optimization, Application Reliability
Logon Health
WDATP Automated Remediation
Conditional Access based on WDATP device risk
Threat Analytics
Emergency Outbreak Updates
Advanced hunting
Cloud Credential Guard
Diagnostic data viewer
Windows Autopilot enrollment status page
Windows 10 Enterprise in S mode
Shared Windows Devices
Nearby Sharing
Dictation
Timeline
Windows Defender Exploit Guard, System Guard, Application Guard, Application Control
Mobile Device Management
Windows Analytics Update Compliance
Windows Analytics Device Health
Co-management
Enterprise search in Windows
Continue on PC
OneDrive Files On-Demand
Narrator
Mixed Reality Viewer
Windows Autopilot
Windows Defender ATP
Windows Defender Security Center
Express update delivery
Hyper-V
Windows 10 Subscription Activation
Windows Insider Program for Business
Paint 3D
Cortana at work
Night light, mini view
Windows Information Protection
Windows Hello for Business
Windows Analytics Upgrade Readiness
App-V, UE-V
Hybrid Azure Active Directory Join
Windows Ink
Mobile Device Management
AAD Join
Windows Store for Business
Windows Update for Business
Mail, Calendar, Photos, Maps, Groove, Skype
Windows Defender Antivirus
Windows Hello
Microsoft Edge
Device Guard
Credential Guard
BitLocker
SmartScreen
Windows as a service
In-place upgrades
Continuum
Cortana
Windows 10 core

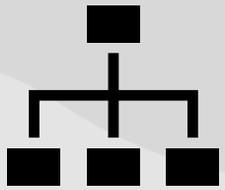
OS のバージョンアップで
重大な問題が多く発生するのは
暗号化やウイルス対策ソフト

ディスク暗号化は
BitLocker

ウイルス対策は
Windows Defender AV

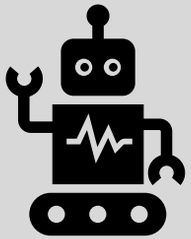
全て Microsoft で検証済みです！

Windows Defender を検討すべき理由その 3



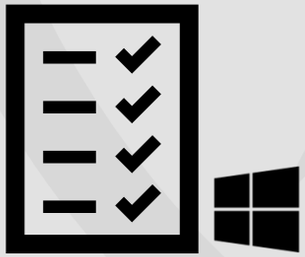
管理の一元化

＋



オペレーションの
自動化

＋



検証項目の
削減

＝ ムダな作業からの解放

Windows Defender を検討すべき理由

Trust - 信頼

パートナーとしての信頼性

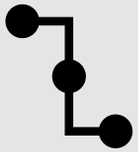
Technology - 技術

OS を作るベンダーの
OS のためのセキュリティ

Operation - 運用

自動化による作業軽減
検証項目の削減

Connection - 連携



Microsoft 365 Enterprise

Office 365

Office 365 ProPlus
Exchange
OneDrive
SharePoint
Teams

Enterprise Mobility + Security (EMS)

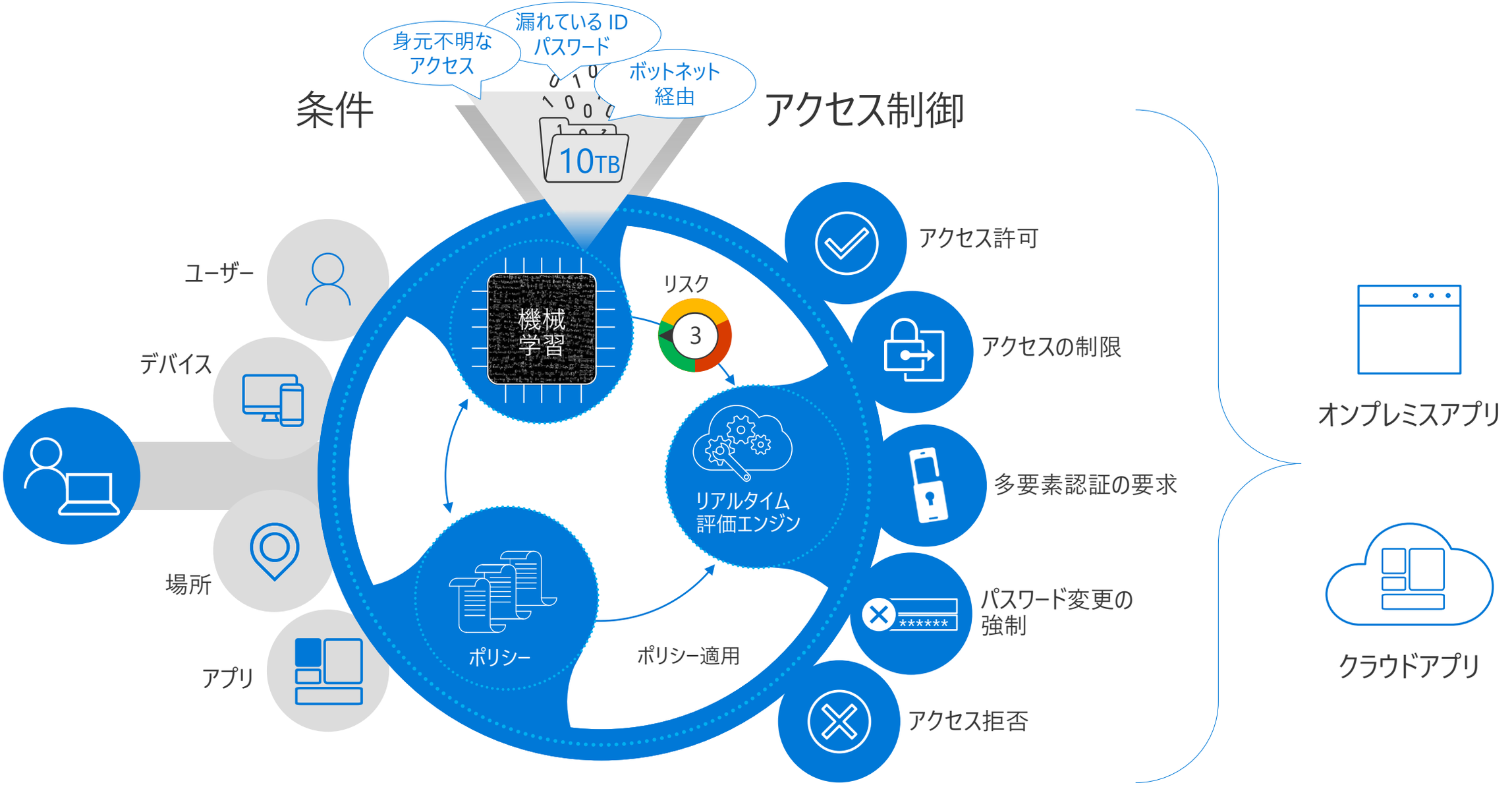
Azure AD
Intune
Azure Information Protection
Cloud App Security
Azure ATP

Windows 10

Microsoft Defender ATP

理由その 4
幅広い製品ポートフォリオだからできる
Microsoft 365 システム連携

Azure AD の条件付きアクセス



Microsoft Defender ATP + O365 ATP

検知

マクロ付き WORD ドキュメント

攻撃者

攻撃者のサーバーへ接続

Microsoft Defender ATP

エンドポイントの異常行動を検知

セキュリティ / IT管理者

Office 365 ATP

メールサンドボックスセキュリティ

エクスプロイト

インストール

永続化

WORDファイルからEXE ファイルの生成と実行

decode-backdoor.exe

ASEP レジストリへの登録

HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run.

Scheduled Task への登録

Schtaskexe xxxx.

権限昇格

攻撃者サーバーから EXE ファイルを ダウンロード＆実行

mcujpJRy.exe

資格情報の盗難

攻撃者サーバーから EXE ファイルを ダウンロード＆実行

mimikatz.exe

Microsoft Defender ATP + O365 ATP

検知

自動対処

マクロ付き WORD ドキュメント

攻撃者

攻撃者のサーバーへ接続

Microsoft Defender ATP

エンドポイントの異常行動を検知、
自動化で対処

セキュリティ / IT管理者

Office 365 ATP

メールサンドボックスセキュリティ

エクスプロイト

インストール

永続化

WORDファイルからEXE
ファイルの生成と実行

~~decode_backdoor.exe~~

ASEP レジストリへの登録

~~HKLM¥Software¥Microsoft¥Windows¥CurrentVersion¥Run~~

Scheduled Task への登録

~~Schtasks.exe /xxxx~~

権限昇格

攻撃者サーバーから
EXE ファイルを
ダウンロード＆実行

~~meujpJRy.exe~~

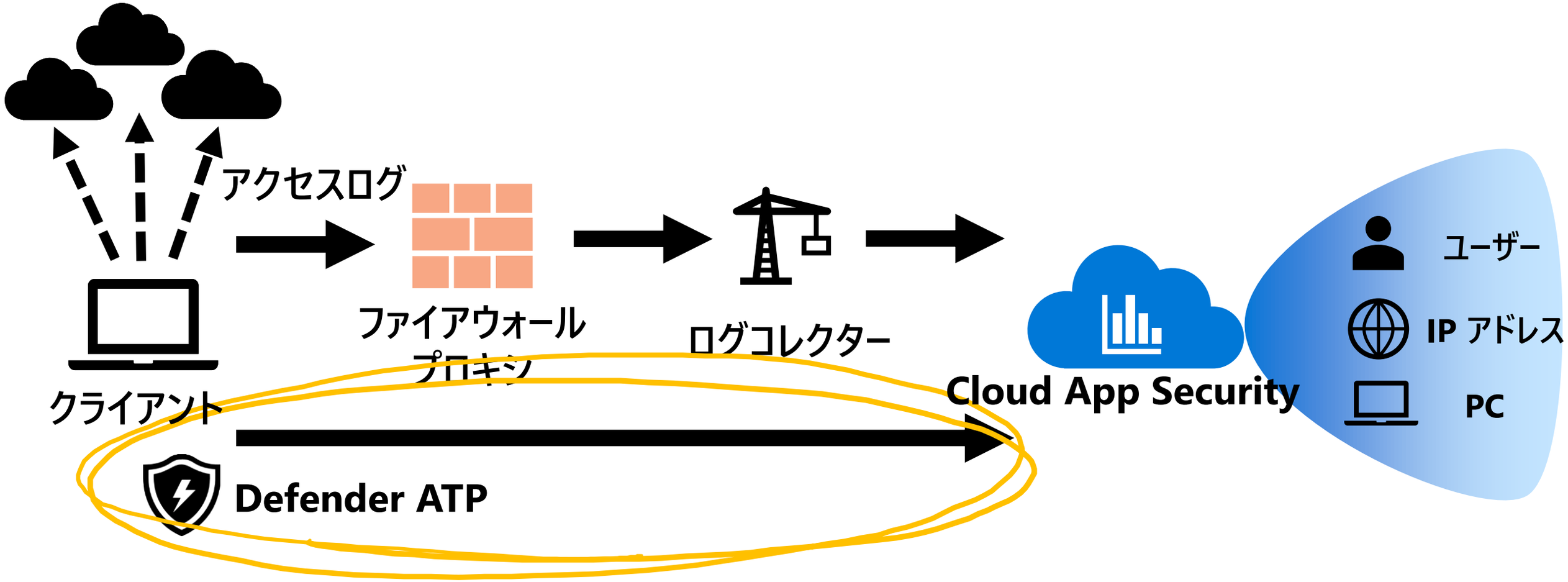
資格情報の盗難

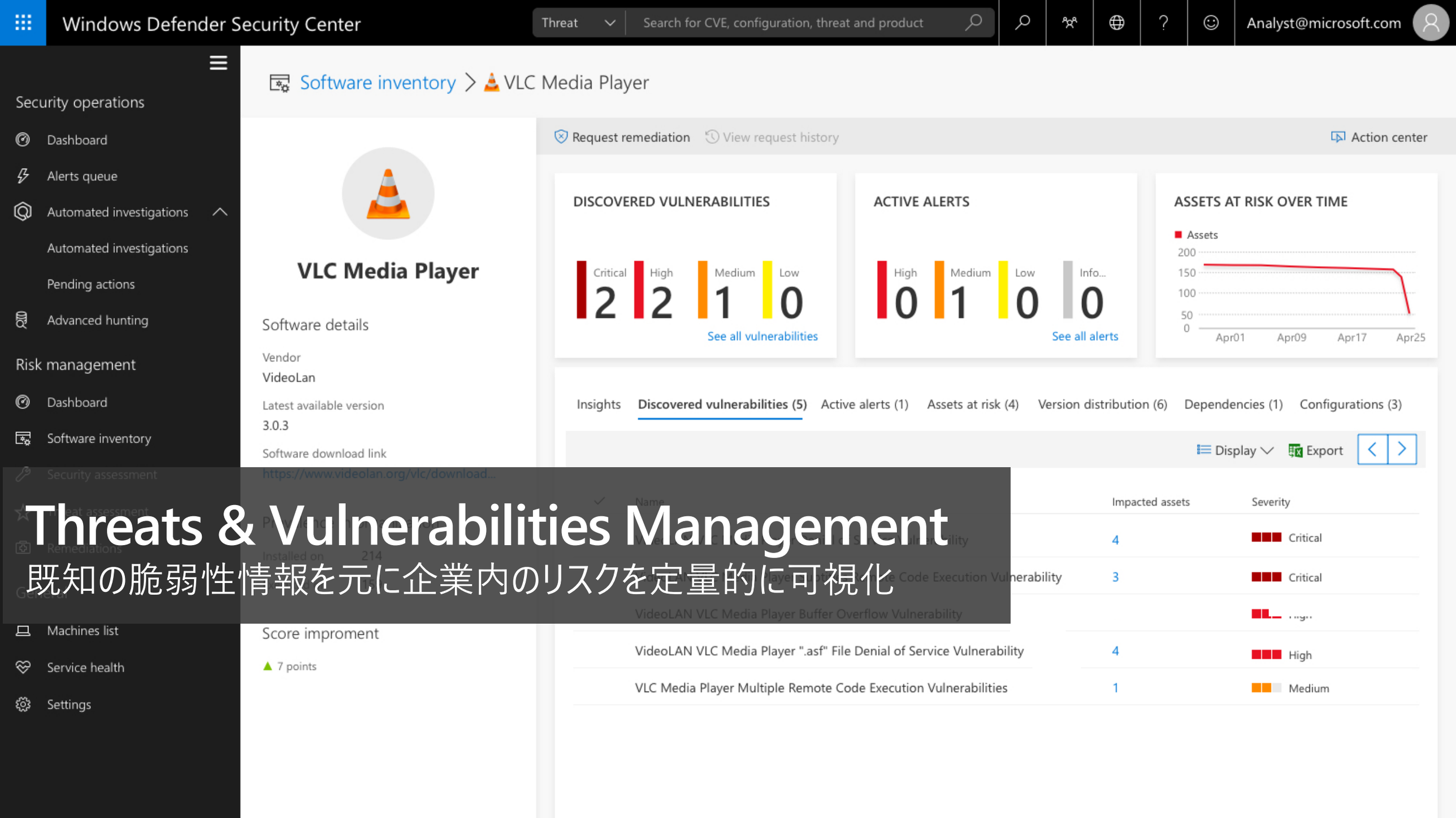
攻撃者サーバーから
EXE ファイルを
ダウンロード＆実行

~~mimikatz.exe~~

Microsoft Defender ATP

Cloud App Security



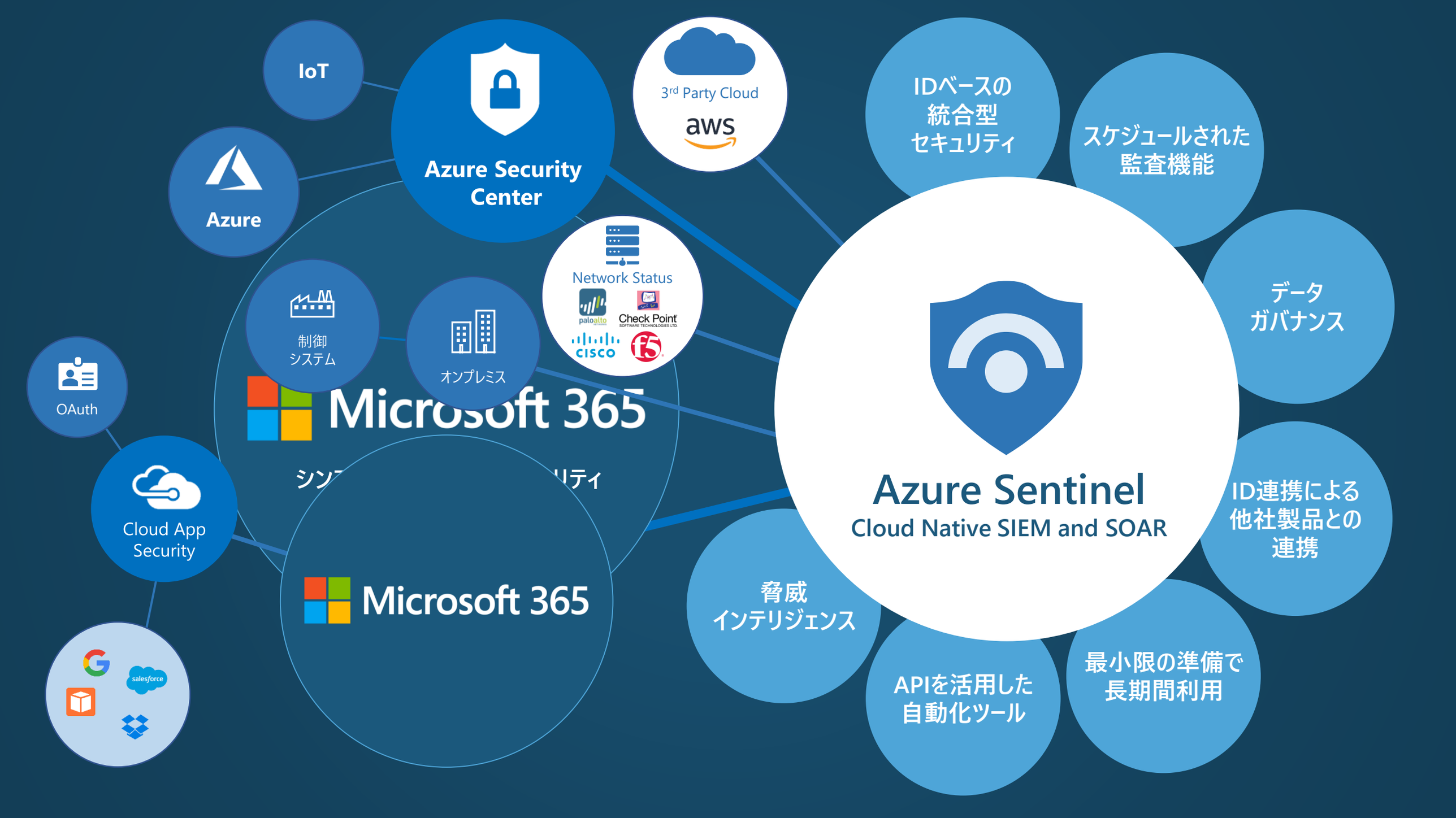


Threats & Vulnerabilities Management

既知の脆弱性情報を元に企業内のリスクを定量的に可視化

Microsoft Flow

さまざまなアプリやサービスを対象とした
ワークフロー自動化サービス


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
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
Network Status
paloalto
Check Point
SOFTWARE TECHNOLOGIES LTD.
cisco
f5
制御
システム
オンプレミス
Microsoft 365
OAuth
Cloud App
Security
Microsoft 365
salesforce

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

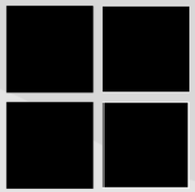
- Microsoft 365
- Azure
- Microsoft Partners

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

Windows Defender を検討すべき理由その 4



M365 サービス
連携

クラウド サービス
連携

やりたいことが
自由に

幅広いサービスとの連携による利便性と可能性

Windows Defender を検討すべき理由

Trust - 信頼

パートナーとしての信頼性

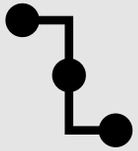
Technology - 技術

OS を作っているベンダーの
OS のセキュリティ

Operation - 運用

自動化による作業軽減
検証項目の削減

Connection - 連携



幅広いサービスとの連携
による利便性と可能性

Microsoft's mission

Empower every person and every organization on the planet to achieve more

地球上のすべての個人とすべての組織が、
より多くのことを達成できるようにする

Microsoft

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

Partner Alliance 設立

5000人

学生向けセキュリティ
教育実施予定

Windows Defender を検討すべき理由 5

みなさんがもっと活躍できるように