

Microsoft Defender for IoT

Takehiro Hirai
IoT Technical Specialist
GPS - Global IoT Partner Ecosystem



アジェンダ

- IoT セキュリティについて
- Microsoft Defender for IoT の概要
- ワークショップについて

Microsoft の セキュリティ ミッション： より安全な世界を実現し、組織のデジタル変革を可能にする

Microsoft にとって セキュリティ は、3,500人以上の体制による 100億ドル規模の
ビジネスであり、5つの Gartner Magic Quadrant と 7つの Forrester Wave Report
において Leader に選ばれています

最近のセキュリティ関連の買収として、CyberX、ReFirm Labs、RiskIQ、CloudKnox
などがあります

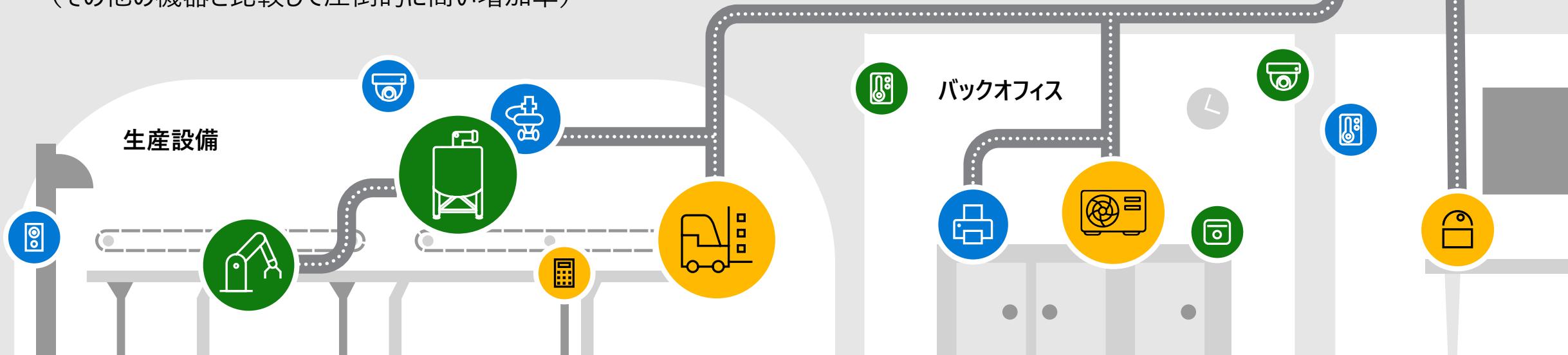
今後5年間でサーバーセキュリティへの投資を4倍の200億ドルへ拡大します



アンマネージドの IoT/OT デバイスが増加中

攻撃対象領域はここ数年で既に3倍に拡大、
今後も 22% の拡大を予想しています

2021年に 約120億台 だったデバイスは、
2025年には 約270億台 に増加する見込み¹
(その他の機器と比較して圧倒的に高い増加率)



1. <https://iot-analytics.com/number-connected-iot-devices/>

OT/IoT セキュリティ チャレンジ - 特別な考慮事項

数量

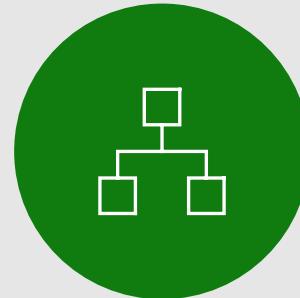


多くのビジネスライン
デジタルトランスフォーメーションの加速



セキュリティアナリストあたりの
管理デバイス数の増加

ビジネスへの影響



異なるテクノロジー
多くのソリューション



様々な入力ソースからの
インシデントの把握

優先順位



重要なインシデントの特定
アラートの重要度決定



内容に基づく
インシデントの優先順位付け

実際の IoT 攻撃事例

ZDNet

MUST READ: Firmware attacks are on the rise and you aren't worrying about them enough

NASA hacked because of unauthorized Raspberry Pi connected to its network

NASA described the hackers as an "advanced persistent threat," a term generally used for nation-state hacking.



DARKReading

SIGN UP FOR OUR NEWSLETTERS

Verkada Breach Demonstrates Danger of Overprivileged Users

In re-evaluating supply chains, companies should classify vendors with super admin privileges to devices or backdoors as a significant threat.

ZDNet

Hackers are attacking smart building access systems

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.



ZDNet

Triton hackers return with new, covert industrial attack



Traces of a hacking group behind the destructive Triton malware have been found at a new infrastructure facility following an infamous attack in the Middle East.

Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password



The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant.

The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

f g t m b

CIO, CISO が直面する IoT/OT 関連の主要課題

IoT の普及とリスク

68%

の組織が、IoT/OT はビジネスイノベーション、戦略的目標の支援に不可欠と回答¹

60%

が、IoT/OT のセキュリティが IT/OT インフラの中で最もセキュリティが低い側面の1つと捉えている¹

31%

の組織が、セキュリティの懸念により IoT/OT のプロジェクト採用の延期、制限、中止を経験

技術的なギャップ

71%

IoT/OT デバイスの完全なインベントリが存在しない割合¹

70%

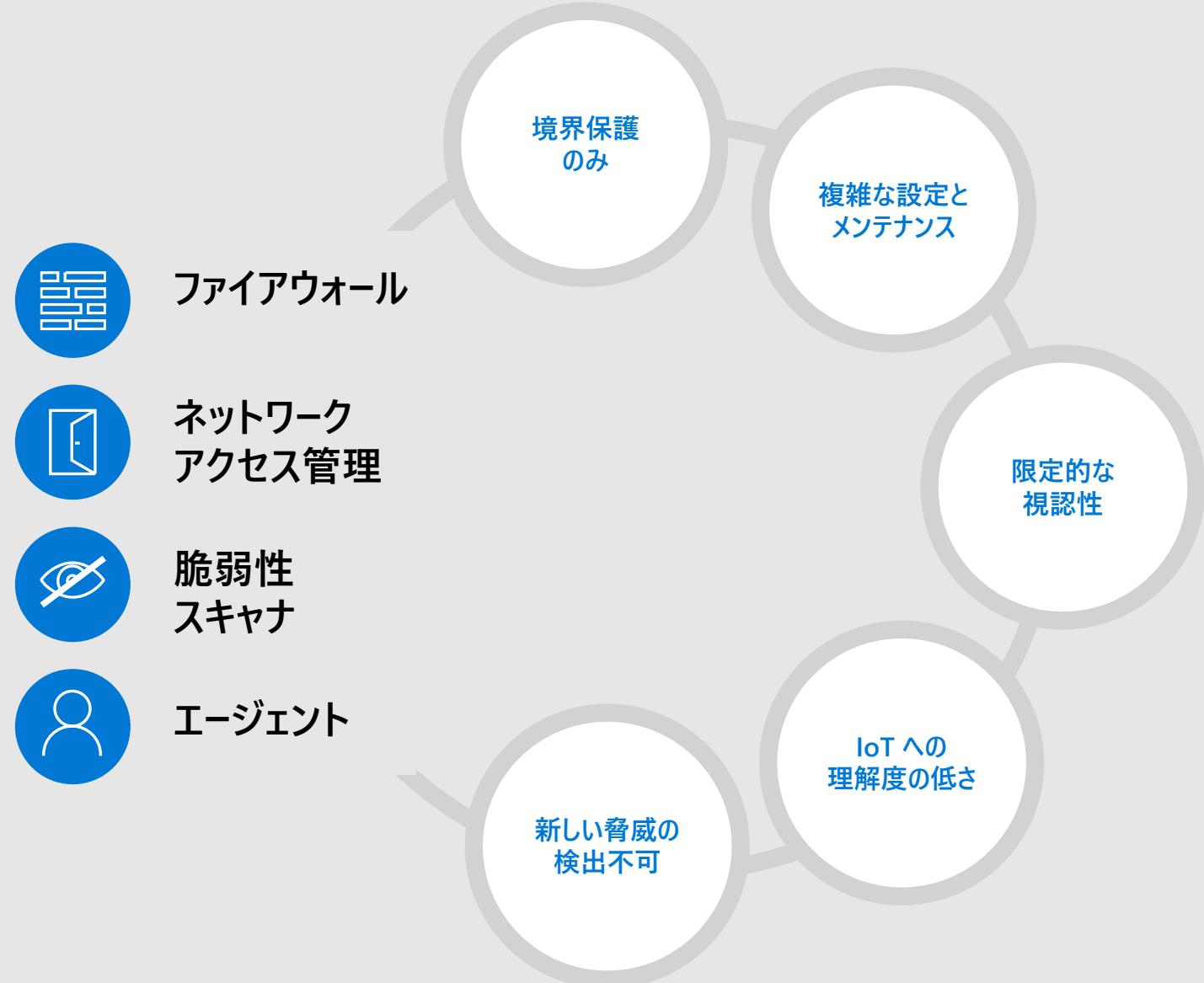
IoT デバイスが安全である（脆弱性が緩和され、セキュアな設定が行われている）という確信が平均以下の割合¹

61%

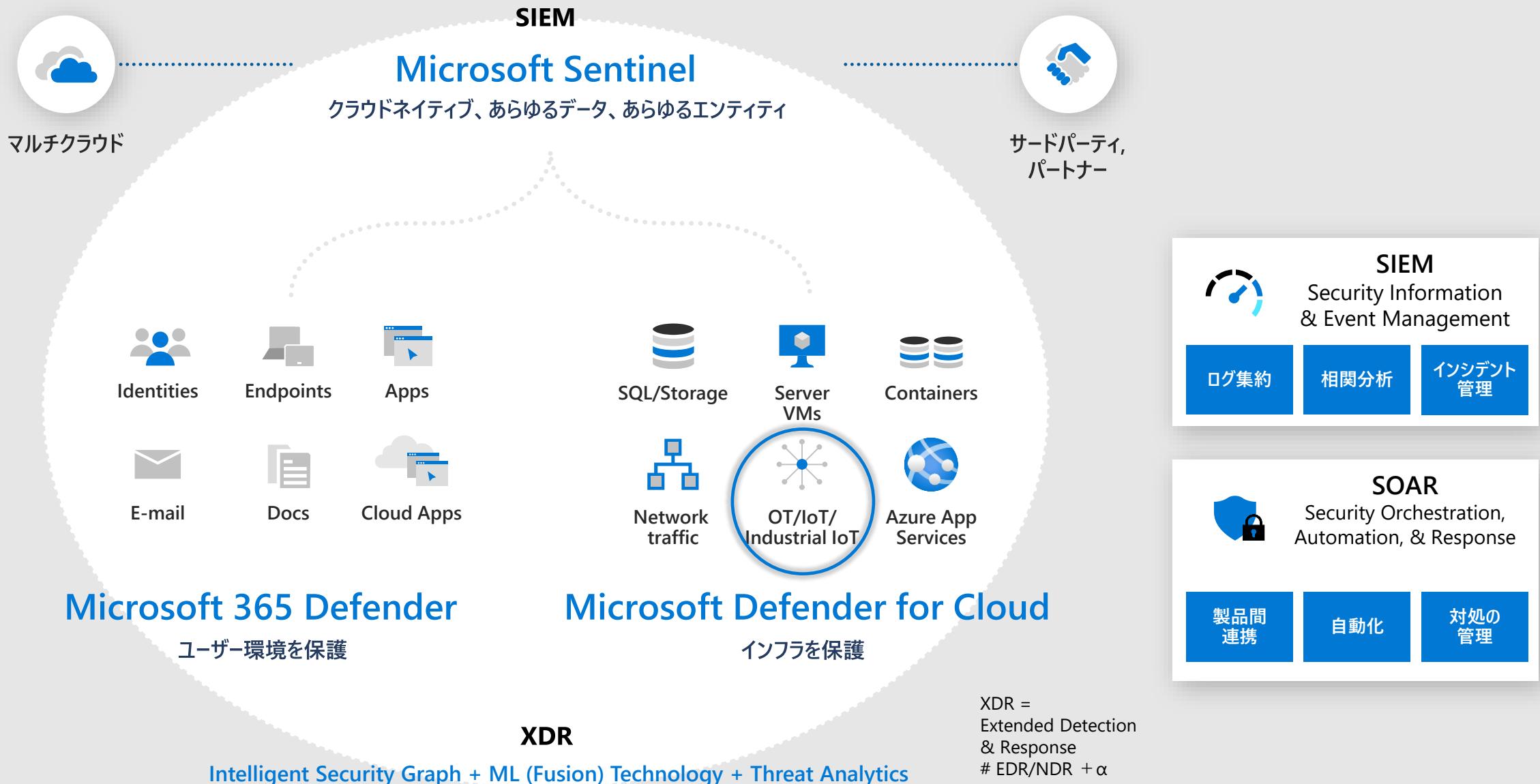
IoT デバイスのリスクの特定に関する技術的な信頼度が平均以下の割合¹

1. The State of IoT/OT Cybersecurity in Enterprise Organizations, Ponemon Institute, October 2021

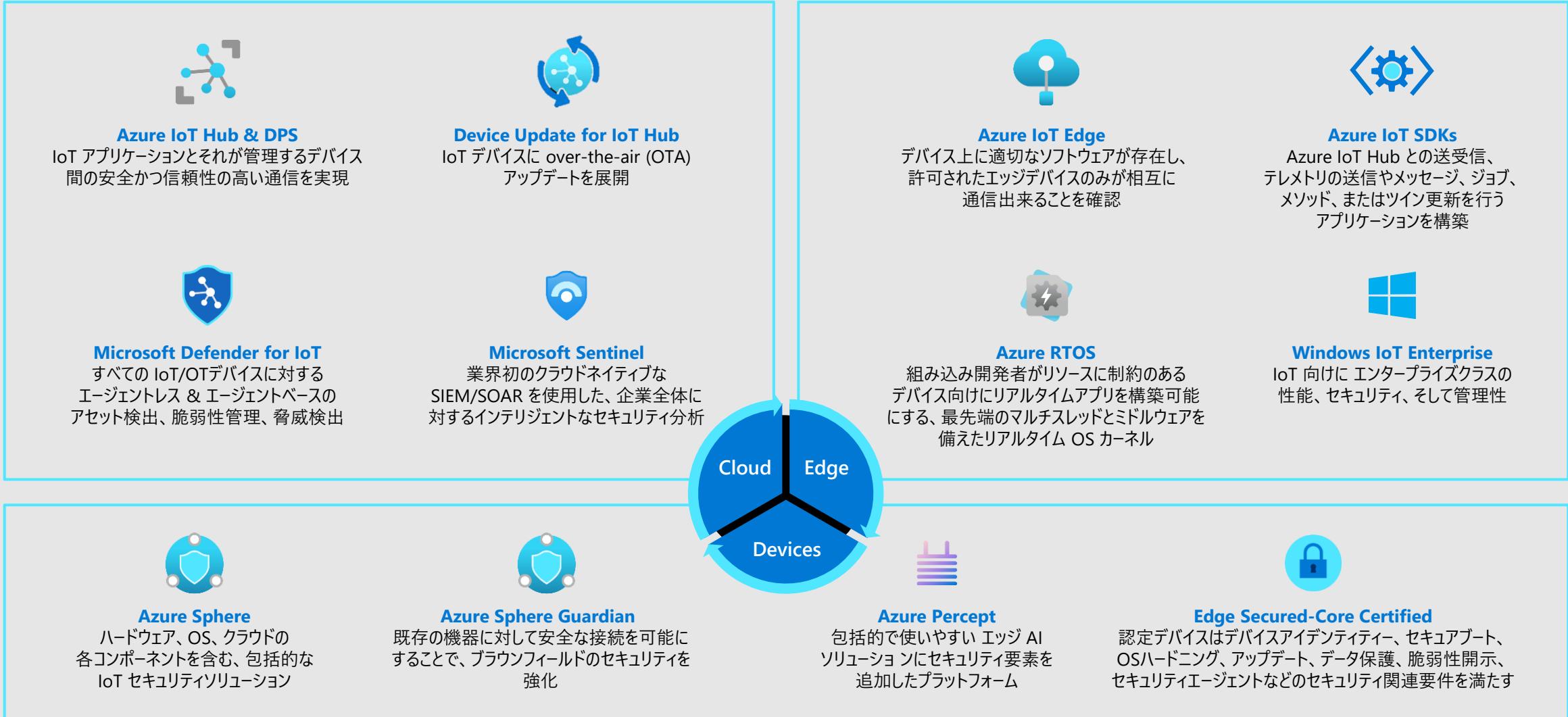
既存ソリューション の課題



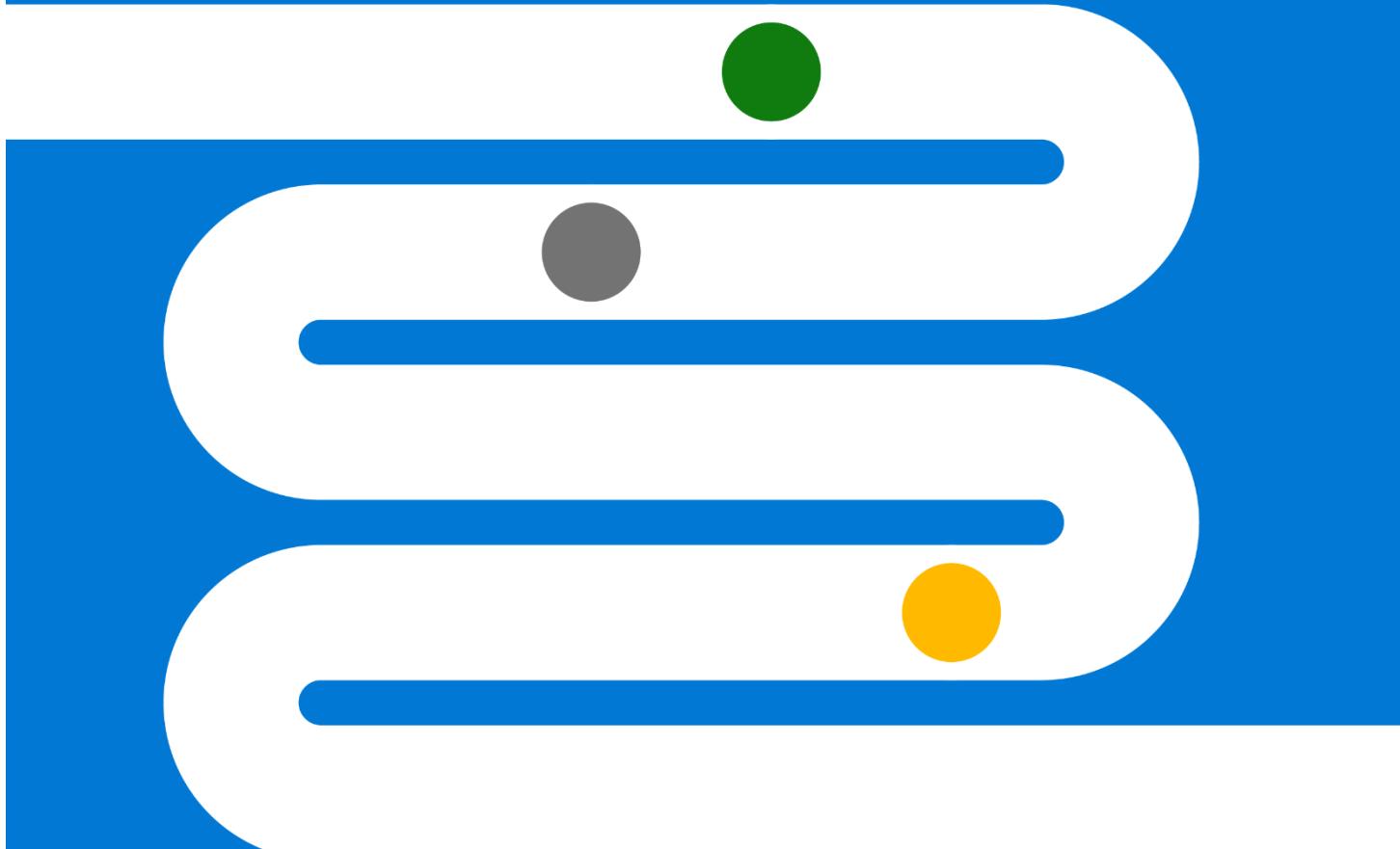
Microsoft が提供する、統合されたセキュリティ運用エクスペリエンス



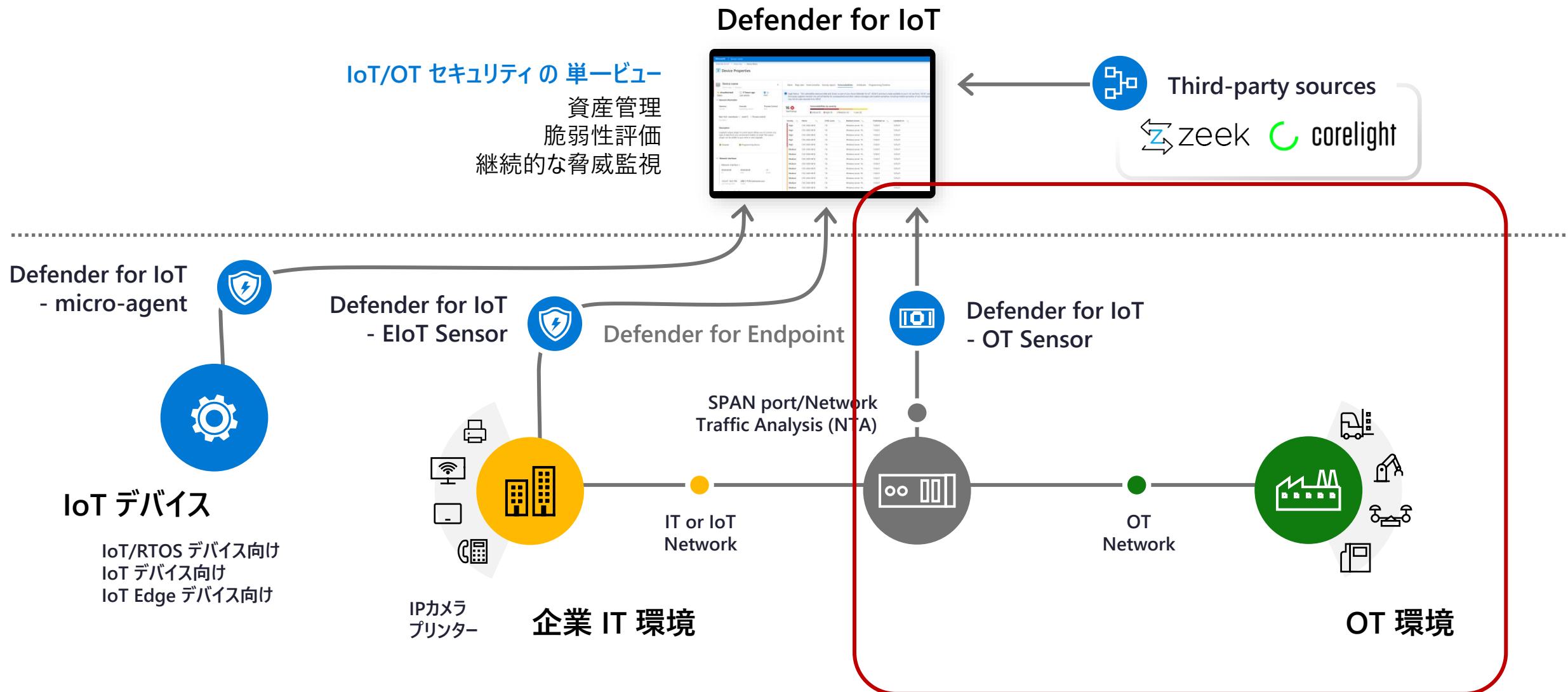
ゼロトラスト IoT を実現するためのサービス群

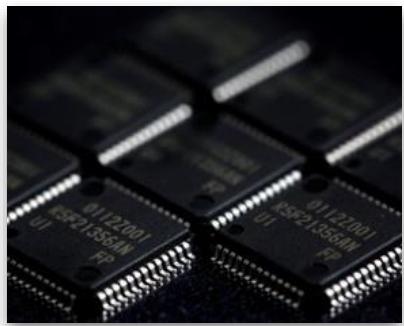


Microsoft Defender for IoT

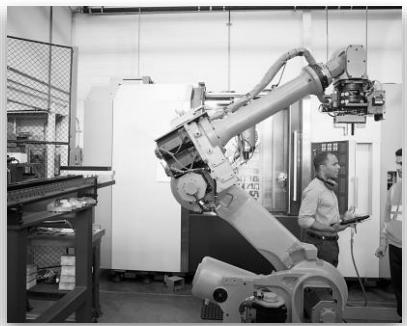


Microsoft Defender for IoT - 多様なデータソースを幅広くカバー

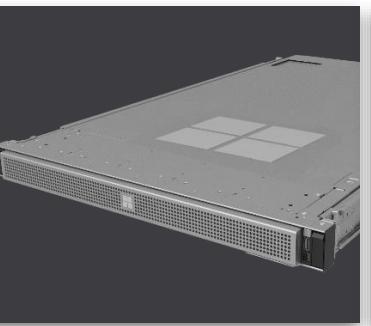




センサー + 制御



センサーからインタラクティブへ



統合プラットフォーム



グローバルスケール

Microcontroller

Azure RTOS

IoT Devices

Azure IoT Device SDK

Edge Devices

Azure IoT Edge

Defender for IoT - OT sensor

Defender for IoT - EIOT sensor

Defender for IoT - micro-agent (agent)

Azure Sphere

Edge Appliances

Azure Stack Edge
Azure Stack HCI

Firewall Manager

Defender for Endpoint

For Servers

Defender for Cloud for K8S

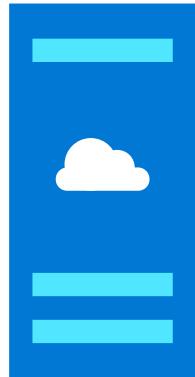
For App Services
For Storage
For SQL
For Key Vault
for Container
for RM
For DNS

Defender for Cloud

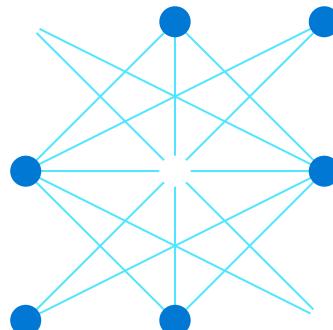
Microsoft Defender for IoT - OT Sensor

IoT/OT 環境向け エージェントレス セキュリティ

IoT/OT 環境を意識した行動分析と脅威インテリジェンスを備えた NDR (Network Detection & Response)



エージェントレス セキュリティ
生産への影響は“ゼロ”
1日未満の作業で導入が可能



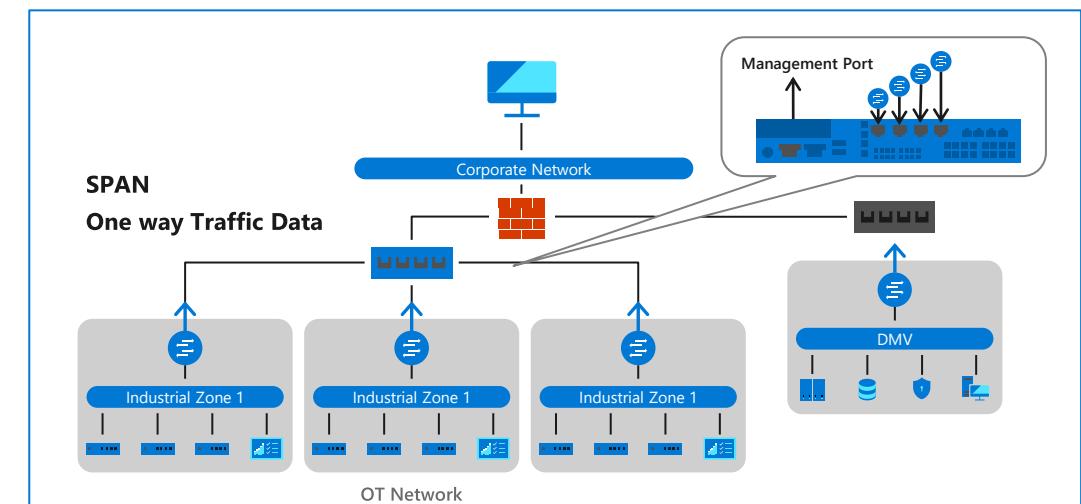
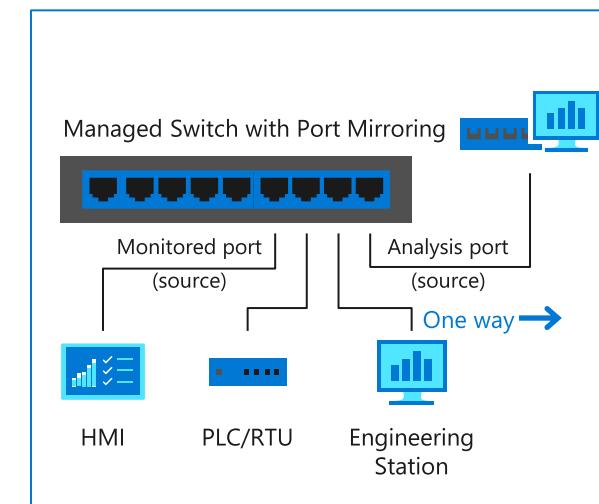
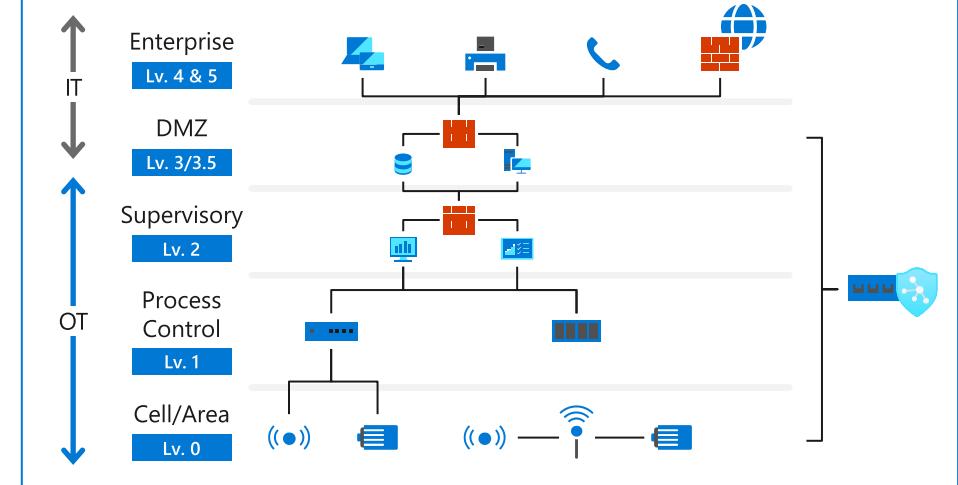
レガシー及び独自のデバイスにまたがる
IoT/OT資産、脆弱性、脅威の
継続的な可視化



Microsoft Sentinel や既存の SOC ツール
との統合により、IT/OTの統合的な
モニタリングとガバナンスを実現

Microsoft Defender for IoT - OT Sensor

- センサー：物理、または仮想アプライアンス
- ネットワーク・スパン・ポート/ネットワーク・タップに接続
- 複数のスイッチへの接続
- 完全なパッシブ型のスマートセンサー
- PCAP 分析機能（パケットキャプチャ分析機能）
- オンプレミスの管理用 Web コンソール、または Microsoft Defender for IoT による管理
- SIEM との統合



Microsoft Defender for IoT - OT Sensor

“すべて” の IoT/OT デバイスを検出



What is it?

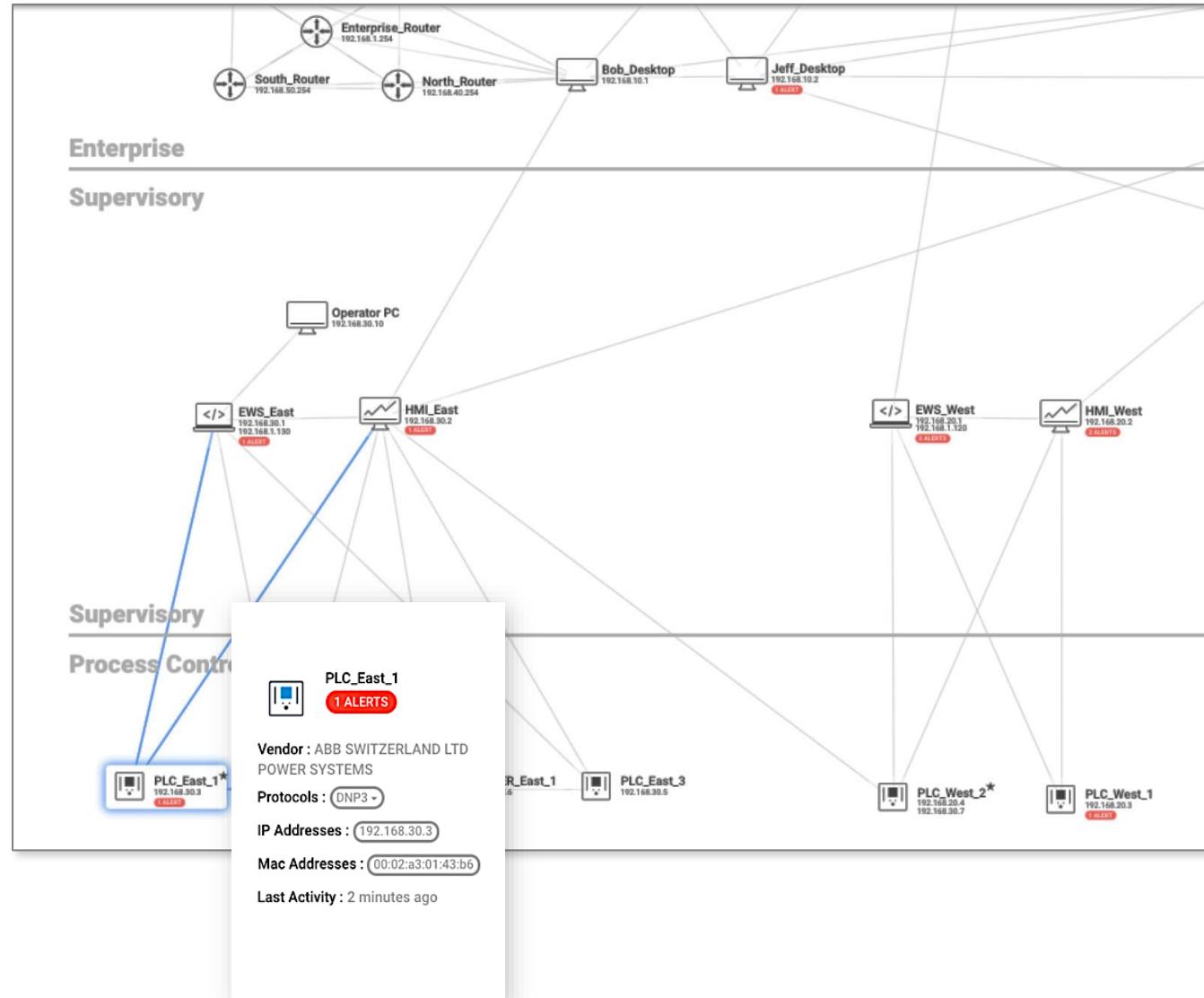
パッシブでエージェントレスのセンサーにより
収集された産業プロトコルを分析、デバイスの
詳細情報を特定、デバイスインベントリ、
デバイスマップを自動的に作成

製造元、種類、シリアル番号、
ファームウェアレベル、IP または MAC アドレス



Benefits

IoT/OT ネットワークトポジ全体が視覚化、
デバイスの通信パスを通じて運用上の問題
(例: デバイスの構成ミス) の根本原因を迅速
に特定



Microsoft Defender for IoT - OT Sensor

リアルタイムIoT/OT脅威アラート
- 5つのエンジンと機械学習を利用した分析を実施



アラート カテゴリ



Policy Violation

ポリシー違反エンジンによる
以前に学習したトラフィックからの逸脱の検出をトリガー



Protocol Violation

プロトコル違反エンジンによる
検出プロトコル仕様に準拠していないパケット構造またはフィールド値の検出をトリガー



Operational

運用エンジンによる
ネットワークの運用上のインシデントまたはデバイスの誤動作の検出をトリガー



Malware

マルウェア対策エンジンによる
悪意のあるネットワーク アクティビティや既知の攻撃の検出をトリガー



Anomaly

異常エンジンによる
逸脱 (ネットワークスキャンを想定外デバイスが行っているなど) の検出をトリガー

アラート一覧

<https://docs.microsoft.com/ja-jp/azure/defender-for-iot/organizations/alert-engine-messages>

Unauthorized Internet Connectivity Detected

Policy Violation | Sep 29, 2021 2:43:26 PM (3 minutes ago)

A device defined in your internal network is communicating with addresses on the Internet. These addresses have not been learned as valid addresses.

Device 192.168.0.110 communicated with addresses shown in External Addresses. Verify that this device is properly configured.



More About this Event

External Addresses : 137.220.100.146 over port FTP (21)

20.82.209.183

Remediation Steps

- Select Learn to allow all internal devices to communicate
- Select Acknowledge to save the alert. Another alert will trigger if the issue occurs again.

Port Scan Detected

Anomaly | Sep 29, 2021 2:42:06 PM (3 minutes ago)

Scan detected.

Scanning device: 10.0.100.20

Scanned device: 10.0.100.104

Scanned Ports: 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089...

It is recommended to notify the security officer of the incident.



Remediation Steps

- Multiple scans in the network can be an indication of a new device in the network, a new functionality of an existing device, improper configuration of an application (for example, due to a firmware update, or a new deployment), or malicious activity in the network, such as reconnaissance.
- During the reconnaissance phase, a tool usually collects system configuration data, including data about any installed antivirus applications and steals data on the computer systems themselves, which is then sent back to the attackers.

EtherNet/IP CIP Service Request Failed

Operational | Sep 29, 2021 2:42:09 PM (7 minutes ago)

EtherNet/IP server 10.0.100.104 returned an error result Connection failure to client 10.0.100.20. This indicates a server error or an invalid request by the client.



Remediation Steps

- Check if any operational process has been affected.
- Examine the processes related to the affected device.

is an approved scanner and mark it as a Scanning Device.

[Learn](#) [Acknowledge](#)

DeltaV Install Script

Sep 29, 2021 2:43:42 PM
DeltaV device 192.168.111.20 programmed device 192.168.111.2 by downloading code to the device using script STARTDEV.

Alert Detected

Sep 29, 2021 2:43:27 PM
An internal client 192.168.0.110 performs excessive login attempts to SMB server 192.168.10.100. First account names used: MAL/Administrator. This is suspected to be a password brute force, which is an att...

[more](#)

[PCAP file](#)

Alert Detected

Sep 29, 2021 2:43:27 PM
A device defined in your internal network is communicating with addresses on the Internet. These addresses have not been learned as valid addresses.

Device 192.168.0.110 communicated with addresses s...

[more](#)

[PCAP file](#)

Alert Detected

Sep 29, 2021 2:43:09 PM
A device 192.168.119.22 sent a Stop PLC command via Siemens S7 to device 192.168.119.3. The device will stop operating until start command will be sent.

[more](#)

[PCAP file](#)

Remote Access Connection Established

Sep 29, 2021 2:43:05 PM
Connection detected from 192.168.0.110 to 192.168.119.22 using TeamViewer

[more](#)

[PCAP file](#)

Alert Detected

Sep 29, 2021 2:43:05 PM
A device 192.168.119.22 sends a Stop PLC command via Siemens S7 to device 192.168.119.3. The device will stop operating until start command will be sent.

[more](#)

[PCAP file](#)

Microsoft Defender for IoT - OT Sensor

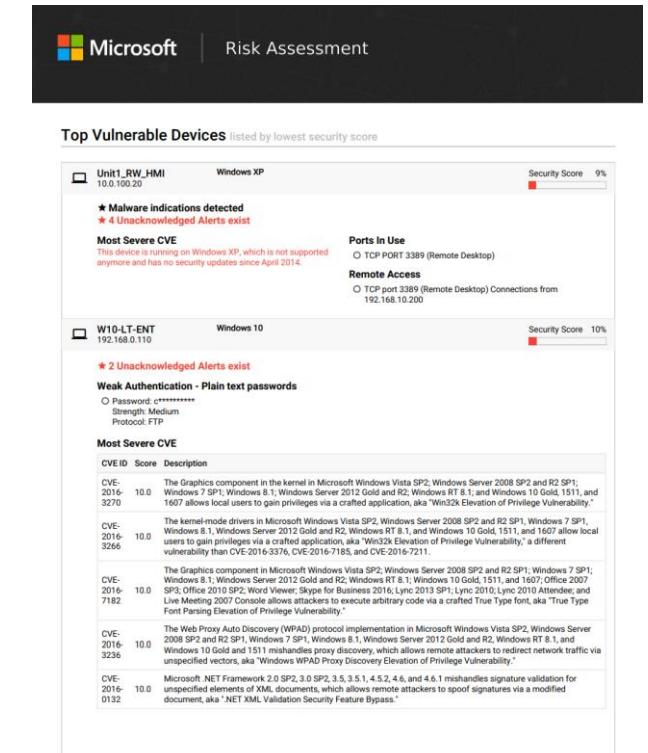
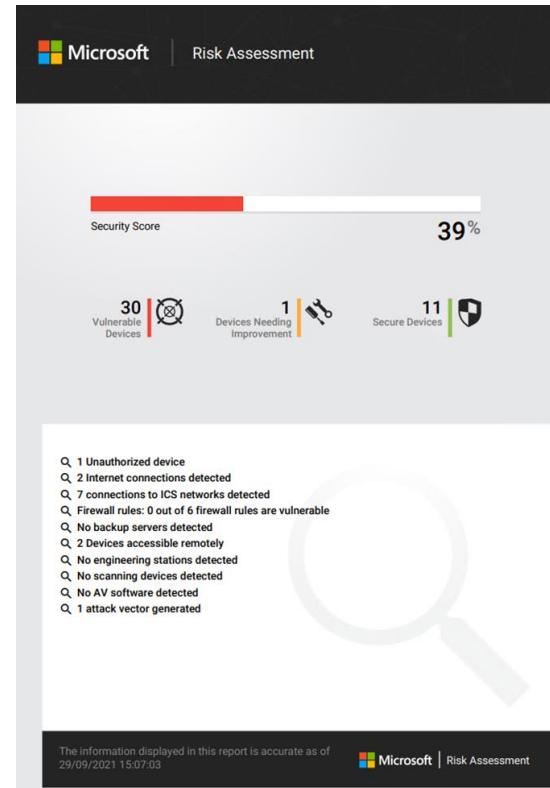
リスクアセスメント レポート



What is it?

センサーにより収集された情報からOT環境の
リスクアセスメントレポートを作成

- ・デバイス、ネットワークデバイスのセキュリティスコア
- ・デバイスの内訳 (脆弱, 改善が必要, 保護)
- ・セキュリティおよび運用上の問題に関する分析情報



Microsoft Defender for IoT - OT Sensor

攻撃ベクトル レポート



What is it?

悪用されるデバイスの脆弱性情報をもとに
攻撃ベクトルをリアルタイムで計算、
特定ターゲットへの攻撃実現可否を分析



Benefits

攻撃シミュレーションを実行することなくリスクを
評価し、攻撃シーケンスを軽減する情報を入手

The screenshot displays two main windows from the Microsoft Defender for IoT platform.

Attack Vectors (Top Window): This window shows a list of attack vectors for a simulation named "av1". The vectors are categorized by color: red, orange, and yellow. Each vector entry includes a device name, IP address, and target device name and IP address. For example, one red vector is "W10-LT-ENT 192.168.0.110 > U1-PLC1-R 10.0.100.104".

Vector	Source Device	Target Device	
W10-LT-ENT	192.168.0.110	U1-PLC1-R	10.0.100.104
HVAC-CTL	192.168.0.17	U1-PLC1-R	10.0.100.104
Unit1.RW_HMI	10.0.100.20	U1-PLC1-R	10.0.100.104
OT-JUMP	192.168.10.200	U1-PLC1-R	10.0.100.104
USPCU-EWS-S-P00	10.0.100.15	U1-PLC1-R	10.0.100.104

Devices Map (Bottom Window): This window shows a network topology for the "Subnets: Unit2-Rockwell (10.0.100.0/24)". It highlights the "Enterprise Supervisory" and "Supervisory Process Control" layers. A context menu is open over a device icon labeled "U1-PLC1-R". The menu options include:

- View Properties
- Unauthorize
- Mark as Non Important
- Show Events
- Activity Report (Last 1 Hour)
- Activity Report (Last 6 Hours)
- Activity Report (Last 12 Hours)
- Activity Report (Last Day)
- Simulate Attack Vectors
- Add to Custom Group
- Delete

Right Panel (W10-LT-ENT): This panel details a targeted attack sequence:

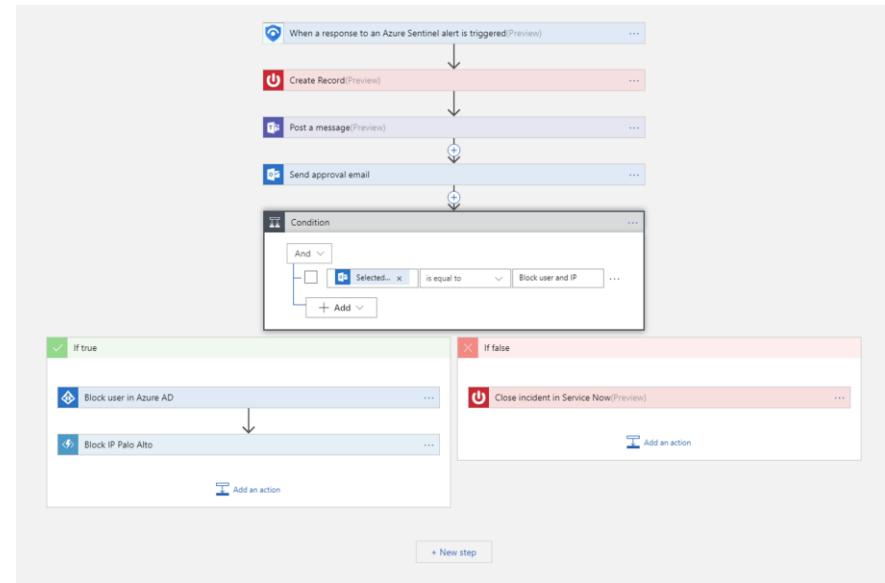
- INTERNET CONNECTION:** W10-LT-ENT is exposed to external threats due to internet connectivity.
- KNOWN CVE:** Device OT-JUMP has a known CVE vulnerability CVE-2016-3270 that can be exploited. Description: The Graphics component in the kernel in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1311, and 1607 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability".
- OUTDATED OS:** Device Unit1.RW_HMI is running Windows XP operating system, which is no longer supported and contains multiple known vulnerabilities with no security updates or hotfixes.
- KNOWN CVE:** Device U1-PLC1-R has a known CVE vulnerability CVE-2012-6437 that can be exploited. Description: Rockwell Automation EtherNet/IP products; 1756-ENBT, 1756-EWEB, 1768-ENBT, and 1768-EWEB communication modules; CompactLogix L322 and L336 controllers; 1788-ENBT FLEX Logix adapter; 1794-AENTR FLEX I/O EtherNet/IP adapter; ControlLogix 18 and earlier; CompactLogix 18 and earlier; GuardLogix 18 and earlier; SoftLogix 18 and earlier; CompactLogix controllers 19 and earlier; SoftLogix controllers 19 and earlier; ControlLogix controllers 20 and earlier; GuardLogix controllers 20 and earlier; and MicroLogix 1100 and 1400 do not properly perform authentication for Ethernet firmware updates, which allows remote attackers to execute arbitrary code via a Trojan horse update image.

Microsoft Defender for IoT - OT Sensor

Microsoft Sentinel (SIEM/SOAR) との連携

- IT/OT 境界を越えた攻撃を含む多段階攻撃を識別
- (OT に特化した) SOAR プレイブック

The screenshot shows the Microsoft Azure Sentinel Investigation interface. At the top, it displays the incident details: "No Traffic Detected on Sensor Interface", "High Severity", "New Status", and "Unassigned Owner". The last update time is listed as "11/4/2019, 6:35:22 AM". The main pane shows a network diagram with nodes: "PLC (BRISTOL BABCOOK INC.)", "Workstation", and "Router-CISCO". A red arrow points from the PLC node to a circular icon containing a shield, which is labeled "No Traffic...". Below the diagram, there is a detailed device information panel for the PLC, including its device name, IP address (192.168.1.1), MAC address (00:10:04:15:a2:11), vendor (BRISTOL BABCOOK INC.), firmware version (serial B4516909, model_address=3, model 400130-01-7), protocols (Emerson OpenBSI), model (1756-L234ER-QB123-LOGIX5327), and last seen (17:00 01.06.2020). The device type is listed as PLC.



Microsoft Defender for IoT - micro-agent



ソースコード

- プロジェクトの構築段階で micro-agent をファームウェアに組み込むことが可能
- ソースコードをカスタマイズし、必要なものだけを取り込むことが可能
- 操作系を絞った制限付きデバイスにも対応



バイナリ パッケージ

- 一般的な OS を搭載する IoT デバイスに対し、導入後のインストールをサポート

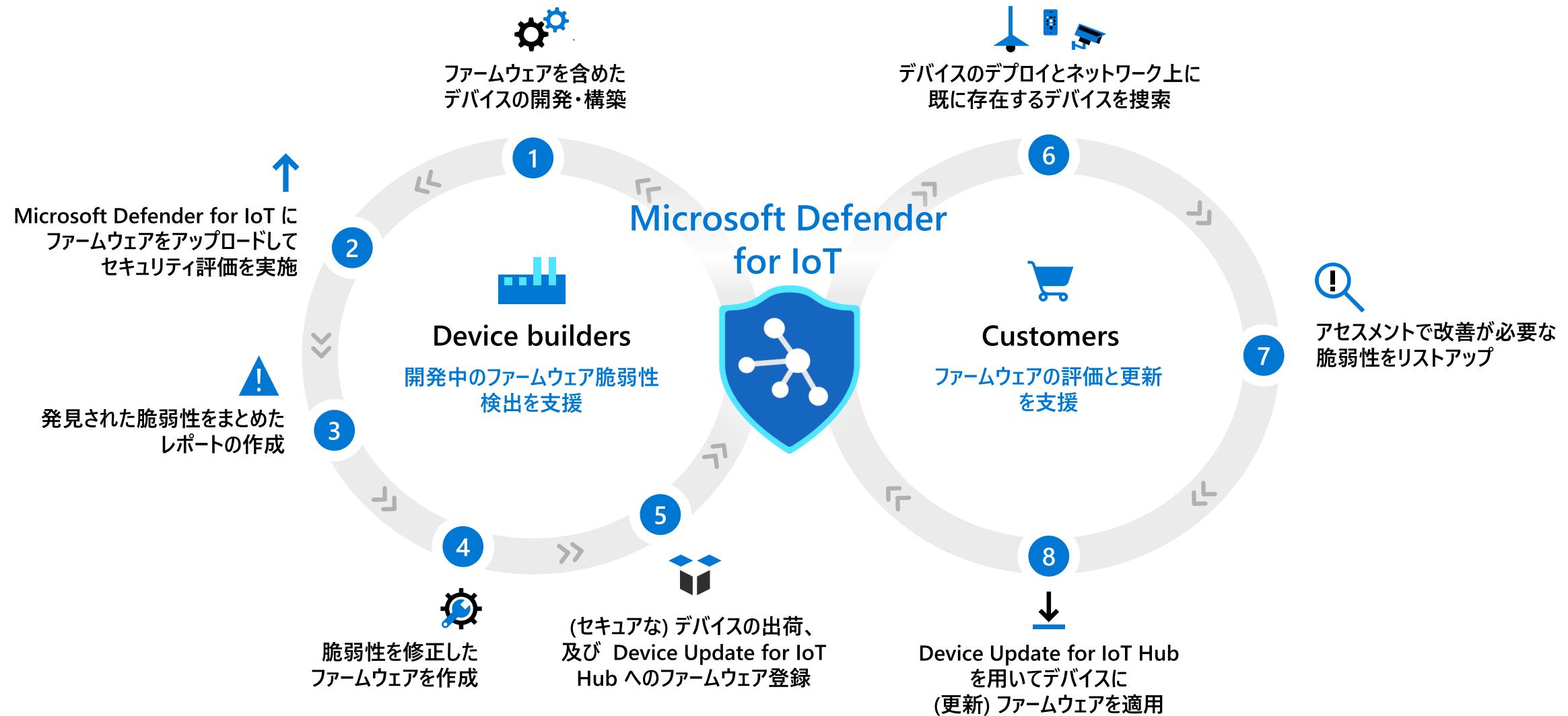


スタンドアローン、または Azure IoT と統合

- スタンドアローンエージェントとして、または Azure IoT エコシステムと統合してデプロイすることが可能
- Azure RTOS に組み込み
- Azure IoT Edge に統合

<https://docs.microsoft.com/ja-jp/azure/defender-for-iot/device-builders/overview>

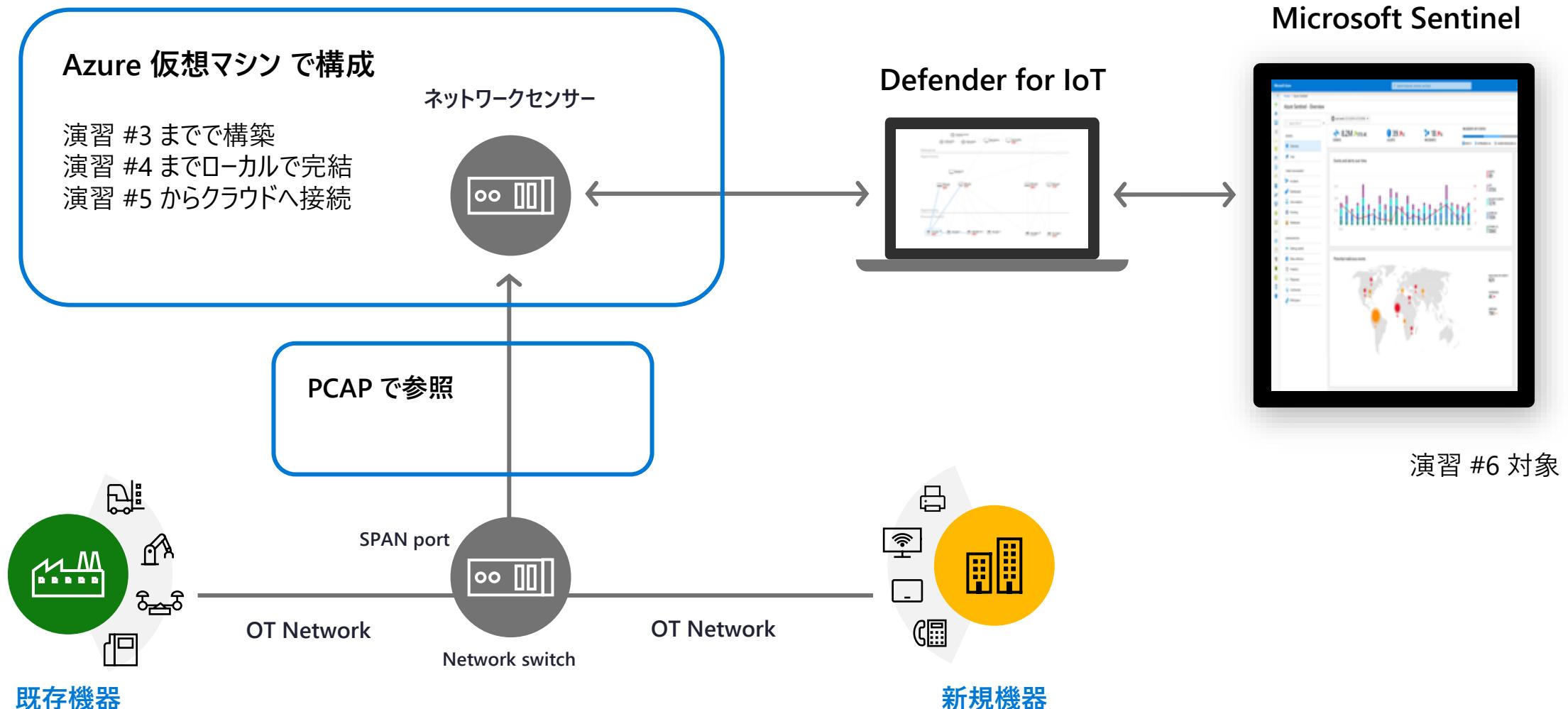
Defender for IoT に Refirm Labs サービスを統合



ワークショップについて



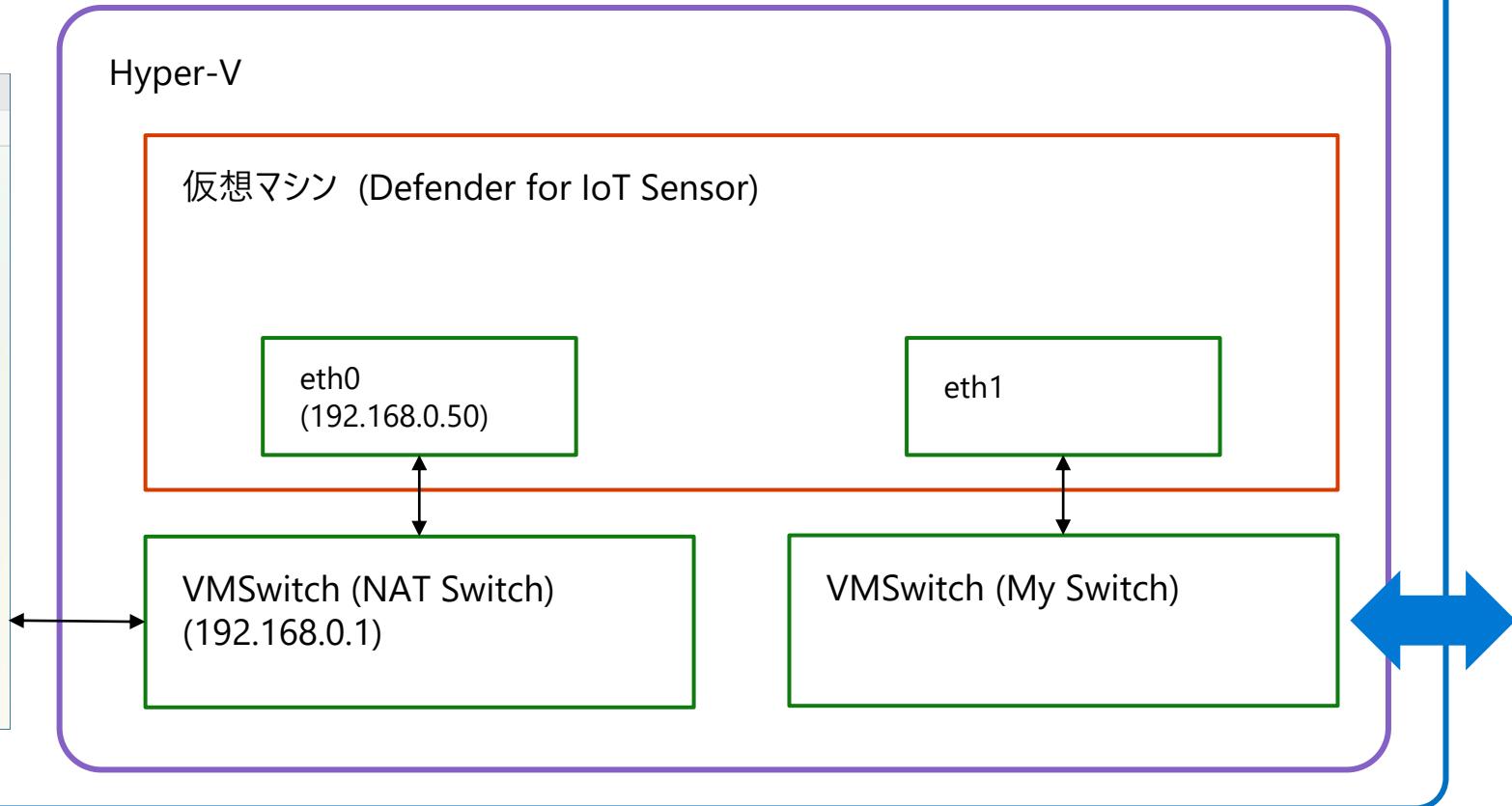
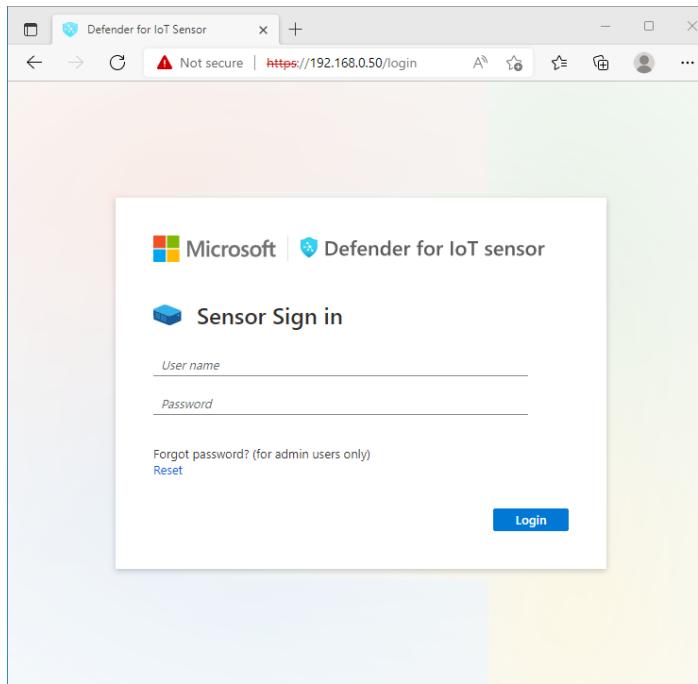
ワークショップ の構成



Defender for IoT - OT sensor に触れていただく

ワークショップ の構成 - 仮想マシン

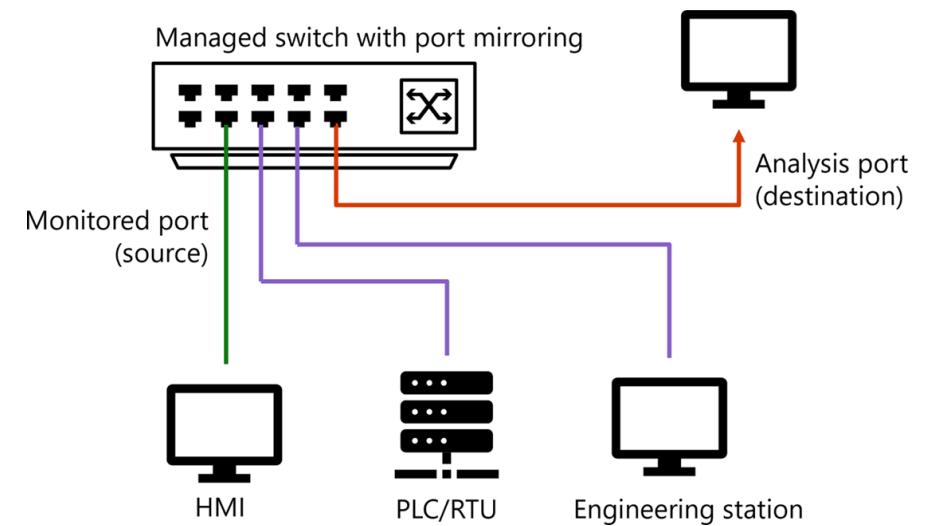
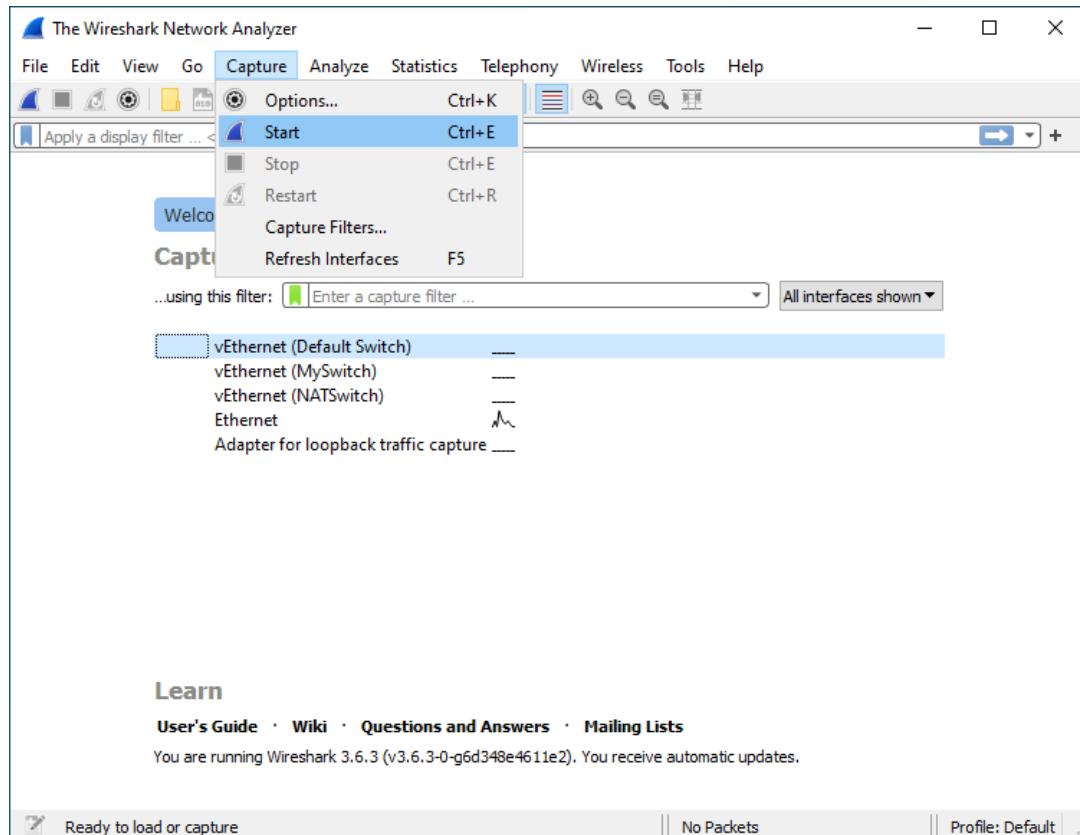
仮想マシン (Standard_D4s_v3) - Windows 10



RDP 接続

PCAP の取得について - Wireshark

- PCAP の取得 자체は比較的簡単
- 期待通りのキャプチャが可能なネットワーク構成を組む方がやや難しい



<https://docs.microsoft.com/ja-jp/azure/defender-for-iot/organizations/how-to-set-up-your-network>

Defender for IoT (sensor) 10.5.x / 22.1.x について

- 今後の新機能やクラウド連携の拡張は 22.x に対して実施 (日本語対応含む)
- 10.5.x もまだサポート中 (今回は 複数の PCAP ファイル利用のため、10.5.5 を利用)



<https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/release-notes>

ワークショップで用いる ファイル について

- <https://aka.ms/md4iotiso> # Defender for IoT 10.5.x の ISO ファイル
- <https://aka.ms/md4iotpcaps> # PCAP ファイル (解凍して利用)

