ADVANTECH

Enabling an Intelligent Planet

Advantech IT/OT Total Security Sales Kit

Rison.Yeh

Alex.Lai

Scan & Contact us

Ransomware, Vulnerabilities and Industrial Control Security

Colonial Pipeline boss confirms $4.4m ransom payment

19 May

Colonial Pipeline has confirmed it paid a $4.4m (£3.1m) ransom to the cyber-criminal gang responsible for taking the US fuel pipeline offline.

Its boss told the Wall Street Journal he authorised the payment on 7 May because of uncertainty over how long the shutdown would continue.

"I know that's a highly controversial decision," Joseph Blount said in his first interview since the hack.

The 5,500-mile (8,900-km) pipeline carries 2.5 million barrels a day.

According to the firm, it carries 45% of the East Coast's supply of diesel, petrol and jet fuel.

Chief executive Mr Blount told the newspaper that the firm decided to pay the ransom after discussions with experts who had previously dealt with DarkSide, the criminal organisation behind the attack.

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 June

The world's largest meat processing company has paid the equivalent of $11m (£7.8m) in ransom to put an end to a major cyber-attack.

Computer networks at JBS were hacked last week, temporarily shutting down some operations in Australia, Canada and the US.

The payment was reportedly made using Bitcoin after plants had come back online.

JBS says it was necessary to pay to protect customers.

In a ransomware attack, hackers get into a computer network and threaten to cause disruption or delete files unless a ransom in cryptocurrency is paid.

"This was a very difficult decision to make for our company and for me personally," said JBS chief executive Andre Nogueira.

Gang behind huge cyber-attack demands $70m in Bitcoin

5 July

The gang behind a "colossal" ransomware attack has demanded $70m (£50.5m) paid in Bitcoin in return for a "universal decryptor" that it says will unlock the files of all victims.

The REvil group claims its malware, which initially targeted US IT firm Kaseya, has hit one million "systems".

This number has not been verified and the exact total of victims is unknown.

However, it does include 500 Swedish Coop supermarkets and 11 schools in New Zealand.

Two Dutch IT firms have also been hit, according to local media reports.

Ransomware Attack Tactics & Tools

Phase I

Reconnaissance to gain initial access through phishing, remote desktop protocol (RDP) abuse, and exploiting known vulnerabilities.

Phase II

Lateral movement and privilege escalation by using legitimate tool to gain Domain Controller (DC) or Active Directory access, which will be used to steal credentials, escalate privileges, and acquire other valuable assets for data exfiltration.

Phase III

Download and install malware to start encryption process and lock down system.

INITIAL ACCESS

- Phishing email (attachments, links)
- Compromised RDP/valid accounts
- Exploits of public-facing application

CREDENTIAL ACCESS

- PowerShell
- Mimikatz
- LaZagne
- NetPass

DISCOVERY

- AdFind
- BloodHound
- Cobalt Strike
- SMB tool

LATERAL MOVEMENT

- AdFind
- BloodHound
- Cobalt Strike
- PsExec
- SMB tool

EXECUTION & IMPACT

Defense evasion tools

- **PC Hunter**
- **Process Hacker**
- **Revo Uninstaller**
- **BAT file**

Exfiltrate data & Deploy

- **MegaSync**
- **7-Zip**
- **PuTTY**

Advantech IT/OT Total Security

Comprehensive cybersecurity solution to prevent attacks, stop damage and restore operation

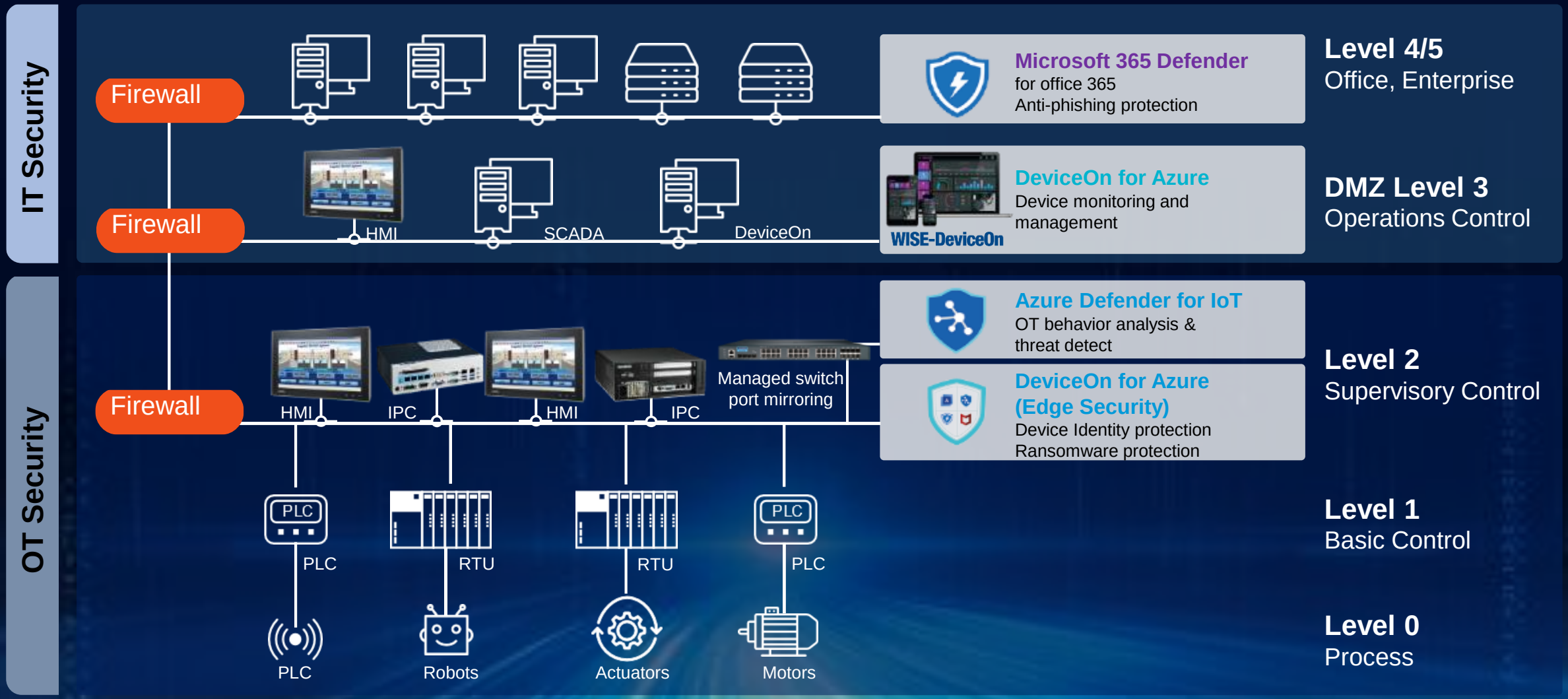
Extended Detection & Response (XDR)

- Anti-phishing & malware protection
- Secure email attachments/links
- Device Monitoring and Management
- Network segregation & protection

Endpoint Detection & Response (EDR)

- Container and software updates
- Secure Device Identity Protection (TPM 2.0)
- OT behavior analysis & threat detect
- Ransomware Protection & Recovery (McAfee)
- OOB Management & control (iBMC)

Purdue Model Compliant IT/OT Converged Network Defense

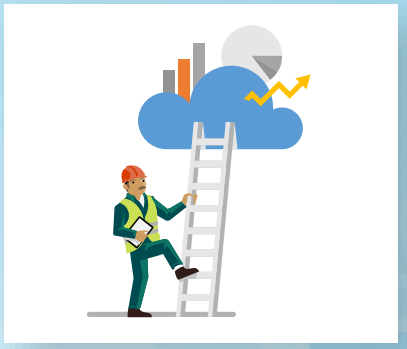


- Purdue Model (PERA) – 1990 reference model for enterprise architecture
- IEC-62443 – Standards for Industrial communication networks – IT security for networks and systems

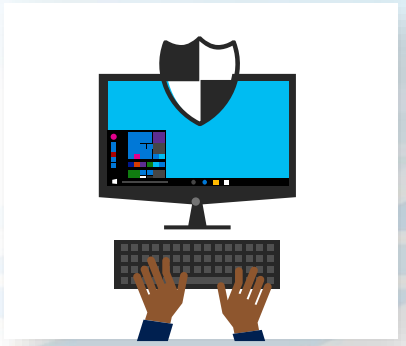
Microsoft 365 Business Premium

Exchange Teams SharePoint OneDrive Outlook Word Excel PowerPoint Publisher Access Intune Azure Information Protection Defender Conditional Access Windows Virtual Desktop

Anti-phishing

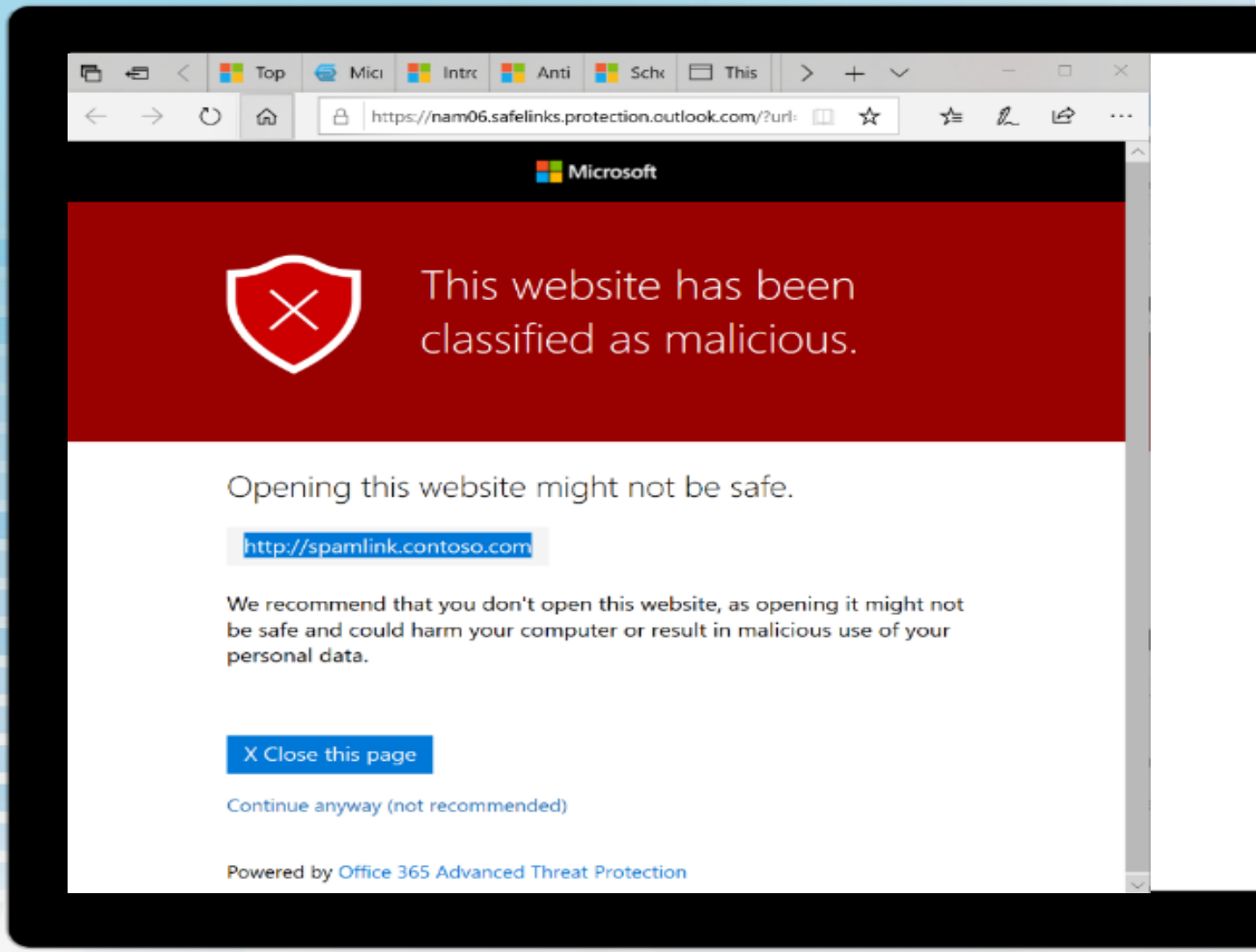


Safeguard confidential business data



Windows Defender

Secure Windows devices data



Global IoT/ICS Risk Report

Vulnerability data from 1,800+ industrial control system (ICS) networks

71%

Sites have outdated Windows versions no longer receiving security patches

64%

Have unencrypted passwords facilitating compromise

66%

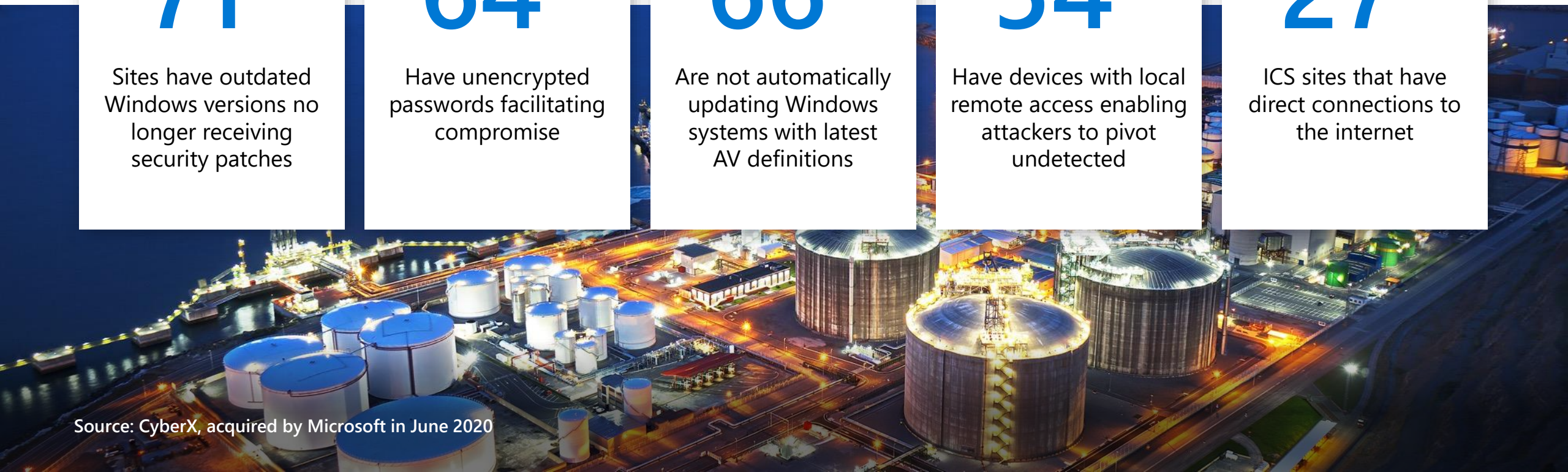
Are not automatically updating Windows systems with latest AV definitions

54%

Have devices with local remote access enabling attackers to pivot undetected

27%

ICS sites that have direct connections to the internet



Source: CyberX, acquired by Microsoft in June 2020

Azure Defender for IoT

Protecting, Monitoring all managed/ unmanaged OT devices

Azure Native Services

Azure Sentinel (optional)

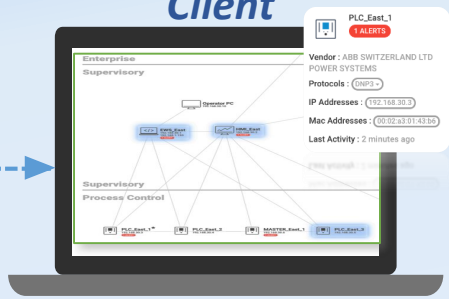
Simplify data collection across different sources, including Azure, on-premises solutions, and across clouds

Advantech Hardware + Defender for IoT

Sensor Gateway

SPAN port

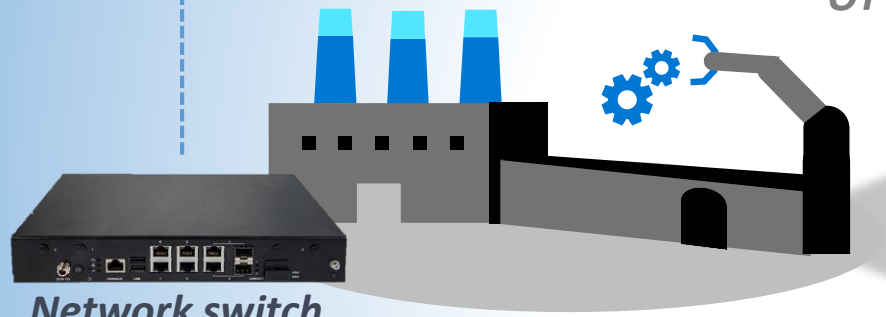
Client



Azure Defender for IoT

- Deep Packet Inspection (DPI)
- OT-aware behavioral analytics & threat intelligence
- Zero impact of implementation

Factory Brownfield



Network switch

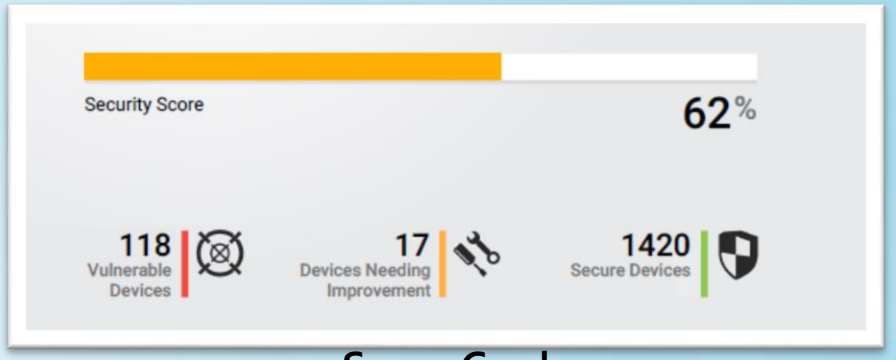
OT Networking

PLC

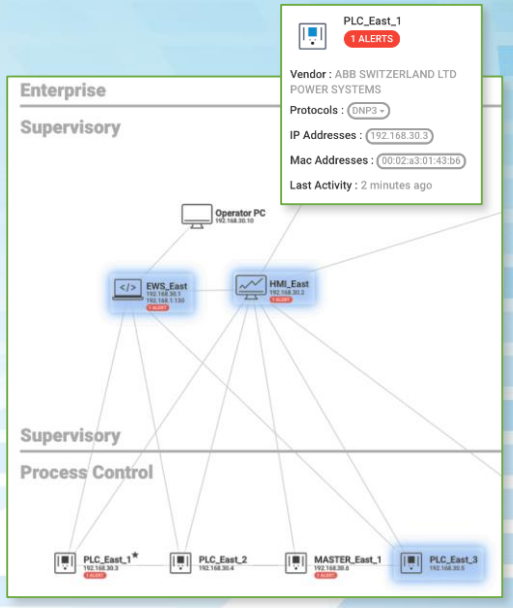
RTU

HMI

Azure Defender for IoT



Score Card

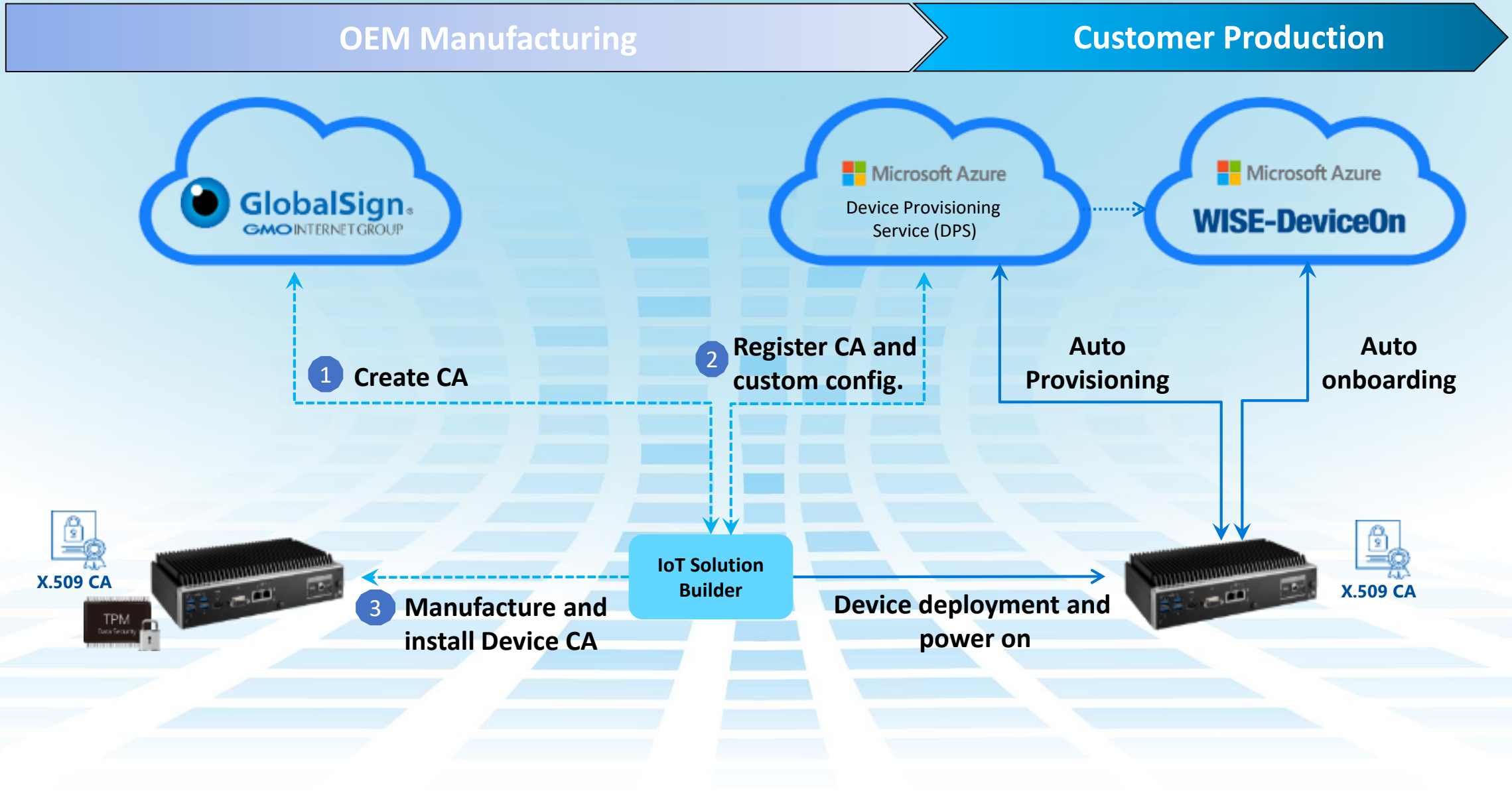


Agentless
Zero production impact roll in

Continuous visibility into
IoT/OT assets, vulnerabilities

DeviceOn Secure Device Identity

Secure Connection, Onboarding, Provisioning



Edge Security : Ransomware Protection and Recovery

Prevention & Protection

Ransomware & Malware Attack

Microsoft Azure

WISE-DeviceOn

Edge Security

Remote protection activation

Recovery

Encrypted files & Lock down system

One-click recovery back to normal

Acronis Active Protection
Ransomware detection & recovery

McAfee Application Control
Whitelisting protection

Acronis Backup
System backup & bare-metal recovery

OOB Management & Control
Remote recovery and power control

Traditional factory maintenance	WISE-DeviceOn
On-site disassembly and installation	Remote Operation
Single operation	Batch operation
Takes 1 WEEK to operate 100 devices (2 p)	Takes 1 HOUR to operate 100 devices (1 p)

90%

Efficiency improvement

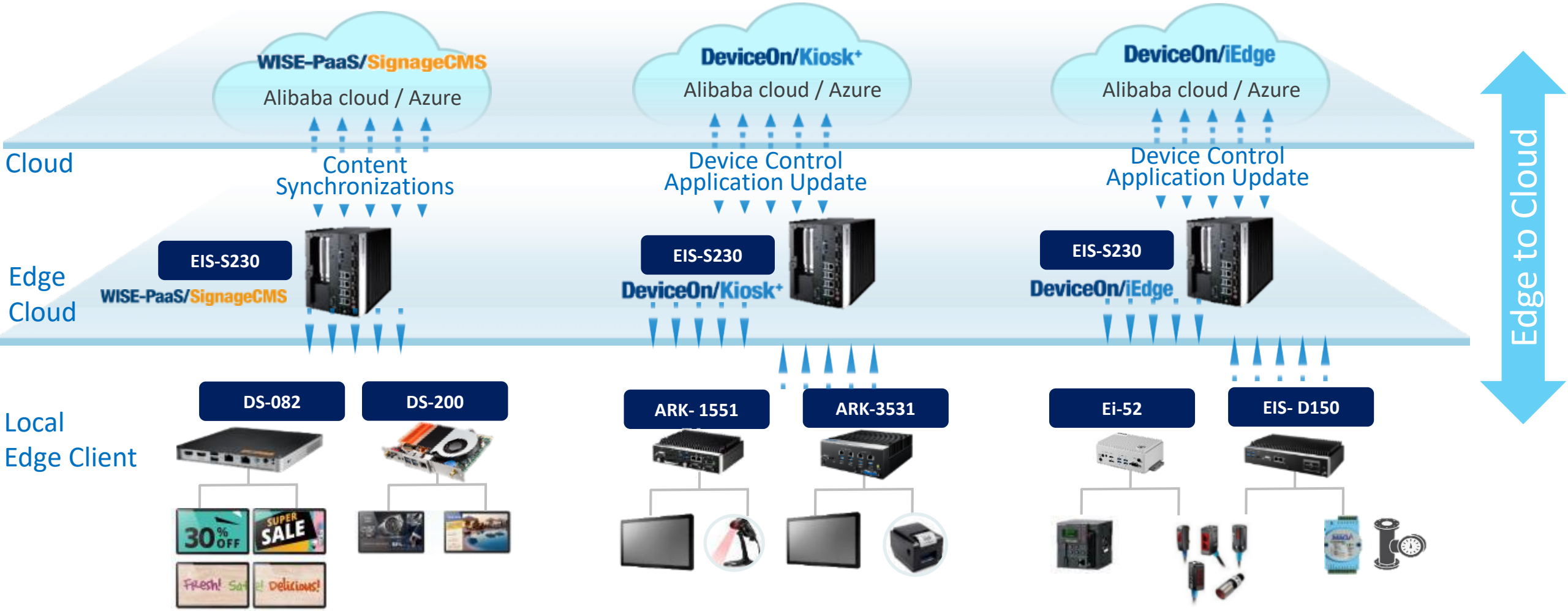
Co-Creating the Future of the IoT World

Defender for IoT Support Protocol

DeltaV	BACnet	ROC
EtherNet/IP	DNP3	GOOSE
ABB Totalflow	EMERSON ROC	OVATION ADMD
AMS	FOXBORO I/A	Yokogawa
OPC	HONEYWELL	IEC 60870-5-104
SIEMENS-S7	MMS	TOSHIBA COMPUTER LINK
SRTP	MODBUS	VLAN
SUITELINK	OASYS	…

Azure Defender for IoT supports a broad range of protocols across diverse industrial equipment. For custom or proprietary protocols, Microsoft offers an open SDK for easy development, testing, and deployment of custom protocol dissectors as plug-ins, without divulging proprietary information about how protocols are designed or sharing PCAPs that may contain sensitive information.

EIG Integrated Edge to Cloud Solutions



Edge manageability iBMC, whitelist and backup service

MIC-770W V2

- ✓ Remote management: power on/off, reset, force shutdown, etc. when OS crashed
- ✓ IEM SI service upgrade
- ✓ McAfee, Acronis lite DeviceOn bundle version

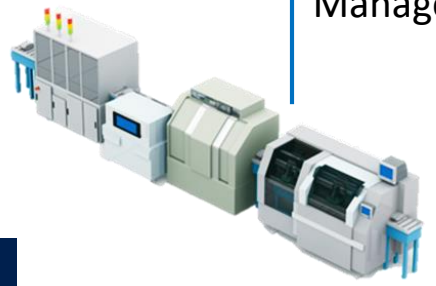
McAfee™ Acronis

WISE-DeviceOn *iBMC*

IEM SI control room

In-band Management

Out-of-band Management

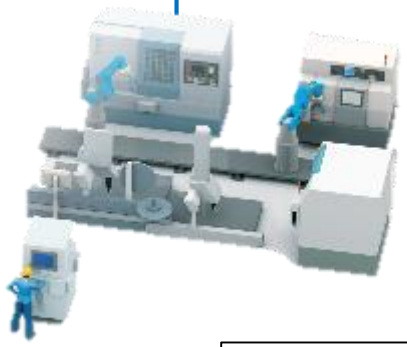


iBMC

End user A

In-band Management

Out-of-band Management



iBMC

End user B

ADVANTECH