How to Secure IoT Gateways from Cyberattacks

Solution eBook

ADVANTECH

Gateway security is critical in IoT ecosystems because gateways are a key point for collecting data in any connected application. As such, ensuring the security of IoT gateways is of paramount importance. But how to ensure security of IoT gateways? Facing a global increase in cyberattacks, Advantech is applying its experience to understanding information security vulnerabilities in industrial applications. In response, the company is providing IoT gateway hardware and software integrated security solutions and services in response.

Data & System Security

Identity & Access Control

Over-the-Air Updates and Secure Boot

Threat Detection & Recovery

Advantech IoT Gateway Security Solutions & Services

Public & Private Cloud

Edge to Cloud Security

DeviceOn for Azure

- Remote prevention, control & recovery for cyber security
- 10,000+ scalable, cross-geo monitoring, control, OTA
- Azure IoT Edge & PnP edge apps by use case

Acronis Cyber Protect

Acronis

- One-key disaster recovery, instant failover
- Active protection against ransomware
- Centralized management of hybrid cloud deployment

3rd Party Cloud Integration

aws

Alibaba Cloud

Applications & APIs

Device Lockdown Utility

ubuntu

- Unified write filter
- Keyboard & USB filter
- Update policy mgmt

Device Operation and Mgmt

DeviceOn

- HW & SW monitoring
- Device abnormality detection
- Remote diagnostics

Embedded Security Solution

McAfee

- Configuration toolkit
- Whitelist protection
- No virus code needed

Backup & Recovery Solution

Acronis

- Whole system backup
- Incremental backup
- One-key recovery

OT Behavior Analysis & Threat Detecting

Azure Defender for IoT

- Message screening
- Threat identification
- Risk notification

Operating Systems

ubuntu

- Security hardening toolkits
- Live patch service w/o rebooting
- Extended security maintenance

Windows

- UEFI Secure Boot
- Security Update
- WHQL testing
- Defender

VxWorks | QNX | CentOS | Yocto

IoT Gateway Devices

Multi-Layer Security

- Storage security
- Boot management
- Boot Guard, BIOS Guard

Onboard TPM (trusted platform module) 2.0

In-Chassis Add-On USB Security Dongle Support

By subscription

ADVANTECH

Advantech Select IoT Gateway Portfolio

Compact Gateway
for 5G & AI Applications

EI-52
- Ready-to-use powerful system
- Plug-in 5G & AI computing
- EdgeX edge-to-cloud connectivity

Slim Gateway
for Self-Service Kiosks

ARK-1551
- Intel® 8th Generation Core™ i5
- 4 x USB 3.1, 2 x GbE, 4 x COM
- Flexible storage support

DIN Rail Gateway
for Smart Automation

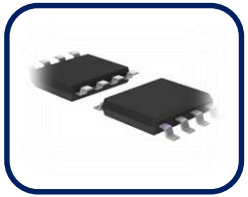
ARK-1221
- Rugged design w/DIN rail mounting
- DDR4 memory up to 32GB
- 4 x TSN 2.5G LAN ports

OPC UA Gateway
for Environment Monitoring

EIS-D210
- Ultra palm-size
- Sensor & device connectivity
- iEdge for data & device mgmt.

Hardware Security Highlights

BIOS & Storage



Solidified SPI

- SPI data solidified
- Authority control
- Secure flash

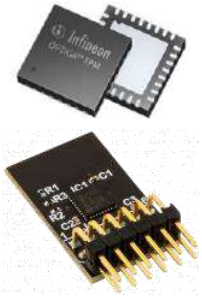
Storage Security

- HDD password
- Storage encryption
- Configuration tool

Booting Management

- Keyboard/mouse only
- Certified device
- Secure boot

TPM 2.0



Highest Security for Platform Protection

- Independently evaluated and certified security:
  - Common Criteria EAL 4+ (international standard)
  - FIPS 140-2 Level 2 (US standard)
  - Combined certification for easier logistical handling
- RNG, tick-counter, dictionary attack lock-out
- Built-in algorithms including RSA, ECC, SHA-256, AES

Physical Security Key

In-chassis physical security key

- Protected in-chassis space available for physical keys with different form factors
- Supports toughest two-factor authentication (2FA)
- Physical key bundled chip contains codes and protocols for identification

ADVANTECH

Embedded OS Level Security

Windows

UEFI Secure Boot

Secure Boot for Windows is a standard developed by OEM to help make sure that a device boots using only software that is trusted by OEM. When the PC starts, the FW checks the signature of each piece of boot software, including UEFI FW drivers, EFI applications, and the OS.

Security Updates & Long-Term Support

Microsoft releases security updates monthly. These updates address various issues and vulnerabilities that are being exploited in the wild.
Windows 10 IoT Enterprise LTSC, which receives 10 years of support.

WHQL Testing

Windows Hardware Quality Labs Testing is Microsoft's testing process. It involves running a series of tests on third-party device drivers and then submitting the log files from these tests to Microsoft for review. The procedure may also include Microsoft running their own tests on a wide range of equipment. Products passing WHQL tests means that the hardware or software has undergone some share of testing by Microsoft to ensure compatibility.

Windows Defender

The virus & threat protection section contains information and settings for antivirus protection from Microsoft Defender Antivirus and third-party AV products.

ubuntu

UEFI Secure Boot

On Ubuntu, all pre-built binaries intended to be loaded as part of the boot process are signed by Canonical's UEFI certificate, which itself is implicitly trusted by being embedded in the shim loader, which has been signed by Microsoft. When the PC starts, the FW checks the signature of each piece of boot software, including UEFI FW drivers, EFI applications, and the OS.

Security Updates & Long-Term Support

Security updates are provided for 10 years for long-term support (LTS) releases. With the default configuration for unattended upgrades (16.04 and after), these updates are applied to your system automatically. Ubuntu LTS receives 10 years of support (includes an additional 5 years with the paid ESM service).

Ubuntu HW Certification

Canonical has developed rigorous certification tests to ensure compatibility between hardware and the Ubuntu operating system. A full battery of tests is performed on each hardware and software component for robustness before a device earns the distinction of being Ubuntu certified. With regular regression testing, Ubuntu certified hardware is continuously tested in a lab to ensure the latest updates work well on the certified device.

Linux Kernel Self-Protection

Kernel self-protection is the design and implementation of systems and structures within the Linux kernel. It is aimed at protecting against security flaws in the kernel itself. This covers a wide range of issues, including removing entire classes of bugs, blocking security flaw exploitation methods, and actively detecting attack attempts.

ADVANTECH

Secure Gateway Lifecycle Management

Onboard, Configure, Monitor, Update, Retire

WISE-DeviceOn

Empowers Edge Intelligence

Plan

Device Onboarding & Registration

- ✓ Zero-touch onboarding
- ✓ Batch import, provisioning & configuration
- ✓ Device migrate, transfer, replace & retire

Data Acquisition & Visualization

- ✓ Device real-time & historical data
- ✓ Built-in WISE-PaaS/Dashboard

Device Monitoring & Diagnostics

- ✓ Hardware & software monitoring
- ✓ Power management
- ✓ Remote troubleshooting
- ✓ Backup/recovery, protection
- ✓ Windows 10 lockdown (security & protection)
- ✓ Device anomaly detection (rule engine)
- ✓ Notifications & alerts

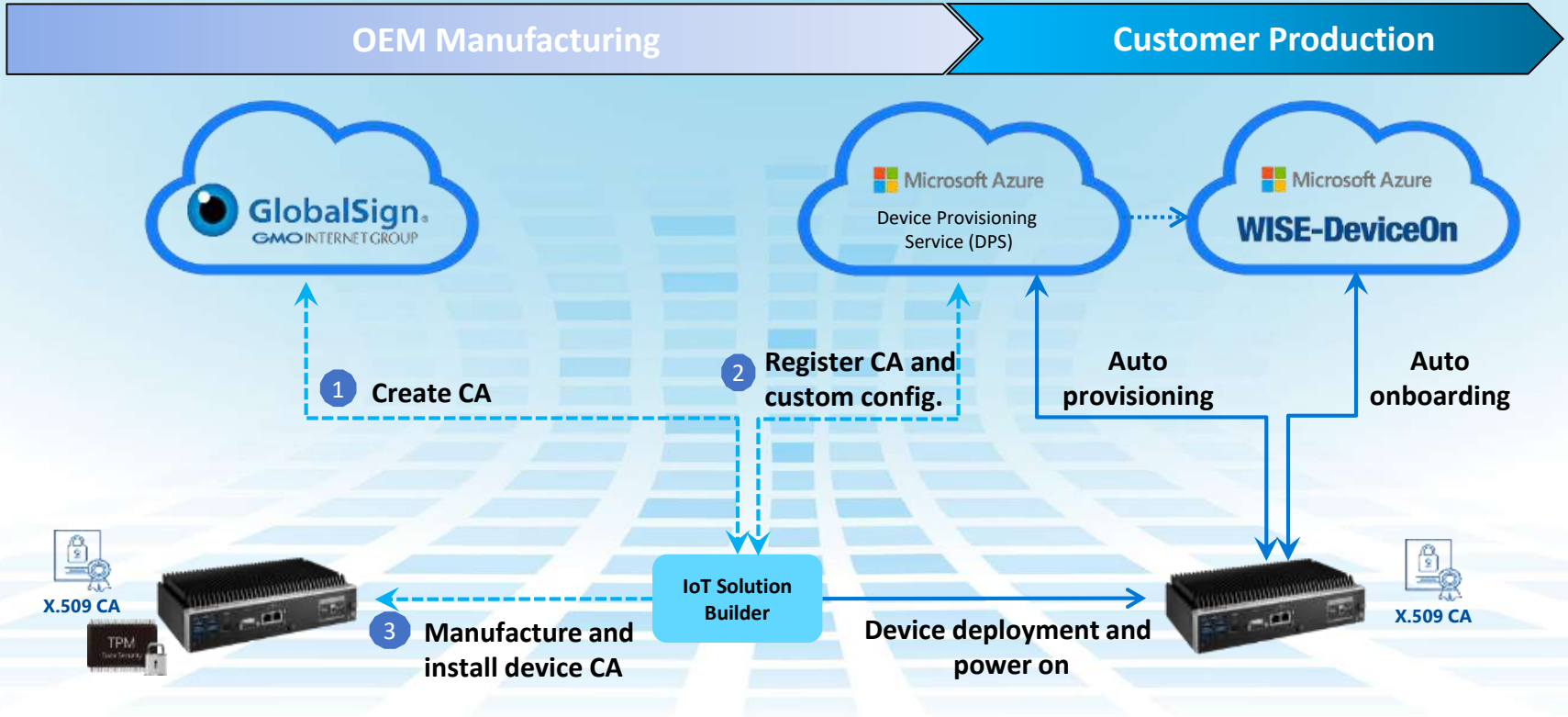
Device SW Updates & Maintenance

- ✓ Software, firmware & configuration updates
- ✓ Advantech BIOS updates
- ✓ App store & management

EOL

Secure Gateway Identity

Secure Connection, Onboarding, Provisioning

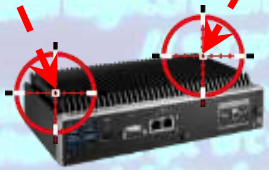


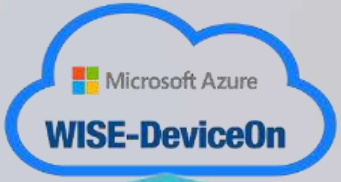
ADVANTECH

Ransomware Protection & Recovery

Prevention & Protection

Ransomware & Malware Attack





Edge Security

Remote protection activation

One-click recovery back to normal

Recovery

Encrypted files & Lock down system

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

Acronis / McAfee for Data Safety and Security

Acronis

Acronis Cyber Protect
Integrated Cyber Protection

Reliable backup and recovery

+

Next-generation cybersecurity and anti-ransomware

+

Enterprise protection management

McAfee

McAfee Whitelisting Solution

Prevent from "unauthorized' application installation

+

Access rights control – who, when, what.

+

Manage McAfee configurations and policies from a single location

Acronis Cyber Backup
Easy, Efficient, and Secure Protection

- Superior data protection: 20+ platforms protected
- Fast, reliable recovery
- The most secure backup with built-in anti-ransomware protection

Acronis True Image
Cyber Protection for Small Environments

- Cyber protection solution for up to 5 workstations
- Special editions targeting specific OEM needs: disc cloning, one-click factory reset, advanced backup

McAfee Application Control

Application Control

McAfee Application Control w/ePO

Application Control	ePO

McAfee Embedded Control

Application Control	Change Control

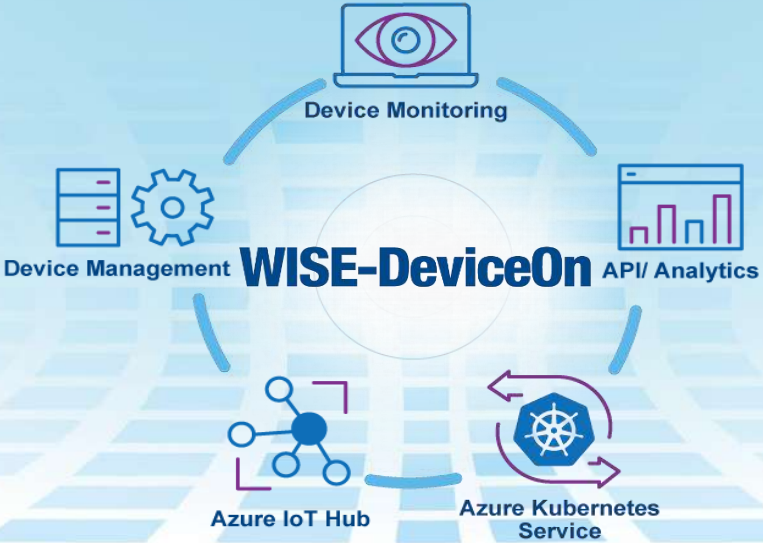
McAfee Integrity Control

Application Control	Change Control	ePO

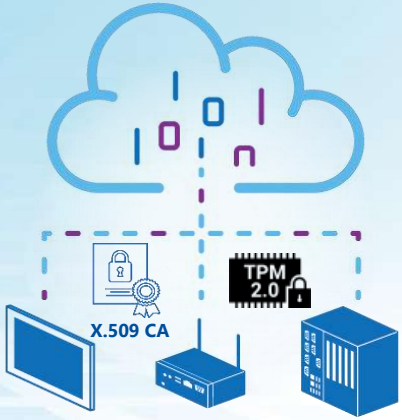
DeviceOn For Azure – Edge-to-Cloud Security

Edge to Cloud Security
Prevent, Control, Recover

10,000+ Scalable, Cross-Geo
Monitoring, Control, OTA



Azure IoT Edge & PnP
Edge Apps by Use Case



Freemium for Advantech HW or Advantech Azure CSP
Manufacturing, Retail, Healthcare + Microsoft/Azure Ecosystem

Azure Defender for IoT

Protect & Monitor 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

Secure Gateway

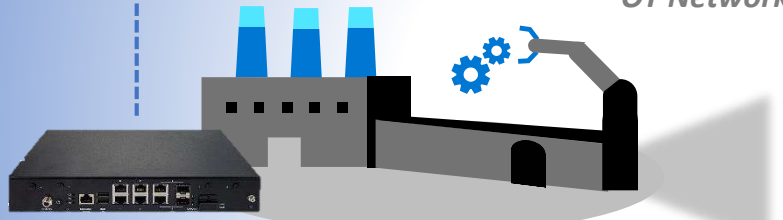
Client

SPAN port

Azure Defender for IoT

- Deep packet inspection (DPI)
- OT-aware behavioral analytics and threat intelligence
- Zero impact of implementation

Factory Brownfield



OT Networking

Network switch

PLC

RTU

HMI

EI-52 *Compact Gateway for 5G & AI Applications*

PHASE IN	2021 / JUNE

LONGEVITY	2027 / Q4

Plug & Play System Design

Easy start-up and configuration for IoT deployment
11th Gen Intel® delivers powerful computing in a compact package with built-in SSD/memory

Edge-to-Cloud Interconnection

Integrated software architecture and low-code integration
Sensing data integration and built-in remote device management software

RF Certified 5G and Wi-Fi[1,3] Platform

Compatible Wi-Fi and 5G modules achieve faster throughput
RF CE-RED and FCC system-certified ready with AIW-355 and EWM-W189H02E

5G WiFi and AI Platform Ready

Compatible AI acceleration module with Intel® Movidius™ Myriad X VPU
Compatible Wi-Fi and 5G modules achieve faster throughput and higher traffic capacity

AIW-355
5G Module

VEGA-330
AI Module

EWM-W189
802.11AC/a/b/g/n
WLAN + BT 5.0

11th Gen Intel® Core™ i5-1145G7E
4 cores, 8 threads, 8M Smart Cache, up to 4.1 GHz

11th Gen Intel® Core i3-1115G4E
2 cores, 4 threads, 6M Smart Cache, up to 3.9 GHz

11th Gen Intel® Celeron 6305E
2 cores, 2 threads, 4M Smart Cache, up to 1.8 GHz

EDGEXFOUNDRY™
WISE-DeviceOn

ARK-1551 *Compact System for Automation Control & Kiosks*

PHASE IN	2020 / JUNE

LONGEVITY	2026 / Q2

Compact yet High Performance

- Intel 8th Gen. Core i5 processor
- Powerful graphics platform with 4K2K HDMI

Multiple Storage Options

- 1 x removable HDD/SSD drive bay
- Supports dual storage, including 2.5" SATA & mSATA
- Supports SQF NVMe Storage (mPCIe / M.2 2230 E key)

Industrial Design & I/O Interfaces

- 12~28 V_{DC} input
- -20~55 ℃ operating temperature support
- 4 x RS-232/422/485, 8-bit DIO

8th Gen Intel® Core™ i5-8365UE
4 cores, 8 threads, 6M Smart Cache, up to 4.1 GHz

8th Gen Intel® Core i3-8145UE
2 cores, 4 threads, 4M Smart Cache, up to 2.4 GHz

8th Gen Intel® Celeron 4305UE
2 cores, 2 threads, 4M Smart Cache, up to 2.0 GHz

WISE-DeviceOn

ARK-1221 *DIN Rail System for Gateway and Edge Computing*

PHASE IN	2022 / JUNE

LONGEVITY	2027 / Q2

Small yet Smart and Strong

- Intel Atom x6413E Quad Core CPU
- Dual-channel DDR4 memory up to 32GB
- Operation temperature from -40 to 60 ℃
- Wide power input range 12 to 28 V_{DC}

High Speed I/O & Device Support

- Supports 2.5Gbps LAN
- 2 x USB 3.2 ports
- 1 x M.2 2280 B key NVMe

Security Features

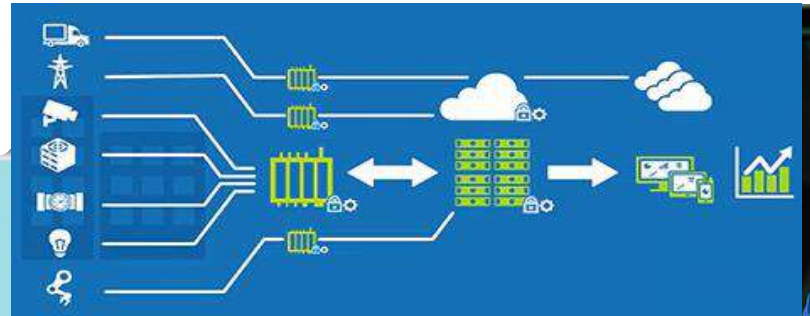
- Internal USB 2.0 type A for security dongle
- Modular TPM design
- McAfee white list protection & Acronis backup bundled
- DeviceOn/iEdge for provisioning & onboarding

8th Gen Intel® Core™ i5-8365UE
4 cores, 8 threads, 6M Smart Cache, up to 4.1 GHz

8th Gen Intel® Core i3-8145UE
2 cores, 4 threads, 4M Smart Cache, up to 2.4 GHz

8th Gen Intel® Celeron 4305UE
2 cores, 2 threads, 4M Smart Cache, up to 2.0 GHz

DeviceOn/iEdge



EIS-D210 *OPC UA Gateway for Environment Monitoring*

PHASE IN	2018 / JUNE

LONGEVITY	2024, Q1

Intel® Celeron N3350
2 cores, 6W, 1.1 GHz turbo boost, up to 2.4 GHz

Preconfigured Edge Gateway

- Easy start-up and configuration for IoT deployment
- Intel Atom N3350 CPU with essential IO ports for IoT gateways

Smart IoT Connectivity

- Integrated software architecture and low-code integration
- Data integration and industrial protocol support (OPC UA/MQTT/Modbus)

Edge-to-Cloud Management

- DeviceOn/iEdge provides device monitoring and edge cloud management
- Public cloud service support (Advantech WISE-PaaS, Azure and AWS)

DeviceOn/iEdge

Co-Creating the Future of the IoT World