ADVANTECH WISE-DeviceOn

Defend Your Business against Ransomware and Cyberattacks

White Paper
Advantech IT/OT Total Security

Table of Contents

Introduction

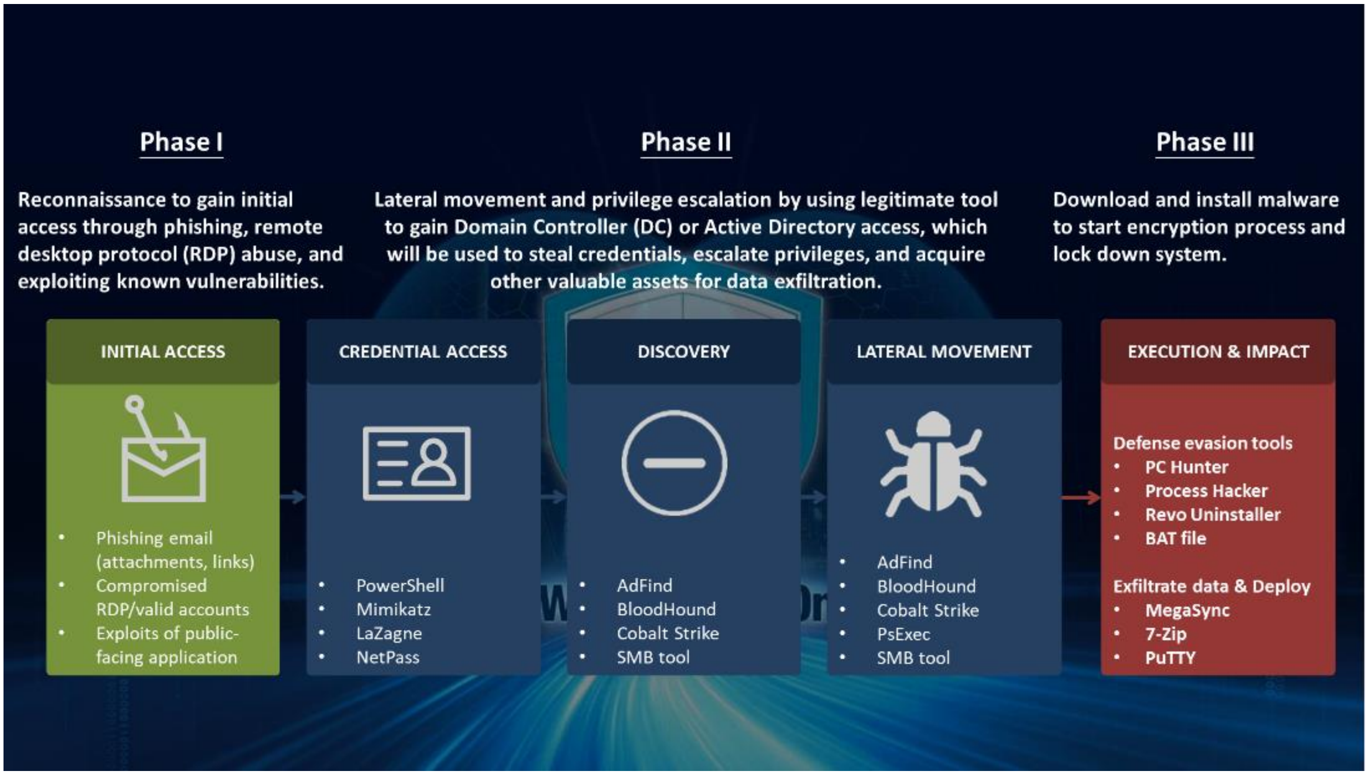
The IoT ecosystem continues to expand in all occupations. Connecting devices to the Internet brings diversified business applications, such as asset performance management (APM) in automated production, supply chain management (SCM) in process manufacturing, and tracking management in the logistics. To increase commercial competitiveness, enhance product capacity, and decrease costs, all of these applications must integrate IT, IoT, and OT technologies while introducing new applications. Analogously, industrial control systems (ICS) in manufacturing are based on OT technology, and have moved from closed to open networks. This has increased the threat of unexpected information security risks and breaches.

Indeed, major hacking incidents directed at companies are frequently appearing in the headlines. This demonstrates that hacking and ransomware attacks are a real and rapidly growing threat. Likewise, hacker organizations are more organized and systematic. Seeking to extort higher ransoms quickly, these organizations have shifted their attention to very specific enterprises and OT manufacturers.

Accordingly, the cyber security threat environment for IT and OT has become increasingly dire. Strengthening the awareness of information security, and improving information security defenses, from IT to OT, is now an imperative for enterprises.

In addition, companies need to respond through a variety of security controls, including real-time monitoring and rapid prevention/protection measures.

Ransomware Attack Tactics and 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

Let’s analyze the strategies and tools used in ransomware attacks. In general, the main tactics used in these attacks are roughly the same. There are more than 300 continually evolving attack methods or tools.

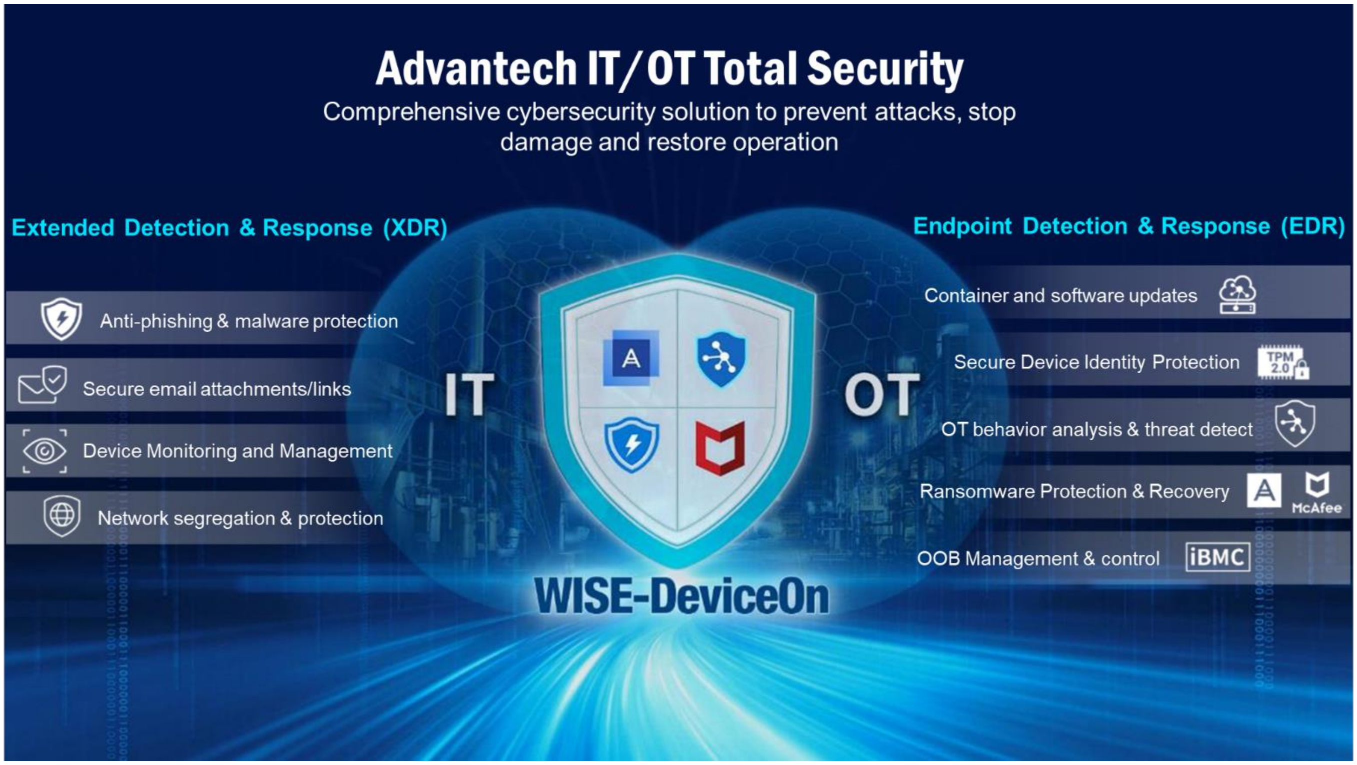
Attacks are divisible into three strategic stages:

Stage one: The attackers investigate the company to determine whether the target is worth the attack, in terms of difficulty and potential profit. Initial access may be obtained simultaneously through phishing emails, brute force cracking, RDP desktop sharing accounts, or open web application vulnerabilities.

Stage two: After the attacker obtains initial access, they use breaches to invade the internal network. In order avoid detection by internal anti-virus software, the attacker will avoid activating the virus malware at this stage. Instead, they’ll use legitimate tools, such as Powershell or Rootkit, to perform lateral movements, explore AD account servers to escalate privileges, gain more device control, and attempt to obtain internal confidential information. Finally, they will establish ransomware download and data upload channels.

Stage three: At this stage they will choose a suitable time — eg. target a company's off-hours before a long weekend to download the virus and launch a zero-day attack. During this attack, they will start to encrypt important information and lock systems and devices. This will force the company to pay a ransom, usually in cryptocurrency.

Advantech IT/OT Total Security

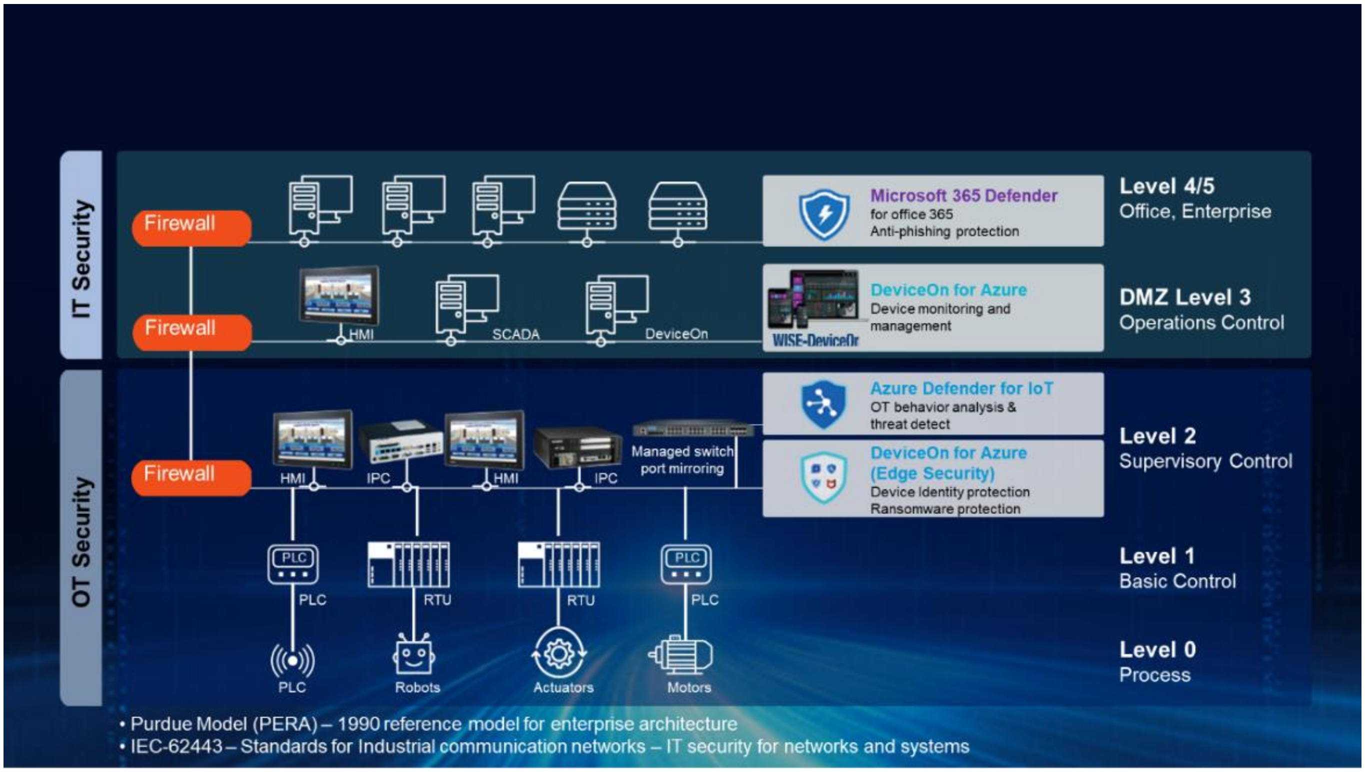

Advantech IT/OT Total Security
Comprehensive cybersecurity solution to prevent attacks, stop damage and restore operation
Extended Detection & Response (XDR)
Anti-phishing & malware protection
Secure email attachments/links
Device Monitoring and Management
Network segregation & protection
IT
OT
Endpoint 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
WISE-DeviceOn

Advantech collaborates with IT and security partners from various fields — including Microsoft, Acronis and McAfee — to provide a comprehensive solution that resists ransomware and protects systems from attacks by hackers. This solution is based on the DeviceOn platform, and integrates some security technologies from different aspects of IT and OT.

This solution further delivers core device management services to the IT side. These services help monitor the devices' software and the health status of key hardware components at any time. Likewise, these services strengthen IT boundary security protection, network isolation/segregation, remote control security, device identity management, and anti-phishing mechanisms.

This solution uses OTA updates to keep devices up to date with the latest software and security patches. Combined with the hardware's trusted security module (TPM), it provides a device identity that establishes a secure network connection with the central system. In addition, it is equipped with an OT network security monitoring system that continuously monitors the OT device network behavior for abnormalities. Finally, it cooperates with corresponding edge security solutions — such as remote protection, disaster recovery, and OOB management — creating a complete, effective, and secure safety net.

Purdue Model Compliant 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

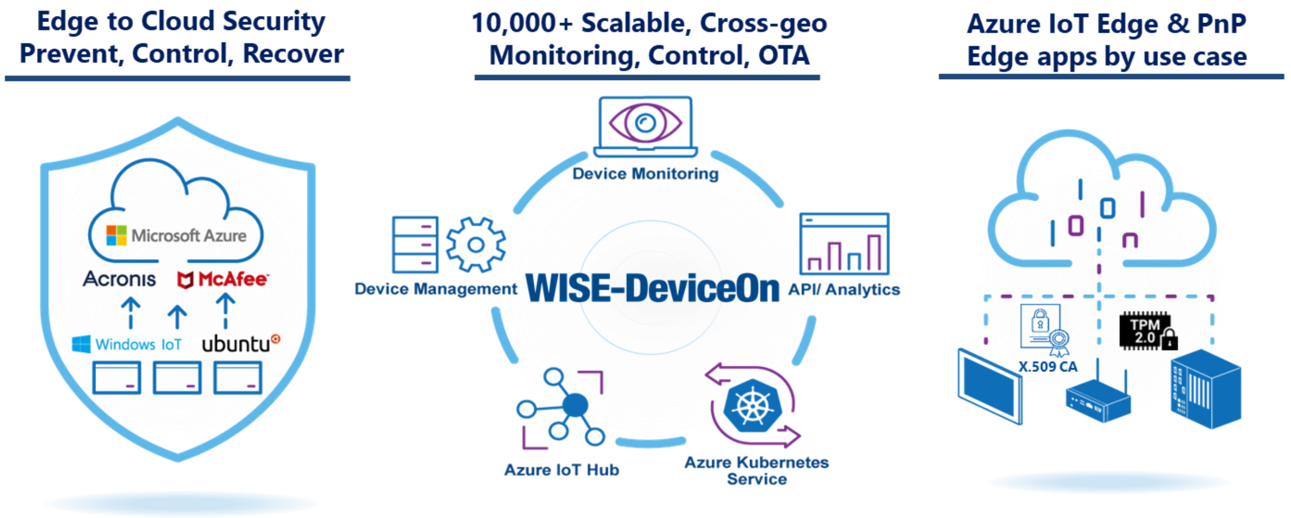
The entire IT-OT converged solution complies with IEC62443 and Purdue Model network architecture industrial control security standards and recommendations. This model enables users to plan and organize physical network segmentation in its entirety and configure the corresponding solution to the appropriate network segment. This in turn empowers security management at different network levels by dividing the user’s assets.

The Purdue Model network architecture configures external network security protection at the IT layer by dividing assets such as M365 Defender and DeviceOn. This facilitates connection between IT and OT, while providing a secure external management channel. It also enables the integration of OT-side security solutions, such as Azure Defender for IoT and DeviceOn related Edge Security solutions to ensure your edge system integrity.

IoT Management Optimized for Securing Production Environments

The development of IoT has increased the use of edge devices in many industries. These devices create solutions that improve machinery/product reliability, prevent cyber threats by strengthening device security access-control, and ensure smooth operation by reducing equipment failure. WISE-DeviceOn reorganizes software architectures to decouple data and services. In addition, it uses a containerized architecture to integrate with AKS (Azure Kubernetes service) and other PaaS services — yielding a complete solution with high scalability, availability, security, and reliability.

Device Management via Azure Cloud (DeviceOn for Azure)



Advantech WISE-DeviceOn is now fully integrated with Azure Cloud. Wise-DeviceOn can support large projects with hundreds of thousands of devices while addressing performance management concerns via the cloud’s capacity for auto scaling, high availability, advanced security, and rapid deployment.

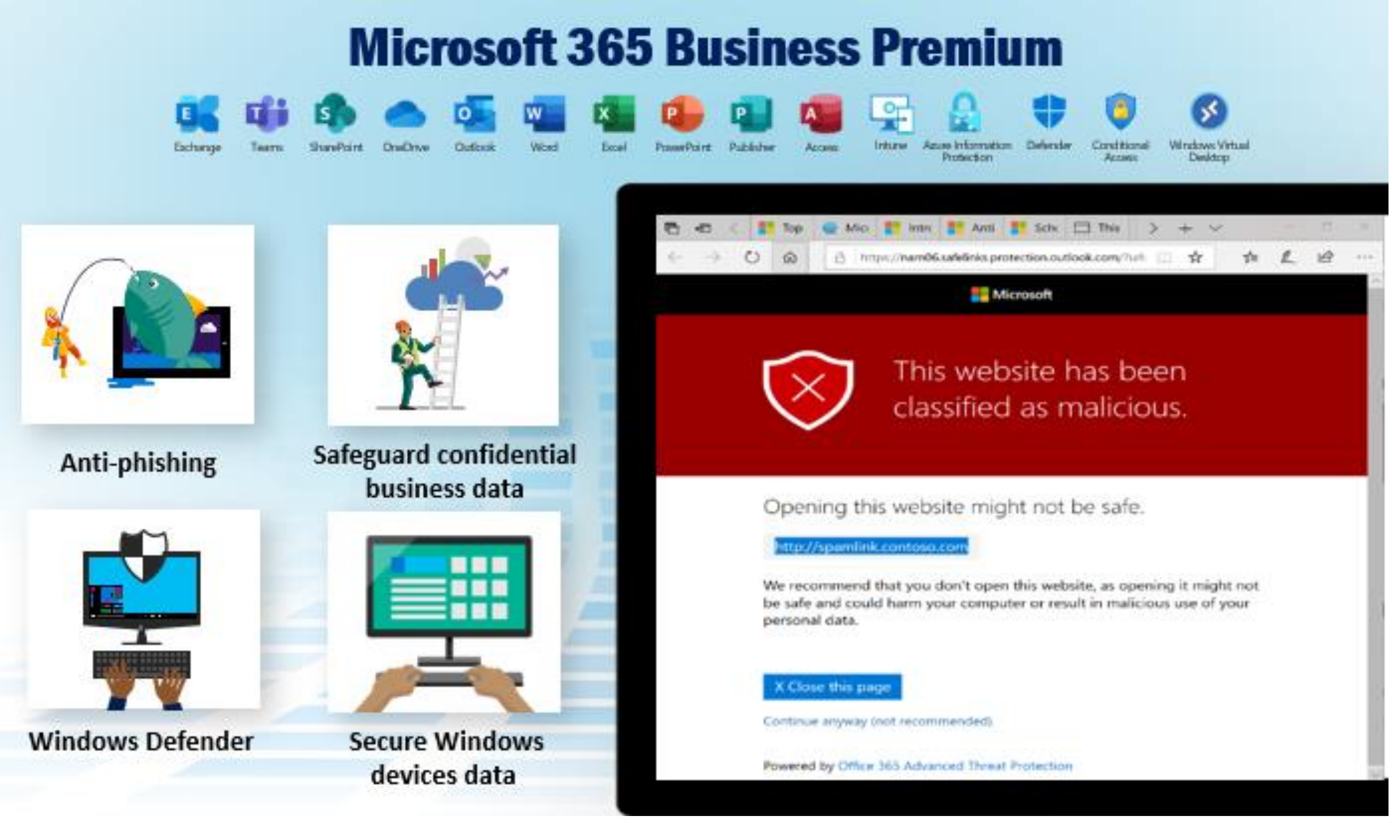
WISE-DeviceOn makes onboarding, visualizing, operating, and managing industrial IoT devices easier than ever. This simple, out-of-the-box solution leverages a single console adaptable to different device types. It helps monitor device health, allows remote power on/off, troubleshoots problems, and sends software and firmware updates over-the-air (OTA). Enterprises that use Azure can perform daily IoT device management, and flexibly scale out platform capabilities to accommodate and manage hundreds of thousands of devices and enhance overall IoT device security.

Block Phishing Mail and Safeguard of Business-critical Data

Microsoft 365 Business Premium

Some attacks come from the wild frontiers of IT and use phishing emails to penetrate corporate systems. M365 BP is designed for SMB and is capable of identifying strange patterns and abnormal behaviors using anti-phishing intelligence and AI inference. Following detection, M365 BP immediately runs suspicious attachments/links through the Windows virtual sandbox.

Emails will not be sent to the employee until the potential threats are deemed safe. Likewise, users can leverage the built-in Windows Defender to scan any suspicious files, viruses, and databases. This helps prevent interaction with ransomware and malware, protects files in key system folders, and avoids the loss of confidential data.


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
Top
Mic
Intn
Anti
Schi
This
https://nam06.safelinks.protection.outlook.com/?url
Microsoft
X Close this page
Continue anyway (not recommended)

This website has been classified as malicious.

Opening this website might not be safe.

http://spamlink.contoso.com

We recommend that you don't open this website, as opening it might not be safe and could harm your computer or result in malicious use of your personal data.

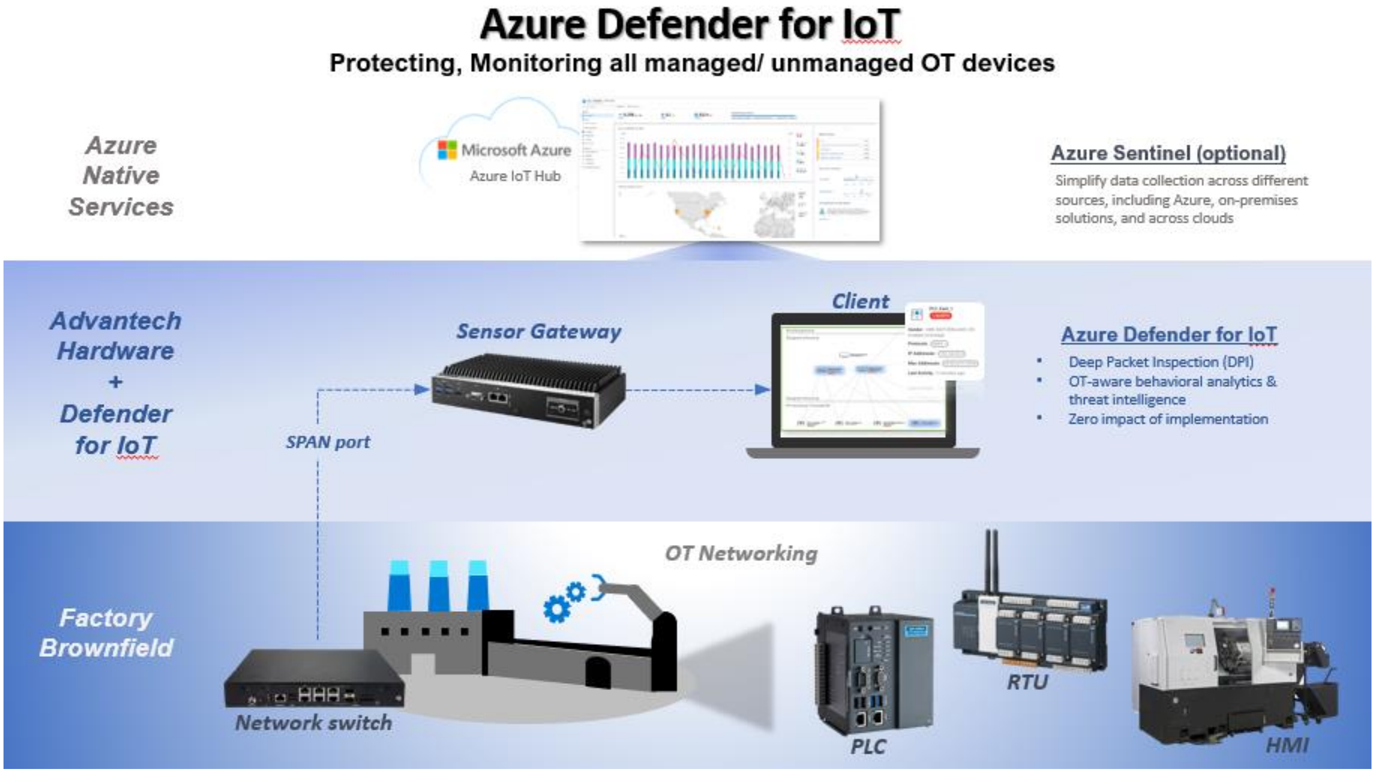
Powered by Office 365 Advanced Threat Protection

Threat Detection and OT Behavior Analysis

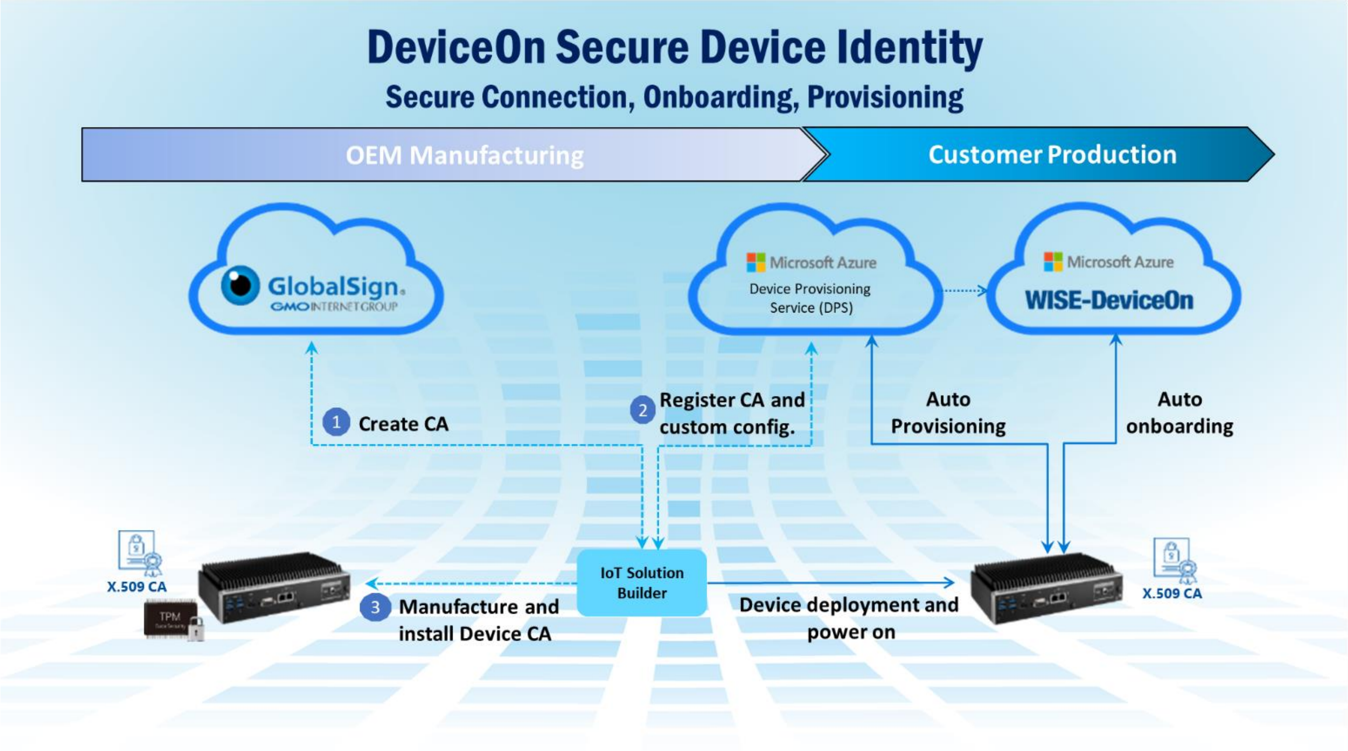
Azure Defender for IoT

The current generation of OT is no longer a closed network. Indeed, IT-OT convergence is becoming mainstream. Azure Defender for IoT is a specialized asset-discovery and security-monitoring solution for IoT/OT environments that protects network infrastructures from cyber-attacks.

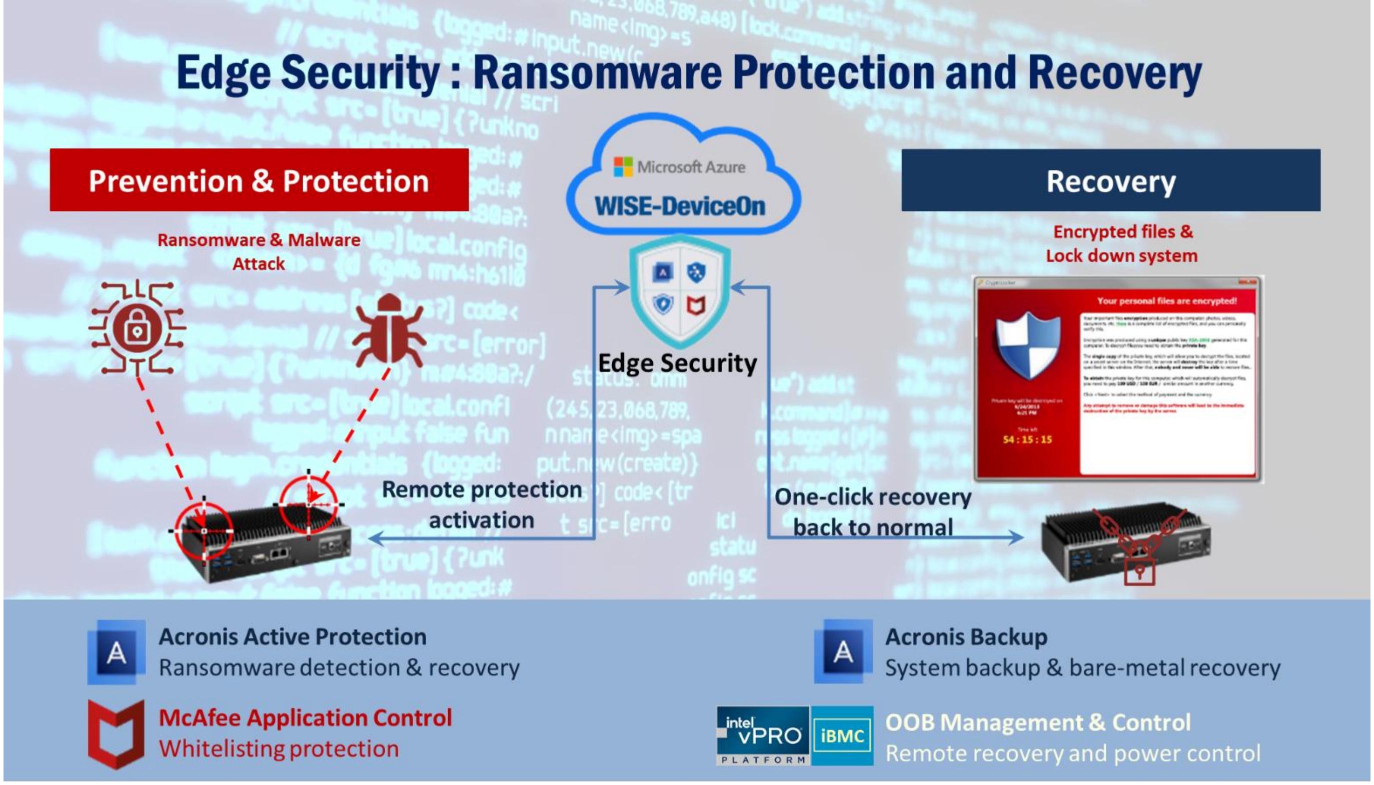
In sum, it provides agentless security without impacts on performance or operational downtime during deployment. This is because it only analyzes network traffic obtained from SPAN/mirror ports of the network switch. This enables Deep packet inspection (DPI) and monitoring of all OT devices throughout the entire network and managed and unmanaged devices are discoverable to enhance factory visibility. Through the use of specialized OT-aware behavior analysis with machine learning and OT-specific threat intelligence, any suspicious traffic or ransomware risks traversing the entire network are identified, and a full assessment report is delivered in seconds. Get a bird's-eye view across IT/OT boundaries featuring interoperability with Azure Sentinel or 3rd SIEM/SOAR to enhance enterprise security with less effort.


Azure Defender for IoT
Protecting, Monitoring all managed/ unmanaged OT devices
Azure Native Services
Microsoft Azure
Azure IoT Hub
Azure Sentinel (optional)
Simplify data collection across different sources, including Azure, on-premises solutions, and across clouds
Advantech Hardware + Defender for IoT
Sensor Gateway
Client
SPAN port
Azure Defender for IoT
Deep Packet Inspection (DPI)
OT-aware behavioral analytics & threat intelligence
Zero impact of implementation
Factory Brownfield
OT Networking
Network switch
PLC
RTU
HMI

Prevent Attacks and Restore Operations


DeviceOn Secure Device Identity
Secure Connection, Onboarding, Provisioning
OEM Manufacturing
Customer Production
GlobalSign.
GMO INTERNET GROUP
Microsoft Azure
Device Provisioning Service (DPS)
Microsoft Azure
WISE-DeviceOn
1 Create CA
2 Register CA and custom config.
Auto Provisioning
Auto onboarding
X.509 CA
TPM
IoT Solution Builder
3 Manufacture and install Device CA
Device deployment and power on
X.509 CA

Advantech DeviceOn provides secure device identity as the basis for comprehensive security alongside fundamental device monitoring and management features. DeviceOn uses the hardware TPM to store unique X509 certificates as device identity in order to establish a secure connection for interaction with other devices, services, or users. This prevents unauthenticated devices from joining the secure network. Likewise, malicious actors cannot use illegal devices or connections to join the network and undermine security. Auto provisioning and onboarding for large numbers of IoT devices can be achieved alongside security features using device identity credentials stored in hardware. This is accomplished using Azure Device Provisioning Service (DPS), which adds DeviceOn server IP, creates a device certificate to handle security, and other customer configurations.


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
Your personal files are encrypted!
54 : 15 : 15
One-click recovery back to normal
Acronis Active Protection
Ransomware detection & recovery
McAfee Application Control
Whitelisting protection
Acronis Backup
System backup & bare-metal recovery
intel vPRO PLATFORM
iBMC
OOB Management & Control
Remote recovery and power control

DeviceOn integrates 3rd party security solutions including Acronis Active Protection, Acronis Backup & Recovery, McAfee Application, and Advantech iBMC OOB management. It provides complete edge security against ransomware attacks. This edge integrated security solution enables the system to leverage a whitelist that protects against unauthorized processes that infiltrate the system. It also detects and isolates ransomware immediately, and recovers encrypted files instantly. Damaged and locked-down systems can be recovered out-of-band and remotely returned to normal without getting touch to field-side devices in worst-case scenarios. The following sections elaborate on these individual functions:

Acronis Active Protection

Acronis Active Protection is an advanced ransomware protection technology. Completely compatible with the most common anti-malware solutions. Acronis technology actively protects system data — including documents, media files, and programs. Acronis Active Protection does not need to wait for virus signature updates to detect new and unknown ransomware programs; and defends against zero-day attacks. If ransomware begins to encrypt files, Acronis quickly detects and halts this process. Because Acronis is a backup solution, any data exposed and encrypted before the process is halted can be recovered from a variety of backup sources. Alternative anti-ransomware solutions are usually incapable of ending an attack once it has started. Likewise, they have no way of recovering files encrypted by the attack. Conversely, Acronis Active Protection detects and deflects attacks while restoring files of any size!

Acronis Backup & Recovery

Combining with anti-ransomware technologies (Active Protection), Acronis Cyber Backup delivers the cyber protection that today’s organizations need to avoid costly downtime, unhappy customers, and lost revenue. Acronis Cyber Backup minimizes potential data loss by backing up often without affecting system performance or productivity. It can quickly execute bare-metal recovery to reduce the impact of damaged or encrypted systems which have been locked by ransomware attacks and cannot be powered on.

McAfee Application Control

With intelligent whitelisting protection, McAfee Application Control prevents zero-day and APT attacks by blocking the execution of unauthorized applications and processes that are used to move laterally and infiltrate whole network system in the phase II of a ransomware attack.

OOB Management & Control

Integrate with Intel vPro® AMT and Advantech’s iBMC chip to provide continuous out-of-band connection capabilities that operate independently of the operating system, and can correct a wider range of system problems even when the operating system has shut down. Users can repair damaged drivers, application software, or operating systems that cannot run or boot on an unresponsive system, or use KVM to monitor operating system updates, or boot to the system BIOS. This means under ransomware attack, most affected devices cannot be powered on, but with OOB, users still can leverage this technique and network connection to execute remote power-on and one-click recovery for parts of the system.

Conclusion

Cyber-attack approaches and tactics are constantly evolving. As such, there is no single technology that can completely prevent hackers from invading corporate networks. However, if an organization adopts the right people, procedures, and technologies to monitor and protect their own environment, even if they are attacked, they can still prevent disaster. According to ESG (Enterprise Strategy Group), 80% of organizations believe that their incident detection/response procedures are lacking. This is why Advantech partnered with Microsoft to develop an IT/OT total security solution in response. Multiple security solutions are included in one package to simplify management, strengthen the protection of physical vulnerabilities, protect asset-centric OT systems, and leverage the Azure Cloud to drive IoT innovation. With this solution, enterprises can assemble a complete IoT secure device management platform quickly to stay competitive with less effort.