Protecting Assets

Data & Control

Rest
Physical access to a device will not give access to data

Motion
Transport of data between endpoints/devices is secure

Execution
Data owner has full control over data processing
IoT protection stack

**Device protection**
- Trusted Platform Module (TPM)
- Windows Device Health Attestation
- Secure Boot
- BitLocker

**Threat resistance**
- Windows as a Service
- Device Guard
- Windows Firewall
- Windows Defender*

**Data protection in-motion**
- X.509/TLS-Based Handshake and Encryption

**Cloud security**
- Encryption at Rest
- Azure Active Directory
- Key Vault
- Policy-Based Access Control
- IP-based blocking
- Secure Device Registration
- Standards-based best practices

**Response**
- Device Management
- Device Recovery
- Device-specific repudiation

*Only available on Windows IoT Enterprise
Secure connected Devices

Software cannot protect itself
- Memory can be manipulated
- No trust anchor to rely on

Secure Hardware can protect Software
- Providing hardware root of trust
- Utilizing hardware security features (trusted execution, crypto acceleration, read protected storage)

Devices cannot proof trustworthiness on their own
- Security services are needed to proof health of device – software, hardware and configuration,
7 properties of security for Windows 10 IoT devices

**Hardware Root of Trust**
- Supports strong device identities

**Defense in Depth**
- Various levels of defense in depth including Device Guard, UWP Appx containerization, etc.

**Small Trusted Computing Base**
- Utilize TrustZone for critical processing such as fTPM

**Dynamic Compartments**
- UWP apps run in their own contexts; Windows is built in a compartmentalized way

**Certificate-Based Authentication**
- Certificate (key) protected code execution thru DeviceGuard

**Failure Reporting**
- Different level of failure reporting for HW, OS and apps are available via Watson through OEM portals

**Renewable Security**
- Proven and scalable update infrastructure through Windows updated and Device Update Center.

The example is based on an i.MX6 processor running Windows IoT
Establishing Trust

- **Device**
  - Attestation: Can I trust the device with my assets?
    - Proof of device health
  - Provisioning: Who has access to my assets?
    - Device identity and health

- **Trusted Device**
  - ✓ I can **trust** the device with my assets
  - ✓ I am in **control** of the device

- **Security Claim**
  - Attestation Service
  - Provisioning Service

- **Policy**
Servicing Secure Devices

- Protect data where it is at rest, in motion and during execution by utilizing TEE, secure boot and others
- Establish trust through attestation and provisioning

- Device Health Attestation assess trusted and compliant state
- Azure Security Center
  - cloud-powered, behavioral-based, breach detection
  - Threat intelligence knowledge base
  - Forensic investigation and mitigation capabilities

- Security bulletins and fixes
- Device Update Center scalable, device staging
- Device Management, scalable from low end devices to enterprise, cloud and on-prem

Actionable Information
Building a secure device

- Security is built into the Windows IoT platform and enabled by default for production
- Tools and comprehensive guidance for device image composition and factory line processing

All the information are at Build Secure Devices with Windows on WindowsOnDevices.com -> Docs -> Security
Security offerings

- Proven security technology across a wide range platforms from Server, Desktop, Gaming to IoT
- IoT security benefits from analytics and mitigations of threats across millions of devices

**Device Platform**

Security is built in to Windows

- Secure applications through UWP
- Health attention and provisioning
- Data protection at rest volume encryption and HW supported key storage (BitLocker, TPM)
- Secure execution: DeviceGuard, Secure Boot
- Threat mitigation Device update and management
- Turn-key security and manufacturing tools

**Service offerings**

Windows 10 IoT Core Services

- 10y LTSC support
- Device Health Attention
- Manage updates via DUC (Device Updated center)

Azure Security Center

Windows 10 Enterprise license

- 10y LTSC
- Servicing via Windows Update
- Advanced Thread Protection (ATP)
Windows IoT security promise

Windows IoT provides the best endpoint security to **protect your data at rest, in motion and during execution**.

Windows IoT devices are **built with security in mind**. **Security is not in the way** of your development, deployment and operation.
IoT Security Offering

Protect

Core HW & Platform
- Malware resistance w/ **SecureBoot**
- Securing keys in the **TPM**
- Information protection for data at rest with **BitLocker**
- Execution control via **DeviceGuard for IoT**
- Security updates

Device Attestation
- Security related data points validated by **Remote Health Attestation Service**
- **Measured boot data**, protected by the TPM, sent to service for verification
- **Conditional Access** to sensitive assets based on device health assessment

Windows Defender ATP*
- **Advanced Threat Protection** with cloud-powered, behavioral-based, post-breach detection
- **Anomaly detection**, combined with Microsoft threat intelligence knowledge base
- **Forensic investigation and mitigation** capabilities

Remediate

Recovery and DM
- Remediate the affected device via DM (e.g. flash the device)
- Device Update

* Roadmap
Protection
Protecting Data at Rest

BitLocker
- Proven volume encryption with TPM protected keys
- Used across the Windows ecosystem, desktop, mobile, IoT, ...
- Enterprise manageable

TPM
- Key protection, e.g. BitLocker, Azure IoT Hub access token, ...
- Cross platform supported
- TPM implementations
  - Discrete TPM that can be attached to device
  - Firmware TPM implemented in a Trusted Execution Environment in SoC, e.g. fTPM in ARM TrustZone
  - Emulated Software TPM to be used for SW development and testing only
Protecting data at execution

**Secure Boot** assures that only signed, trusted firmware components are loaded.
Firmware execution policy is anchored in the Hardware Root of Trust (HW RoT)

**Device Guard** enforces execution policy on platform, driver and applications.
Device Guard policy is secured through Firmware.
Detection
Device Health Attestation

Does my device have the right configuration to be trusted?

Remote attestation based on **hardware measured & attested data**

The Device Health Attestation enables IT administrators to

• monitor the security posture of managed devices remotely
• by using hardware (TPM) protected and attested data
• via a tamper-resistant and tamper-evident communication channel

Creating attestable trust
Can I trust that the device provides the right information HW and SW?

- **Root of trust** is established by SoC manufacturer or OEM
- Each component will issue a **certificate** for the component it loads including measurements
- **ECC keys** are generated using the previous component key as seed

**Component Certificate** contains:
- Measurement of the binary
- Public key for this component
- Chain up to previous cert
Advanced Threat Protection for IoT devices

Early threat detection is critical for to mitigate impact on device operation

WDATP is available for Windows 10 Enterprise and Server

- Advanced Threat Protection with cloud-powered, behavioral-based, post-breach detection
- Anomaly detection, combined with Microsoft threat intelligence knowledge base
- Forensic investigation and automated mitigation capabilities

PC have broader attack surface due to open platform and user initiated entry points, email, social media ... These only apply limited to IoT solutions.

Windows IoT

- Device lockdown, purpose build devices with limited well defined user interaction.
- Attack surface: Zero-day-exploits, communication protocol attacks, wrong configurations
Remediation
Windows Update

Connected devices have challenge of new security threads - updates are an essential tool to address this

- Keeps device up to date with critical security software updates
- Utilize the Microsoft proven and scalable infrastructure
- Updates can be easily managed and controlled by device owners
- Easy management via Device Update Center
Introducing Windows 10 IoT Core Services

Commercialize your project with enterprise-grade security and support

Updates

• Take control of Windows updates with cloud-based IoT Core Device Update Center (DUC)
• Manage updates for OS, apps, settings, and OEM-specific files from the cloud
• Distributed over the same global CDN used by Windows Update

Security

• Help ensure the safety of your network and devices with cloud-based Device Health Attestation (DHA)
• Backed by the same security research team and validation process used by 700M Windows 10 devices
• Leverage hardware and cloud services to provide tamper proofing and remote attestation of device health

Support

• Count on stable systems with 10 years of LTSC (Long Term Servicing Channel) support with security updates only (no new features)
• Official Microsoft Lifecycle Support statement - links to software license agreement
• Access to monthly published Windows IoT Core packages for building fully patched images with OEM tools
Privacy: GDPR
Our commitment

- Windows 10 IoT platforms is GDPR complied
- Together with our partners, we are prepared to help you meet your policy, people, process, and technology goals to align with GDPR
- View Microsoft GDPR compliance at www.Microsoft.com/GDPR
Security on Azure IoT Edge
Azure IoT Edge *Device* Security Promises

What is the maximum protection you can expect if the device fell into the wrong custody?

HSM PAL = Hardware Secure Module Platform Abstraction Layer
Azure IoT Edge security with enclaves – Public preview

Enabling Open Enclave SDK for the intelligent edge and simplifying the development of trusted applications across operating systems and hardware platforms.
Extensible Enclave Model

- Foundation TA
  - PKI based ID & Auth
  - Certs store
  - Crypto Libraries
- TA Extensions
  - Metering
  - Trusted I/O
  - Secure Logging
  - Edge Module custom sensitive logic
  - Etc.
Windows IoT Editions
## Windows 10 IoT editions

Microsoft is releasing a new Windows 10 IoT Core Services offering with 10 years of support (LTSC)

New value provided through Windows 10 IoT Core Services

New sales opportunity and broader services attach motion

<table>
<thead>
<tr>
<th>What’s new?</th>
<th>Windows 10 IoT Core</th>
<th>Windows 10 IoT Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Brand new offering</strong> with Windows 10 IoT Core Services</td>
<td><strong>RS5 LTSC cumulative release since RS1</strong></td>
</tr>
<tr>
<td>What’s my purchase model?</td>
<td><strong>Subscription fee</strong></td>
<td><strong>Stable LTSC with RS2-&gt;RS5 features</strong></td>
</tr>
<tr>
<td>Availability &amp; support?</td>
<td><strong>10 years</strong> of distribution and support fixes</td>
<td><strong>10 years</strong> of distribution and support fixes</td>
</tr>
</tbody>
</table>
Thank You