Microsoft

Create more secure IoT solutions with Windows IoT

Contents

This document is provided “as is.” Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Introduction: The IoT security challenge

If you work in the IT industry, you're already aware of the importance of security. Put simply, if security can't be all but guaranteed in today's IT world, then the risk is often unacceptable. In addition to the damage that security breaches can do to an organization's sales and reputation, the strict data protection requirements and high penalties imposed by new regulations such as the European Union's General Data Protection Regulation (GDPR) are just too high to take any chances.

Perhaps nowhere is this dynamic more prevalent than in the rapidly growing world of the Internet of Things (IoT). If you're involved in building or selling such IoT solutions, especially to external customers, you're probably aware of the extent to which IoT security is a barrier to sales. In fact, according to Bain & Company, "Cybersecurity is key to unlocking demand in the Internet of Things." In fact, that's the title of a recent Bain report[1], which states that executives at the enterprises they surveyed:

- Are limiting investment in IoT devices because of concerns about security risks.
- Would be willing to buy on average, at least 70 percent more IoT devices if their concerns were resolved.
- Would be willing to pay an average of 22 percent more for devices with better security.

In its report, Bain concluded that "security remains the leading barrier to IoT adoption." But if you're building IoT solutions, what can you do? How can you deliver highly secure IoT solutions, and just as important, how do you convince customers that you've covered all the bases? To do this, start by identifying some of the unique security risks inherent in IoT solutions:

- IoT devices interact with the physical world, so misuse can have disastrous consequences. A compromised IoT device can negatively affect day-to-day operations, and in extreme cases, might even put lives at risk.
- Factories, infrastructure, and other installations have been automated and locally connected for a long time. Some are now being connected to the internet and exposed to remote attacks for the first time.
- Even IoT devices that aren't connected to the internet are at risk from other devices that have been online; for example, a service technician might plug a laptop or USB drive into a previously disconnected IoT device. Stuxnet is a prime example of such an attack.

To secure an IoT solution, you must secure the IoT devices themselves, the data they contain, the apps they run, device connectivity to the cloud, the services running in the cloud, and the apps that are built on top of those cloud services. What's more, you must address all phases of the IoT device lifecycle—from initial deployment through decommissioning and retirement. Finally, because of the very nature of IoT, you most likely will need to do all this at massive scale.

This paper will address how Microsoft is approaching IoT security and how we're enabling you to deliver highly secure IoT solutions with Windows IoT.

[1] Cybersecurity Is the Key to Unlocking Demand in the Internet of Things, Bain & Company, June 13 2018.

Windows IoT: Intelligent security for your IoT solutions

Windows IoT refers to the group of operating systems that includes Windows 10 IoT Core, Windows 10 IoT Enterprise, and Windows Server IoT 2019. Windows IoT provides built-in, security for IoT devices, including comprehensive tools for protecting data on a device, assessing device health, detecting security issues, and remediating threats through device updates and management. These integrated capabilities span from the device to the cloud, enabling you to deploy IoT solutions at massive scale anywhere in the world, in a highly secure and cost-effective manner.

Before delving into how Windows IoT makes this possible, it's worth taking a moment to describe each Windows IoT offering:

- **Windows 10 IoT Core** is a Windows 10 operating system edition that's optimized for single-purpose IoT devices. It builds on decades of Microsoft experience with embedded devices to deliver the same security, supportability, and manageability as the rest of the Windows 10 family, but with a much smaller footprint (less than 2 gigabytes). Microsoft works with leading system-on-a-chip (SOC) vendors to verify support for Windows 10 IoT Core on their SOCs, which hundreds of different device original equipment manufacturers (OEMs) and original design manufacturers (ODMs) use.

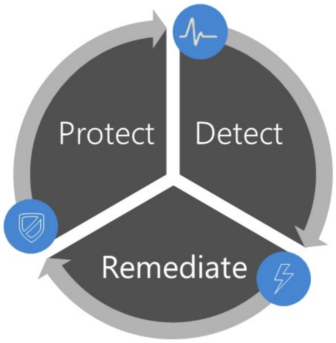
  Note: Microsoft recently launched Windows 10 IoT Core Services, a cloud subscription that provides the essential services to commercialize devices on Windows 10 IoT Core.)

- **Windows 10 IoT Enterprise**, a binary equivalent of Windows 10 Enterprise, is for fixed-purpose IoT devices. It uses the same development and management tools as client PCs and laptops. Devices can be locked to a specific set of apps and peripherals, system messages can be suppressed, and the boot sequence can be customized. You can even have a read-only system that returns to its original state after each power cycle.
- **Windows Server IoT 2019**, a binary equivalent of Windows Server 2019, lets customers create IoT solutions to handle large workloads that require more computing power, storage, and connectivity, such as applying image recognition to multiple video streams. These solutions can aggregate data from many IoT devices and store that data in huge local databases.

The remainder of this paper will examine features and tools that you can use to help ensure security across three key pillars of the IoT security spectrum:

- **Protect data**. Securing data means protecting it at all times, including at rest, during code execution, and in motion. This is done by using BitLocker Drive Encryption, Secure Boot, Windows Defender Application Control, Windows Defender Exploit Guard, secure Universal Windows Platform (UWP) applications, Unified Write Filter, a secure communication stack, and security credential management.

- **Monitor and detect**. Device Health Attestation (DHA) lets you start with a trusted device and maintain trust over time. As the device runs, Microsoft Azure Security Center for IoT can help detect and protect against threats.
- **Update and manage**. You can use Device Update Center and Windows Server Update Services (WSUS) to apply the latest security patches. If you determine that a device might be exposed to a threat, you can remediate that threat by using Azure IoT Hub device management features, Microsoft Intune or third-party mobile device management (MDM) solutions, and Microsoft System Center Configuration Manager (Configuration Manager).



Protect

The previous section touched on Secure Boot and BitLocker as two examples of security mechanisms to which DHA can attest. Next, let's take a closer look at what Secure Boot, BitLocker, and other data protection features in Windows IoT actually do, along with how you can use them to help protect your data at rest, in motion, and during code execution. Again, it's worth pointing out that many of these features require a Trusted Platform Module (TPM). Fortunately, most devices today have a TPM that is implemented either in hardware or firmware.

The following table describes which features or tools apply to each edition of Windows IoT.

Technology	Windows 10 IoT Core	Windows 10 IoT Enterprise	Windows Server IoT 2019
BitLocker	✓	✓	✓
Secure Boot	✓	✓	✓
Windows Defender Application Control	✓	✓	✓
Windows Defender Exploit Guard	N/A	✓	✓
Secure UWP applications	✓	✓	N/A
Unified Write Filter	✓	✓	N/A
Secure communication stack	✓	✓	✓
Management of security credentials	✓	✓	✓

BitLocker Drive Encryption: Protect data at rest

Protecting data at rest means ensuring that physical access to a device won't allow an unauthorized entity access to its data. BitLocker is a full-volume data protection feature that integrates with Windows and helps protect against data theft or exposure because of lost, stolen, or improperly decommissioned devices. It achieves this by encrypting all user files and system files on the operating system drive, including the swap files and hibernation files, and by checking the integrity of early boot components and boot configuration data.

BitLocker provides the most protection when used with a TPM version 1.2 or later. On devices that don't meet this criterion, you can still use BitLocker to encrypt the Windows operating system drive. However, this requires a USB startup key to start the device or to resume from hibernation. You can also use an operating system volume password to protect that volume on a device without a TPM. However, neither option provides the pre-startup system integrity validation of using BitLocker with a TPM. BitLocker support for TPM 2.0 requires Unified Extensible Firmware Interface (UEFI) for the device.

Protect data during code execution

You must also protect data during code execution, which requires ensuring that only the authorized data owner has control over all data processing. Malware is a rapidly growing threat to IoT devices, and its consequences can be especially acute with devices that directly affect our physical environment or the operation of critical infrastructure.

Secure Boot

Secure Boot helps ensure that only trusted operating system boot loaders are started, reducing the risk of a successful firmware rootkit. When a device starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as option ROMs), EFI applications, and the operating system. If the signatures are valid, the device starts, and the firmware gives control to the operating system. Devices without Secure Boot simply run whatever boot loader is present—there's no way for the device to tell whether it's a trusted operating system or a rootkit.

Windows Defender Application Control

Traditional antivirus solutions that employ signature-based detection to fight malware might not catch all threats, especially new ones. Windows Defender Application Control addresses this by moving from a model where all applications are assumed trustworthy unless proven otherwise to one where applications must earn trust in order to run. It does this by restricting the applications that users are allowed to run and by restricting the code that runs in the system core (kernel). MDM solutions such as Intune can distribute and manage Windows Defender Application Control policies.

Note: Prior to Windows 10 version 1709, Windows Defender Application Control was known as Windows Defender Device Guard configurable code integrity.

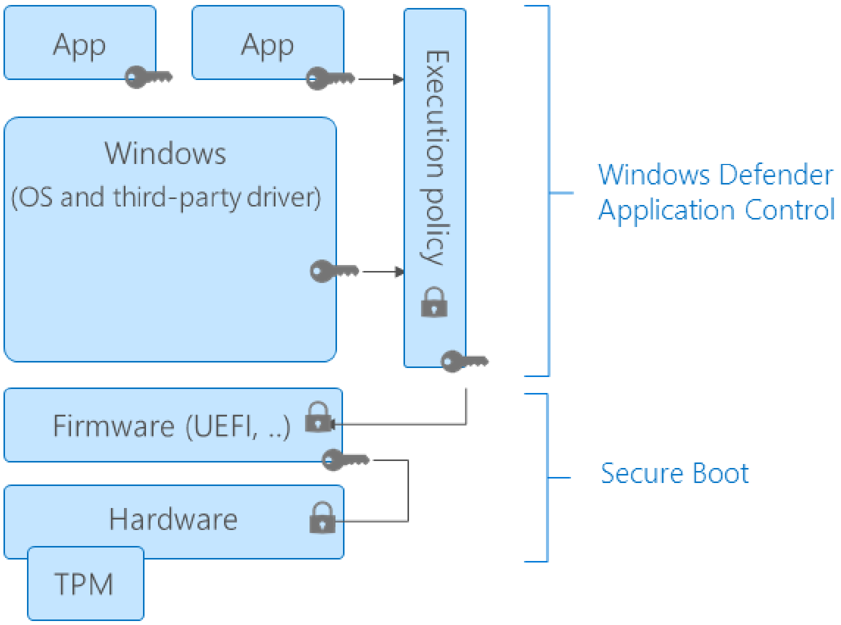


Figure 2. Secure Boot and Windows Defender Application Control both help protect data during code execution.

Windows Defender Exploit Guard

Windows Defender Exploit Guard provides a set of host-intrusion prevention capabilities. These allow you to manage and reduce the attack surface of apps, to lock down devices against a wide variety of attack vectors, and to block behaviors commonly associated with malware attacks.

Note: Prior to Windows 10 version 1709, Windows Defender Exploit Guard was known as Windows Defender Device Guard hypervisor code integrity.

Secure Universal Windows Platform applications

If an attacker does find a vulnerability in an application, you'll want to make sure the damage is as limited as possible. Windows IoT supports the same secure UWP application development model as the rest of the Windows 10 operating systems. Under UWP, applications run in sandboxed fashion so that a compromised application can't interfere with other applications or access their data unless explicitly authorized to do so.

Note: You can use Desktop Bridge to migrate Win32 apps to UWP.

Unified Write Filter

Unified Write Filter helps protect drives in IoT devices by intercepting any writes to the drive, such as app installations, settings changes, and saved data. Instead of saving those writes to disk, Unified Write Filter redirects them to a virtual overlay, which is a temporary location that can be cleared during a restart. You can use Unified Write Filter to build a read-only device that returns to a known state after a power cycle by keeping disk changes in memory instead of writing them to disk.

You can combine Unified Write Filter with the Hibernate Once/Resume Many feature to resume a predefined session. Additionally, you can update and service UWF-protected devices by using Unified Write Filter servicing mode or by adding file and registry exclusions to specific system areas.

Protect data in motion

To keep data secure, you must also ensure that communication channels between IoT devices and other endpoints, such as a local controller or a cloud service, are protected. Windows IoT provides such capabilities through its communication stack, along with proven functionality for managing credentials that are used for secure communication.

Secure communication stack

While data is in motion between secured endpoints, it can pass through less secure channels that might put it at risk. This risk isn't new, which is one reason Microsoft is an active member of many organizations that influence the development of secure communication protocols.

Windows IoT uses the same well-maintained communication stack and cryptographic protocols as other editions of Windows operating systems. For example, secure channel (also known as *Schannel*), a Windows security support provider, implements versions of the Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Secure Sockets Layer (SSL) security protocols. Server Message Block (SMB) 3.0, a network file sharing protocol, also supports high levels of end-to-end encryption. Virtual private networks (VPNs) that use Internet Protocol security (IPsec), support for which is also built into Windows IoT, are yet another method for securing traffic between IoT devices and other endpoints.

Security credential management

Windows IoT provides a proven infrastructure for provisioning and managing credentials for secure communication, including integrated functionality for connecting to Azure IoT Hub by using X.509 certificates.

Detect

When your devices start, and as they run, you'll want to monitor them continually to detect potential threats. DHA and Azure Security Center for IoT provide such capabilities.

The following table describes which features or tools apply to each edition of Windows IoT.

Technology	**Windows 10 IoT Core**	**Windows 10 IoT Enterprise**	**Windows Server IoT 2019**
DHA*	✓	N/A	N/A
Azure Security Center for IoT*	✓	N/A	N/A

** Denotes that an additional license or subscription service is required.*

Device Health Attestation

To maximize security, you must have a trusted device. However, software alone can't protect itself—memory can be manipulated, leaving the software without a trust anchor on which to rely. Device-based security features such as TPMs can meet this need by providing a hardware-based root of trust. TPMs typically include a random number generator, facilities for securely generating cryptographic keys, the ability to create a cryptographic hash of a device's hardware and software configuration, and other capabilities. Popular Windows security features such as BitLocker and Windows Hello for Business take advantage of TPMs.

Even with TPMs used to their fullest potential, however, devices still can't prove trustworthiness on their own. An independent instance is needed to compare TPM output—for example, the hash key summary of a device's hardware and software configuration—to a known good state. You can do so by using the DHA service. Only after such validation can a device be considered trustworthy and safely provisioned.

DHA supports devices that have TPMs implemented in hardware or firmware,[2] enabling you to assess device health and determine whether a device can be trusted—both on startup and periodically over time as a means of maintaining trust. The DHA service is typically called by an MDM system, which is used to specify the security policies to enforce by using DHA.

DHA does three things. First, it reviews the boot logs it receives from an enrolled device. Next, it creates a tamper-resistant (and tamper-evident) DHA report that describes how the device started based on data collected by the TPM. Finally, it delivers the DHA report to the MDM server that requested it via a protected communication channel. If the device doesn't meet policy requirements for device health, the MDM can then generate a report and/or take corrective action, such as reimaging the device, denying access, or creating a service ticket.

By using MDM, for example, you can create a policy that checks the boot configuration and attributes for Secure Boot and BitLocker. By using the DHA service, the MDM solution can enforce this policy to verify that Secure Boot was enabled, trusted and authentic code was loaded, and the Windows boot loader wasn't tampered with. The MDM system can also verify that BitLocker is enabled and that it was actively protecting data when the device was last turned off.

[2] Software TPMs are intended for development purposes only and don't provide any real security benefits. This article provides an overview of TPMs and how Windows operating systems use them.

Microsoft Azure Security Center for IoT

Microsoft recently introduced Azure Security Center for IoT, which unifies security management and enables end-to-end threat analysis and protection across hybrid cloud workloads. It does this by delivering unified visibility and control, adaptive threat prevention, and intelligent threat detection and response across IoT workloads that run on edge, on-premises, and on Azure and other clouds. Refer to our blog about the announcement for more information.

Remediate

To maximize security, you must keep IoT devices current with the latest security updates. You can accomplish this by using Device Update Center or WSUS. If a threat is detected, you must mitigate it, which you can do by using Azure IoT Hub device management, MDM systems like Intune, or Configuration Manager.

The following table describes which features or tools apply to each edition of Windows IoT.

Technology	Windows 10 IoT Core	Windows 10 IoT Enterprise	Windows Server IoT 2019
Device Update Center*	✓	N/A	N/A
WSUS	N/A	✓	✓
Azure IoT Hub*	✓	✓	N/A
Intune or third-party MDM solutions*	✓	✓	N/A
Configuration Manager*	N/A	✓	✓

** Denotes that an additional license or subscription service is required.*

Update

You can use tools such as Device Update Center and WSUS to manage security update deployments for IoT devices, enabling you to easily keep them current with the latest security patches. Microsoft recently announced 10-year servicing for Windows IoT, so you can have confidence that your IoT devices will have long-term support.

Device Update Center

Device Update Center enables you to create, customize, and control device security updates. You can choose to update all devices, or you can flight operating system updates or custom OEM packages to devices based on flight rings, as part of a more controlled distribution. Device Update Center uses the same content distribution network as Windows Update, which millions of Microsoft customers worldwide use to update Windows operating systems and other Microsoft applications. Device Update Center packages can include a combination of operating system updates, apps, drivers, and various other files.

Windows Server Update Services

WSUS supports both centralized update management and update management automation via a management console, helping make it easier for IT administrators to manage the distribution of Microsoft Update releases. WSUS is a built-in server role in Windows Server 2012 and later versions.

Manage

If a threat is detected, you must mitigate it immediately. Depending on the nature of the threat, this might require resetting or restarting a device, taking it offline, changing its security settings, or updating the device’s software. Windows IoT supports a range of Microsoft and third-party enterprise device management tools, enabling you to take such actions quickly, efficiently, and at scale.

Azure IoT Hub

Azure IoT Hub provides a robust set of device management capabilities that enable you to address a broad range of IoT devices efficiently and at scale. Capabilities include those for managing devices based on the concept of device twins (JSON documents that store device state information such as metadata, configurations, and conditions), in addition to direct methods for reading and modifying specific device settings.

Azure IoT Hub device management capabilities support all stages of the IoT device lifecycle:

- Planning—by enabling operators to create a device metadata scheme that enables them to easily and accurately query for and target a group of devices for bulk management operations.
- Provisioning—by enabling operators to securely provision new devices and immediately discover device capabilities.
- Configuration—by enabling operators to specify bulk configuration changes and firmware updates while maintaining device health and security.
- Monitoring—by enabling operators to collect overall device health, view the status of ongoing operations, and specify alerts for issues that might require their attention.
- Retirement—by enabling operators to replace or decommission devices after a failure, upgrade cycle, or at the end of the service lifetime.

Microsoft Intune or third-party MDM solutions

Intune and many third-party MDM systems support industry standards to facilitate the secure management of IoT devices. If you're already using such a system to manage laptops and phones, extending it to manage Windows IoT devices could be a cost-effective way to take advantage of existing investments, resources, and expertise.

Microsoft System Center Configuration Manager

Windows 10 IoT Enterprise and Windows Server IoT 2019 are binary equivalents of Windows 10 Enterprise and Windows Server 2019 respectively, meaning that you can manage them by using existing tools like Configuration Manager. In combination with Intune, you can extend Configuration Manager to manage PCs, Mac computers, UNIX and Linux servers, and cloud-based mobile devices that run Windows, iOS, and Android operating systems, all from a single management console.

Conclusion

Windows IoT offers the tools to deliver highly secure IoT solutions: data protection, device threat detection and monitoring, and updates and management of IoT devices over time—all at massive scale. Just as important, it offers all those capabilities through familiar Microsoft technologies and tools that won't require extensive additional investment, time, or expertise. By taking advantage of Windows IoT security features and capabilities, you can differentiate your IoT solutions and eliminate one of the largest barriers to their adoption.

For more information

Our online documentation provides more information on the security features of Windows 10 IoT Core, Windows 10 IoT Enterprise, and Windows Server IoT 2019.