Microsoft

Windows for IoT

The foundation for your intelligent edge

Contents

Introduction

Cloud computing is revolutionizing the embedded industry and making embedded computing more mainstream with the Internet of Things (IoT). Small and large companies across industries are looking at IoT technologies to digitize their businesses and save money and time while increasing scalability, access and agility.

But there are many challenges in building and commercializing solutions for this changing market. Often companies find there is a lack of available skilled workers, tools and resources to overcome technical challenges to using IoT. Devices used in IoT scenarios can be difficult and complex to implement, test and manage. Incompatible hardware components and connection technologies can make scaling at a commercial level difficult. Ensuring device security and the security of data at rest, in motion and in execution can prove hard to manage and implement. These challenges can delay time to market and make deployments difficult.

The Windows Embedded operating system has long been a trusted and secure solution for embedded systems. It can be found today in millions of devices including ATMs, kiosks, point of sale devices, digital signage, programmable logic controllers, HMI devices in manufacturing plants, medical imaging systems and systems used to manage buildings and cities. We estimate that more than 70 million Windows embedded/IoT desktop/server-based devices have been shipped over the past 10 years.

As new offerings such as Windows 10 IoT have become available, our customers and partners have become increasingly interested in its advanced security, platform and cloud connectivity features as well as their built-in intelligence for handling complex artificial intelligence (AI) and machine learning (ML) workloads.

Windows 10 IoT helps you more quickly build a productive IoT solution with secure, intelligent devices at the edge that can help you gain greater insight and take action quickly. Microsoft solutions, such as Azure Sphere for tiny-microcontroller enabled devices, Windows 10 IoT for smart devices, Windows Server IoT 2019 for high compute and performance needs and Azure Stack for enabling hybrid workloads, help you transform computing at the edge.

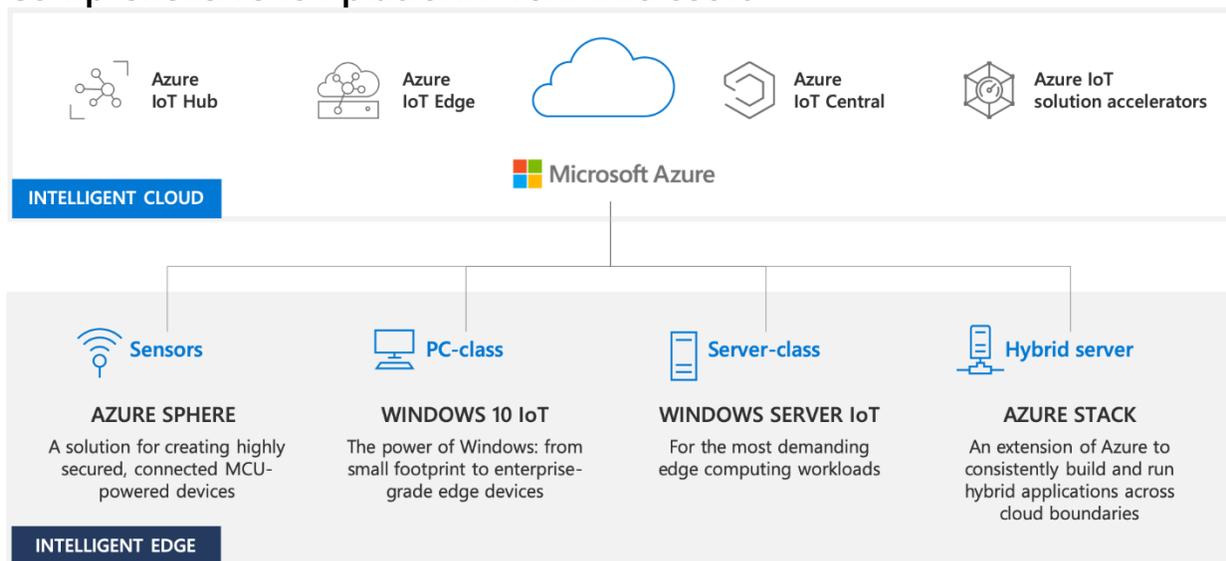## Top IoT Challenges

38%
Complexity/technical challenges

29%
Lack of budget/staff resources

29%
Lack of knowledge

23%
Haven't found the right IoT solutions

19%
Security

Comprehensive IoT platform from Microsoft

And with Windows 10 IoT and Azure IoT optimized to work better together, you can easily move workloads to the edge, granting your edge devices some of the cloud intelligence roles. This gives you greater ability to analyze data, gain insight and take action locally and autonomously.

At Microsoft, our mission is to empower every person and organization on the planet with the tools needed to achieve more through the intelligent edge and intelligent cloud. Our comprehensive IoT platform spans cloud, operating systems and devices. We offer decades of experience with embedded systems. Perhaps most important, we listen to you. We've incorporated customer feedback to help simplify the IoT journey so that any customer — regardless of size, technical expertise, budget, industry or other factors — can create trusted, connected solutions that improve business and customer experiences.

This document provides an overview of Windows for IoT, revealing how Windows for IoT can help you quickly and securely build and commercialize more productive IoT solutions and why you should consider making Windows the foundation for your intelligent edge.

Windows for IoT

Windows for IoT provides a scalable family of operating systems designed for use in embedded systems. Device builders, solution providers and enterprises of all sizes can use it to create secure devices that can be quickly and easily managed and seamlessly connected to the cloud. No matter what types of devices you have, The Windows for IoT family of products can meet your cost, feature and performance needs.

Windows for IoT includes the following products:

Windows 10 IoT Core is a Windows 10 operating system optimized for small, fixed-function devices that require a smaller operating system. Windows 10 IoT Core delivers the same security, supportability and manageability as the rest of the Windows 10 family, but with smart capabilities and a much smaller footprint (less than 2 gigabytes). Microsoft works with leading system-on-a-chip (SOC) vendors such as Intel, NXP and Qualcomm to verify support for Windows 10 IoT Core on their chips and systems. These Windows IoT Core-powered SoCs are used in hundreds of different devices that OEMs/ODMs can use to prototype and commercialize their ideas.

Windows 10 IoT Core Services is a cloud-based subscription that helps device builders move from designing prototypes to building Windows 10 IoT Core-based devices with updates and support. Device builders control updates through Device Update Center (DUC), which provides device stability and scalable updates and can span multiple devices and geographies. OEMs can publish customized updates over-the-air to the operating system, device drivers and their own apps.

Windows 10 IoT Enterprise is a binary equivalent of Windows 10 Enterprise but licensed for dedicated use devices. Windows 10 IoT Enterprise uses the same development and management tools as client PCs and laptops, delivering enterprise-grade manageability and security to IoT solutions. Devices can be locked to a specific set of apps and peripherals, system messages can be suppressed and boot sequences can be customized. You can even have a read-only system that returns to its original state after each power cycle. Windows 10 Enterprise also includes advanced features such as ML, container support, natural user interface and simple connectivity to Azure IoT.

Windows Server IoT 2019 is a binary equivalent to Windows Server 2019, licensed for dedicated use devices. It offers the latest Windows Server 2019 capabilities such as hybrid capabilities with Azure, enterprise manageability, faster innovation for apps (including support for modern container technologies managed by Azure IoT Edge) and advanced multilayer security. Windows Server IoT 2019 can support large-scale compute, large numbers of connections (devices or sensors) and storage workloads where processing on the edge may be required for latency, bandwidth, cost, data residency or privacy

requirements. And because it's a full version of Windows Server 2019, you can use the same familiar development and management tools that you use with your general-purpose servers.

Because Windows for IoT dynamically supports everything from very small devices to powerful servers with the most demanding edge computing workloads, you can easily find the right-sized appliance that meets your specific needs.

Windows 10 IoT Core	Windows 10 IoT Enterprise	Windows Server IoT 2019
400 MHz x86, x64 or ARM CPU 512MB 2 GB storage	1GHz x86 or x64 CPU 1 GB RAM (2 GB for 64-bit) 16 GB storage (20 GB for 64-bit)	1.4GHz x64 CPU 512 MB RAM (2 GB for desktop) 32GB storage

Small-footprint smart edge devices

- Optimized for devices with and without displays
- No OS-shell UX
- Universal Windows Platform (UWP) app experience
- No operating system royalty, (Windows 10 IoT Core Services is available for long-term security, servicing and management, enabling a sustainable business model)

EXAMPLE USE SCENARIOS

- Smart buildings
- Digital signage
- Smart thermostats and lights
- Wearables
- IoT Gateways

Powerful, smart devices

- A rich user experience with Win32 and UWP apps
- Same deployment, manageability and servicing as desktops
- Familiar interface with lockdown features to control user experience
- Functionally identical to Windows 10 Enterprise, but sold through the OEM channel with dedicated use licensing rights

EXAMPLE USE SCENARIOS

- ATMs
- Point of Sale (POS) devices
- Kiosks & Digital signs
- Programmable logic controller (PLC)
- Medical devices

For the most demanding edge computing workloads

- Aggregate data from a large number of 'things'
- Store and analyze very big databases to discover valuable business insights
- Use advanced resiliency and security capabilities
- Take advantage of Azure IoT hosting containers managed by Azure IoT Edge

EXAMPLE USE SCENARIOS

- Video surveillance systems
- Industrial automation
- Life and fire safety solutions
- Medical imaging technologies
- Telecommunication networks

Why Windows for IoT?

Windows for IoT enables ODMs and OEMs to quickly create and manage innovative, secure solutions that address the needs of their businesses and customers.

Microsoft has consolidated all the Windows operating systems into a single core — an operating system that can support devices large and small including clients, servers, HoloLens, wearables, sensors and all types of devices richer than a microcontroller. Enterprise-grade security, manageability and long-term support along with a rich feature set can handle the most advanced scenarios. You can also take advantage of the expertise of thousands of Windows IT admins and developers, existing management infrastructure and a worldwide hardware partner network. The end result is a familiar platform that lets you focus on value-added apps and innovations that you can quickly bring to market.

Learn and do more at the edge

Windows 10 IoT helps build a more productive IoT with secure, intelligent devices at the edge with ML and AI powered by Windows 10. Based on customer feedback, we have designed Windows for IoT to meet three key attributes:

Smart

Do more with smart devices at the edge. Windows for IoT provides a modern app platform, natural user interface capabilities, and powerful machine learning and AI capabilities that run across a broad range of device types.

Secure

With the latest security advances built in and always up to date, Windows for IoT helps protect your IoT solutions throughout development, deployment, and operation.

Fast

With a familiar app environment, tools, and framework, Windows for IoT enables you to create and deploy solutions faster.

Smart: A modern app platform

Windows for IoT provides natural user interface capabilities that support rich interactions, inherited from the vast user interaction models from the rest of the Windows 10 family. Powerful ML and AI capabilities run across a broad range of device types. With built-in Windows ML, you can run your intelligence where it makes the most sense — at the edge or in the cloud — giving you the flexibility you need in many of today's IoT deployments. Recent updates help you do even more at the edge, including event processing, image recognition, advance analytics and other high-value AI functions.

Windows ML enables developers to integrate trained ML models with their apps while taking advantage of GPUs to improve performance. For example, you can use Windows ML to detect manufacturing defects or provide facial recognition in a security and surveillance system. Local evaluation on devices running Windows 10 for IoT helps mitigate concerns of connectivity, bandwidth and data privacy.

Windows ML also lets developers write ML models in the industry-standard Open Neural Network Exchange (ONNX) format and accelerate inferencing using the CPU or DirectX 12-capable GPU from any vendor. This enables you to use lower-cost hardware platforms from a variety of vendors. Azure IoT Edge on helps bring cloud intelligence and analytics securely to Windows 10 IoT devices at scale.

Platform investments

Microsoft continues to innovate and update Windows for IoT. Some of the more recent updates include:

Azure IoT Edge for Windows seamlessly brings cloud workloads to the edge, harnessing the full power of the Windows for IoT platform. You can scale your IoT solutions across cloud or edge with a managed service that delivers cloud intelligence locally by deploying and running AI, Azure services and custom logic directly on cross-platform IoT devices. This lets developers more easily take apps and services developed for the cloud and deploy them on the edge when required by latency or bandwidth concerns, or data privacy or regulatory requirements.

Azure IoT Device Agent simplifies Azure connectivity, provisioning and device management, enabling you to quickly connect to remote configuration, monitoring and management of devices through the Azure dashboard.

Robot Operating System (ROS) for Windows for IoT deploys ROS projects that harness the full power of Windows for IoT and Azure. The Visual Studio Code extension for ROS offers automatic ROS environment configuration and Unified Robot Description Format (URDF) real-time rendering. The latter can graphically show properties of the robot including location, motion, configuration, status and more. These are in addition to well-known features like IntelliSense, on-device debugging and built-in Git commands. Using this familiar toolset, developers can build devices with advanced features like hardware-accelerated Windows ML, computer vision, Azure Cognitive Services and Azure IoT cloud services. These intelligent features help robots autonomously navigate, observe and interact with their environment and work with people in a safer and more natural way.

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 managing devices based on the concept of device twins (JSON documents that store device state information such as metadata, configurations and conditions), offering direct methods for reading and modifying specific device settings. Azure IoT Hub can support all stages of the IoT device lifecycle including:

Planning. Create a device metadata scheme to easily and accurately query for and target a group of devices for bulk management operations

Provisioning. Securely provision new devices and immediately discover device capabilities

Configuration. Specify bulk configuration changes and firmware updates while maintaining device health and security

Monitoring. Collect overall device health, view the status of ongoing operations and specify alerts for issues that might require attention

Retirement. Replace or decommission devices after a failure, upgrade cycle or at the end of the service lifetime

Secure: Built-in platform security designed to keep data and devices safe

To effectively secure an IoT solution requires securing the IoT devices, 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. You most likely will need to do all this at massive scale as well as address all phases of the IoT device lifecycle — from initial deployment through decommissioning and retirement.

Companies often individually approach security features such as strong user authentications, IoT device tracking and management capabilities and secure endpoints for each IoT device. Furthermore, device security is separate from data security, which is separate from identity security. In fact, many Linux solutions use different security components from different vendors, which can create complexity to implement, test and manage, and often requires support from multiple parties. It can also prove a time-consuming task.

Microsoft spends $1 billion annually on cybersecurity, continuously evolving Windows security architecture, so developers can focus on value-added features while helping ensure customer confidence in the devices they build with Windows.

With Windows for IoT, we've built our most secure, integrated operating system ever to help protect your IoT solutions throughout development, deployment and operation. Windows for IoT provides security features 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 cost-effectively deploy highly-secure IoT solutions at massive scale anywhere in the world. For example, Device Health Attestation (DHA)

enables enterprises to raise the security bar of their organization to hardware-monitored and attested security, with minimal or no impact on operation cost.

Windows 10 also includes comprehensive security lifecycle management http://aka.ms/windowssecurity. And with cloud integration, you can take advantage of Azure IoT manageability, security and scalability to streamline processes, reduce costs and create new business models.

Overall, Windows for IoT emphasizes on delivering three key values to the IoT security spectrum:
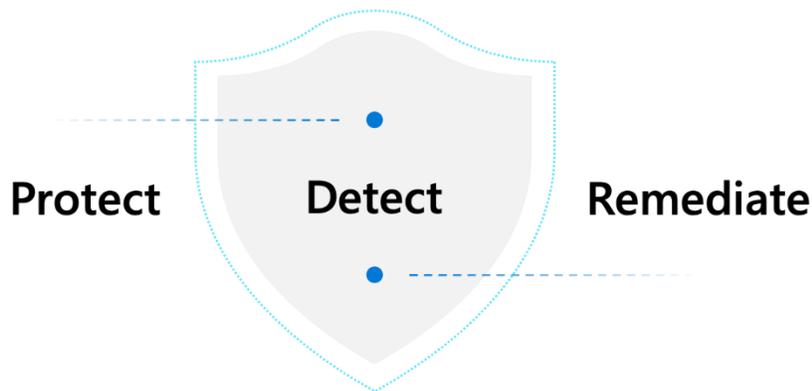
Protect data. Securing data means protecting it and all communications at all times, including at rest, during code execution and in motion. Windows for IoT does that by using BitLocker Drive Encryption (for full-device encryption), Secure Boot, Windows Defender Application Control, Windows Defender Exploit Guard, secure Universal Windows Platform (UWP) apps, Unified Write Filter, a secure communication stack and security credential management. Windows Server IoT 2019 also supports Shielded VMs, failover support with Cluster Sets and Cluster Hardening and protection from drive failures with Storage Spaces and Storage Replica. Access to data is also securely controlled by Azure Active Directory (AAD) and secure network technologies (see also the extensive and evolved lockdown features described in the next section).

Monitor and detect. DHA lets you start with a trusted device and maintain trust over time. As the device runs, Azure Security Center for IoT can help detect and protect against threats. Microsoft added cluster-wide monitoring capabilities to Windows Server IoT 2019, providing clear alerts when something isn't right.

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, third-party mobile device management (MDM) solutions or Microsoft System Center Configuration Manager (Configuration Manager).

Fast: Lower time-to-market and reduced maintenance

With a familiar app environment, tools and framework, Windows for IoT enables you to create and deploy solutions faster. Microsoft provides enterprise-grade development tools as well as hundreds of samples and professionally-maintained documentation (including commercialization guidance for testing and manufacturing) to help you solve complex problems such as extensive sample code. Windows 10 IoT comes with built-in security features and Azure IoT integration. With Visual Studio, you can code and test more efficiently. And we're consistently building out a library of repeatable IoT solutions across industries to help 'jump start' solution creation.

Windows works closely with device manufacturers to ensure Windows 10 IoT and Windows Server IoT 2019 work well across a very broad range of systems, devices and peripherals. The extensive Windows hardware ecosystem provides connectivity to many legacy systems enabling you to use what you have, making it easier to scale and deploy IoT solutions quickly.

Windows also supports familiar Microsoft deployment tools to enable 'zero-touch' provisioning for installing devices in the field and rapid scaling, once in market. An extensive library of management tools can help monitor and update the device OS & apps.

Examples of supported tools and services that can be leveraged for IoT scenarios include:

Azure IoT Hub enables highly secure and reliable communication between your IoT application and the devices it manages. Azure IoT Hub provides a cloud-hosted solution backend to connect virtually any device.

Azure IoT Hub Device Management provides the features and an extensibility model that enable device and back-end developers to build robust device management solutions.

Azure IoT Device Agent enables operators to easily connect their Windows devices to Azure IoT Hub to configure, monitor and manage them remotely from their Azure dashboard.

Azure IoT Hub Device Provisioning Service enables zero-touch, just-in-time provisioning to the right IoT hub without requiring human intervention, enabling customers to provision millions of devices in a secure and scalable manner while lowering the risk of manual error.

Mobile Device Management (Intune or 3rd party MDM) uses industry standards to securely manage a diverse set of devices. For companies already using MDM for laptops and phones, extending it to manage Windows 10 IoT devices can offer a cost-effective way to leverage existing resources and expertise.

Device Update Center provides the ability to create, customize and control device updates to Windows 10 IoT Core and device drivers as well as OEM-specific apps and files. Updates can be flighted to test devices prior to broader distribution. They're distributed by the same content distribution network (CDN) as Windows Update.

System Center Configuration Manager (SCCM) works with Intune to extend your SCCM to manage PCs, Macs and Unix/Linux servers along with cloud-based mobile devices running Windows, iOS and Android — all from a single management console.

Managing devices isn't simply about provisioning and monitoring.

Device operators need easy ways to lock devices and access to business apps. Over the years, Microsoft has evolved lockdown features to be simple, secure, manageable and comprehensive, including the following:

Assigned Access allows you to create a device that only runs a single UWP application, such as a digital sign or library kiosk. It can also create a managed user experience that enables multiple authorized applications, should a use case require it.

Shell Launcher is similar to Assigned Access and configures a device to run an application as the user interface, replacing the default shell (explorer.exe). With Shell Launcher v1, you can only specify a Windows desktop application as the replacement shell, However Shell Launcher v2, enables you to specify a UWP app as the replacement shell.

Microsoft Edge kiosk mode provides a tailored browsing experience for kiosks or digital signs using only a browser.

Unified Write Filter (UWF) can be used 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. UWF also extends the life of your storage media.

UWF with the Hibernate Once, Resume Many (HORM) feature can be used to resume to a predefined session.

You can **block keystrokes and gestures** (e.g. Ctrl-Esc, Ctrl-Shift-Esc, swipe left, etc.) to control user interactions.

You can limit **connecting USB devices** to specific devices you choose such as removable media (e.g. flash drives), keyboards and mice.

You can also control what a user sees from the moment the device is turned on until it's powered off. You can start by showing your logo instead of the Windows logo at boot, or you can auto-restart apps without error messages after an app crash, a system issue or a power interruption. These built-in features give developers a great deal of control over the experience and helps reduce time to market.

Minimizing maintenance over the long life of embedded devices also demands confidence that the solution will be functionally stable and supported for years to come. Windows 10 IoT Core Services, Windows 10 IoT Enterprise and Windows Server IoT 2019 are all available as Long-Term Servicing Channel (LTSC) offerings. This channel offers 5 years of mainstream support and 5 years of extended support. LTSC is appropriate for systems that require a longer servicing option and functional stability over many years. Deployments will not be affected by new features shipped in the Semi-Annual Channel (SAC) releases (The LTSC will continue to receive security and non-security updates, but it will not receive other new features and functionality).
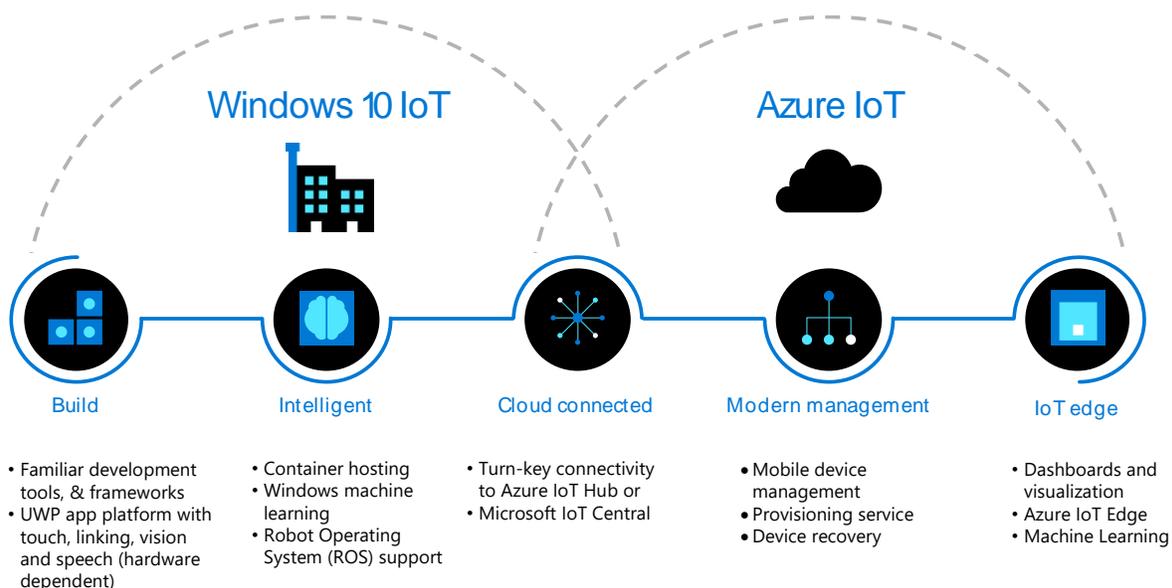
Better together: Windows for IoT and Azure IoT

Windows and Azure are built to optimize each other's features and strengths across the intelligent edge and intelligent cloud enabling you to:

Analyze data where it makes the most sense. You can analyze data at the edge and immediately act on it, sending only the results to the cloud. This makes IoT solutions more responsive and reduces bandwidth costs. For example, minimizing cloud latency is key to a predictive maintenance solution as a delay can endanger expensive machinery.

Move apps seamlessly between the Azure IoT cloud and Windows 10 IoT edge devices. Windows 10 IoT combined with Azure IoT Edge enables the development of advanced analytic apps using familiar programming tools like Visual Studio and multiple programming languages like C, Node.js, Java, Microsoft .NET and Python. You can also capitalize on Azure ML, Azure Stream Analytics and Azure Functions to create more advanced IoT solutions with less time and effort. These apps can be tested in the cloud and then deployed to edge devices by Azure IoT Edge.

With Windows 10 IoT and Azure IoT, you can move workloads to the edge, granting your edge devices some of the cloud intelligence roles. This gives you greater ability to analyze data, gain insight and take action locally and autonomously.

Windows 10 IoT		Azure IoT		
Build	**Intelligent**	**Cloud connected**	**Modern management**	**IoT edge**
• Familiar development tools, & frameworks • UWP app platform with touch, linking, vision and speech (hardware dependent)	• Container hosting • Windows machine learning • Robot Operating System (ROS) support	• Turn-key connectivity to Azure IoT Hub or • Microsoft IoT Central	• Mobile device management • Provisioning service • Device recovery	• Dashboards and visualization • Azure IoT Edge • Machine Learning

Conclusion

Windows for IoT provides a rich device platform, with world-class developer tools, enterprise-grade security and support, and a vast global partner ecosystem. You can do more at the edge with built-in ML capabilities and scale with the power of Azure IoT.

By consolidating all the Windows operating systems into a single core, Windows for IoT lets you support devices large and small, whatever best matches your needs. You can also take advantage of the expertise of thousands of Windows IT admins and developers and existing management infrastructure, giving you a familiar platform and deep knowledge base, so that you can focus on innovating and not building from scratch. Windows for IoT provides you with a trusted, secure and powerful platform to help you handle development and management challenges, and quickly scale innovative IoT solutions that address the needs of your customers.

Customer examples
Windows 10 IoT Core

IDEX uses Windows 10 IoT Core and Azure to create the world's first smart firetruck.

Every day, firefighters across the U.S. answer an average of 90,000 emergency calls. The reliability of their firetrucks in such situations can have life or death consequences. Monitoring and maintaining a firetruck's operational health however, can prove time and resource intensive, requiring hands-on diagnostics and unwanted downtime to resolve issues.

IoT solutions expert IDEX partnered with REV, manufacturer of the highly rated E-ONE Fire and Rescue vehicles, to implement the first-ever Smart Truck Technology platform. The system uses Windows 10 IoT Core and Azure to connect the numerous systems and components of a firetruck to provide technicians and maintenance crews with real-time insights into a vehicle's health. These diagnostic insights and network capabilities are helping technicians and maintenance crews increase vehicle reliability, reduce downtime and save lives.

Learn more about the IDEX and REV Fire Group solution here:
https://www.youtube.com/watch?v=bAT3sORVQqw

REDBACK TECHNOLOGIES

Redback Technologies' uses built-in intelligence supplied by Windows 10 IoT Core to develop an all-in-one solar power system.

When Redback Technologies started developing its residential and light-commercial Smart Hybrid System in 2015, it did so with the goal of giving homeowners an easy-to-install, all-in-one device that would capture the sun's energy and make the most of it — at an affordable price. The end result was its Smart Hybrid System, a compact, out-of-the-box unit that an installer can set up and run within a couple hours.

Without smart features, it would be impossible to centrally monitor systems, manage connected devices like hot water heaters and pool pumps or tell the system when to switch to and from grid power. Windows 10 IoT Core enables the company to put more smart features on the device, such as load shifting, which is used to switch on some appliances during the day when they can take full advantage of solar power. The device also saves surplus power to a battery, so that it can be used to power those appliances when the sun goes down. The fully integrated solar inverter simplifies installation and maintenance and helps shorten the return on investment for some customers to about five years.

Learn more about the Redback solution here:
https://customers.microsoft.com/en-us/story/redback-technologies

ASKEY

A new wearable device, powered by Windows 10 IoT Core, streamlines workflow across industries worldwide.

Askey designs and manufactures smart communications products for homes and industrial settings worldwide. The company wanted to improve workflow for mobile workforces in hotels, retail shops, manufacturing and other settings. These people too often rely on cumbersome electronic devices and paper forms to find and share information. The end result was TurboMate, a wearable device powered by Windows 10 IoT Core. The lightweight device can be clipped to clothing or worn on the wrist, enabling hands-free mobility and making it easy to wirelessly collect and share barcode data and other information. TurboMate also connects to cloud services including Azure IoT Hub and Azure Blob Storage. The Azure platform hosts customized dashboards and provides data management and analytics capabilities. In addition, Windows 10 IoT Core supports a touchscreen, camera, accelerometer, GPS, movement sensors and an optional biosensor for detecting heart rate.

Learn more about the Askey solution here:
https://customers.microsoft.com/en-us/story/askey

IoT solution helps keep emergency vehicles rolling on New York City's busy streets.

Emergency medical service (EMS) and public safety vehicle drivers rely on a constant supply of power—typically provided by the engine—to keep onboard equipment, including medical systems, running and ready for emergencies. The New York City Fire Department (FDNY) needed a solution that would do the seemingly impossible—enable drivers to cut power to the engine while keeping communications systems, heat and air conditioning, lights, refrigerators, life support devices and other mission-critical equipment turned on. The search led to Stealth Power and the installation of idle reduction technology on more than 300 ambulances.

In a groundbreaking initiative, FDNY installed Stealth Power's idle reduction technology, running on Windows 10 IoT Core, in more than 300 ambulances—with 76 more to come. The smart mobile power system includes environmental sensors and battery packs connected to an onboard data collection module running the Windows 10 IoT Core operating system. Stealth Power works with onboard technology with Azure. In addition to cutting fuel consumption and emissions, the IoT solution's real-time and predictive insights help reduce vehicle maintenance and downtime.

Learn more about the Stealth Power solution here:

https://customers.microsoft.com/en-us/story/732918-fdny-stealth-power-azure-powerbi-windows-iot

Customer Examples
Windows 10 IoT Enterprise

CityBeacon builds next-generation intelligent infrastructure that runs on Windows 10 IoT.

When designing smart cities, government leaders strive to take advantage of modern computing and communications while keeping their urban environment free of clutter and protecting citizen privacy. CityBeacon partners with municipalities, mobile network operators, and other ecosystem partners to outfit and deploy networks of SmartHubs within urban areas. Located on city streets and venues, these multifunctional kiosks house a variety of IoT devices, connect them to fast networks and give citizens access to hyperlocal apps and services.

The CityBeacon team uses Windows 10 IoT Enterprise to run the SmartHubs and displays, which are integrated with Azure. SmartHubs offer a flexible and modular architecture that supports a wide variety of uses. A SmartHub can house a set of devices that might include small-cell radio transceivers to support upcoming 5G networks, motion sensors, sensors that provide people count, security cameras, IoT gateways, microphones, speakers, webcams or EV charging apparatus. Each SmartHub has a superfast, telco-grade network connection that meets stringent Telco requirements.

Learn more about the CityBeacon/SmartHubs solution here:
https://customers.microsoft.com/en-us/story/749839-citybeacon

ActionPoint Innovative IoT solution uses the Windows 10 IoT Enterprise operating system to help manufacturers predict and fix problems before they occur.

Many leading manufacturers still use paper checklists, manual processes and legacy closed-loop technologies to monitor and maintain their equipment, in part because the challenge of launching technology that could help them automate their operations and take them online proves daunting. To make the transition easier, custom software developer ActionPoint partnered with Microsoft and Dell Technologies to develop IoT-PREDICT, an industrial IoT solution for predictive maintenance that enables machine learning and incorporates data analytics and other advanced capabilities. IoT-PREDICT helps manufacturers quickly reduce downtime, lower costs and increase the overall efficiency of their equipment and operations.

The IoT-PREDICT solution uses the Windows 10 IoT Enterprise operating system running on Dell Edge Gateway hardware, and combines it with Azure tools to provide state-of-the-art edge computing. For industrial IoT solutions, Windows 10 IoT Enterprise provides enterprise-class power, security and manageability, enabling organizations to deploy secure IoT devices that their IT teams can quickly provision, easily manage, and seamlessly connect to their cloud services as part of their overall cloud strategy.

Learn more about the ActionPoint solution here:
https://customers.microsoft.com/en-us/story/actionpoint-discrete-manufacturing-azure-analytics

acquire Innovative digital display, based on Windows 10 IoT and Azure, captures attention on the Las Vegas Strip.

Acquire Digital has been designing innovative content management software for digital displays since 2001. Its customized, award-winning digital signage packages power more than 20,000 installations worldwide. Simon Property, which has a global portfolio including more than 200 shopping centers, wanted Acquire Digital to help build a more scalable digital signage solution at one of its premier properties — The Forum Shops at Caesars Palace in Las Vegas.

Acquire Digital created a content management system and a media player that could seamlessly deliver multiple layers of content across multiple LED screens for a cinematic experience. The LED displays are powered by content management and media player software running on-premises with Windows 10 IoT. Other components, including advanced analytics and software used to book advertising, run on Azure. The boundary-busting pylon has six large LED screens that display content on the front and back sides of the structure. Simon Property employees easily control content with Acquire Digital's customized content management system.

Learn more about Acquire Digital's customized its digital communications platform solution here:
https://customers.microsoft.com/en-us/story/acquire-digital

Examples of Windows Server IoT use cases

Windows Server has been used in embedded scenarios for years. With Windows Server IoT, you can build dedicated, sever-class appliances that can perform a multitude of functions. Examples include:

Security and surveillance

Analyze multiple video streams in surveillance and security monitoring systems to identify people, activities and potential threats, using AI-enabled cameras. Use Windows Server as an edge-based Video Management System for storage and deeper analysis.

Manufacturing

Use Windows Server IoT 2019 to monitor the health of industrial automation equipment to predict maintenance needs and improve field-service efficiency. Or perform defect detection on high-speed manufacturing lines. You can also use video analytics and AI to perform real-time defect detections on the production line.

Smart buildings

You can enable intelligent building scenarios like optimizing energy use or monitoring enterprise fire and life safety. Build solutions to connect building devices and systems to bring more efficient operations and control to building owners, operators and occupants – optimizing energy, air quality, security, lighting and HVAC with ML.

Healthcare

Windows Server IoT 2019 can be used in medical imaging technologies such as picture archiving and communication systems (PACS) to provide economical storage and access to patient images. Prior versions of Windows Server embedded are being used in automated medication dispensing systems to help protect patient data on-premises.

Smart cities

Windows Server embedded/IoT can be used in solutions that monitor complex and rapidly changing environmental conditions like air and water or to track status and optimize public transit routes based on conditions provided by sensors in vehicles.

Retail

Use a dedicated backend server database for content management services in digital signage or broadcast television systems supporting audio and video communication solutions such as live media, entertainment workflows and streaming. You can develop solutions to monitor shelf inventory and quality (object detection), and track consumer behavior and deliver recommend products.

Resources

Windows resources

General

Windows IoT the foundation for your intelligent edge

Windows Dev Center: Windows for Internet of Things

Windows for IoT documentation

Minimum hardware requirements for Windows 10

Bringing the intelligent edge to robots with ROS on Windows 10 and Azure

Robot operating system on Windows 10 and Azure

LTSC: What is it, and when should it be used?

Microsoft Defender Advanced Threat Protection

Windows 10 IoT Core and Windows 10 IoT Core Services

Windows 10 IoT Core manufacturing guide

Windows 10 IoT Core Services

Windows 10 IoT Core security features

Windows 10 IoT Enterprise

Windows 10 IoT Enterprise manufacturing guide

Windows 10 IOT Enterprise system requirements (Note: same as Windows Pro)

Windows 10 IoT Digital Signage

Windows 10 IoT Kiosk solutions

Configure kiosks and digital signs on Windows desktop editions

Mapping of previous Windows embedded lockdown features to Windows 10 IoT Enterprise

Windows Server IoT 2019

Windows Server IoT 2019 system requirements

Windows Server IoT 2019 security

Azure resources

General

Azure IoT

Azure IoT Hub

Azure IoT Edge

Azure IoT Central

Azure Sphere