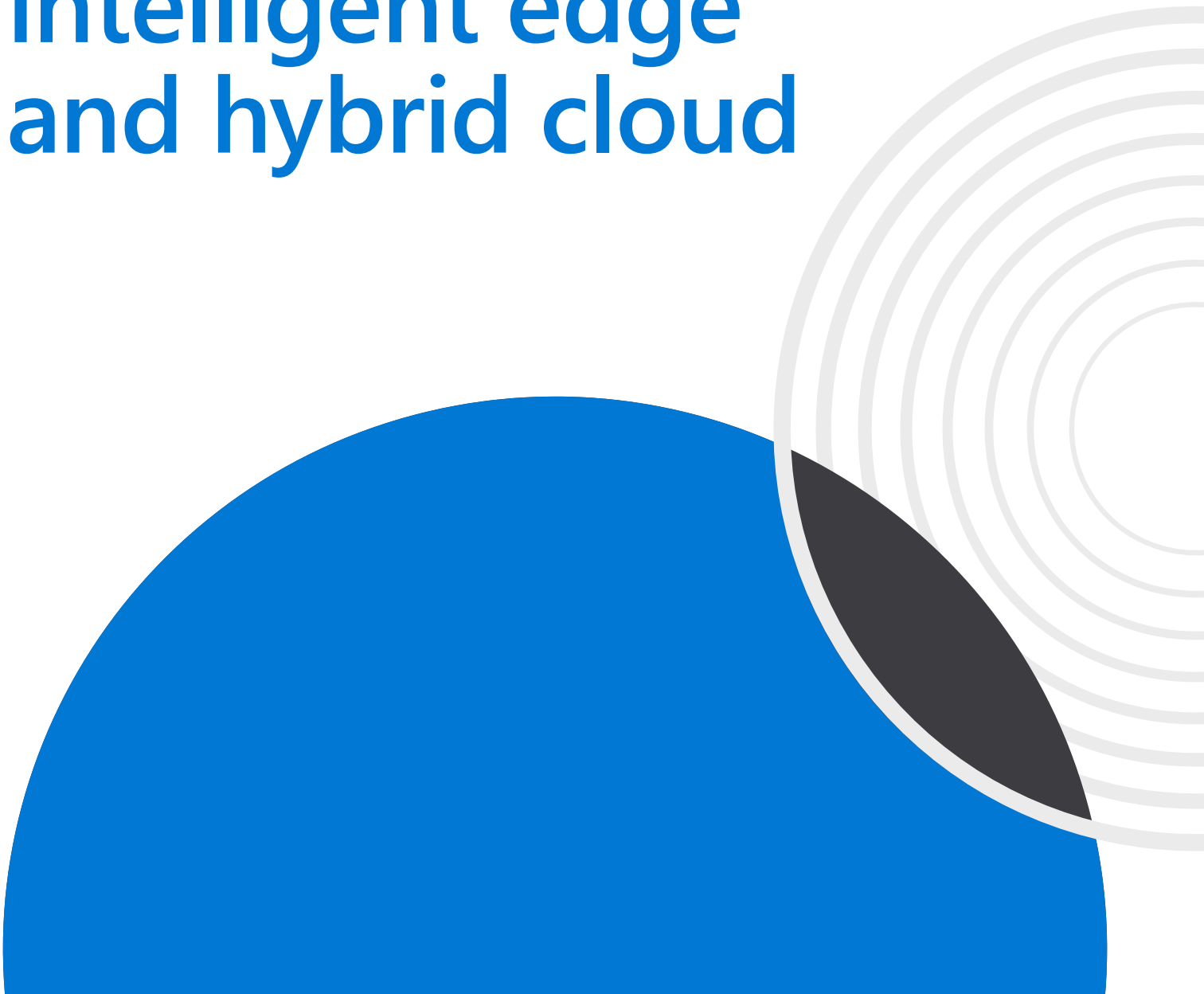
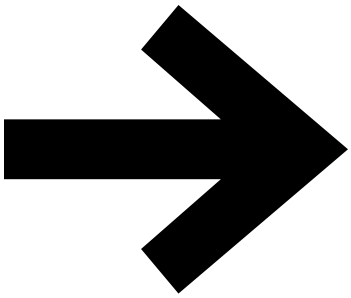
Azure Government e-book series

Microsoft

Transforming government agencies with intelligent edge and hybrid cloud





01 Introduction

Imagine: a looming hurricane warning is becoming a reality. A state of emergency has been announced. Power and communications are down, and emergency response teams need to set up a base of operations and assess the situation.

Enter the mobile command center—a multifunctional operations hub that provides varying levels of communication and coordination capabilities.

Serving as the hub for an ad-hoc wireless network, the command center allows response teams to connect mobile devices and access application services for logistics. This command center is technically a slice of the cloud—compute, app, and storage layers that offer the same robust services and resources that are associated with large cloud service providers.

Extending this fabric is a series of devices that track weather conditions, relay communications, and provide artificial intelligence–assisted vision to spot people needing assistance or identify potential threats. Connecting these devices are edge computing systems that manage sensors and actuators, providing local computing capabilities with a degree of intelligence that enables them to draw instant insights and even act, in particular cases. The data and insights are also communicated back to the command center for additional in-depth analysis.

This enables relief workers to focus more on the tasks related to protecting and preserving human lives—and less on logistics and administration.

Recent advances in intelligent edge capabilities represent an opportunity for the government sector to effectively embrace digital transformation to accomplish their missions. These advances could change the way relief efforts are planned, coordinated, and executed.

Microsoft offers the technologies and solutions to help your agency promote citizen well-being, influence positive societal change, and enhance your services.

The Microsoft commitment

Intelligent cloud and intelligent edge solutions are at the core of the Microsoft effort to facilitate digital transformation of government agencies. Microsoft envisions three key areas to drive a paradigm shift in the way agencies and staff work, encouraging new growth, collaboration, and opportunity for government agencies.

Bringing multi-sense, multi-device capability to applications is the first area that can drive these improvements by focusing on improving the people-centric experience. This capability enables the app experience to work across your devices, and can be extended with automated data collection and analysis through cognitive experiences such as sight and sound.

The second area, artificial intelligence (AI), will be key in making these experiences more intelligent. It will give applications perception, language, and autonomous capabilities that will change the way we interact with technology.

The third area is a secure, ubiquitous, distributed fabric—stretching from on-premises to the cloud and out to the edge. This provides unified security and compliance for all systems, devices, and intelligent sensors.

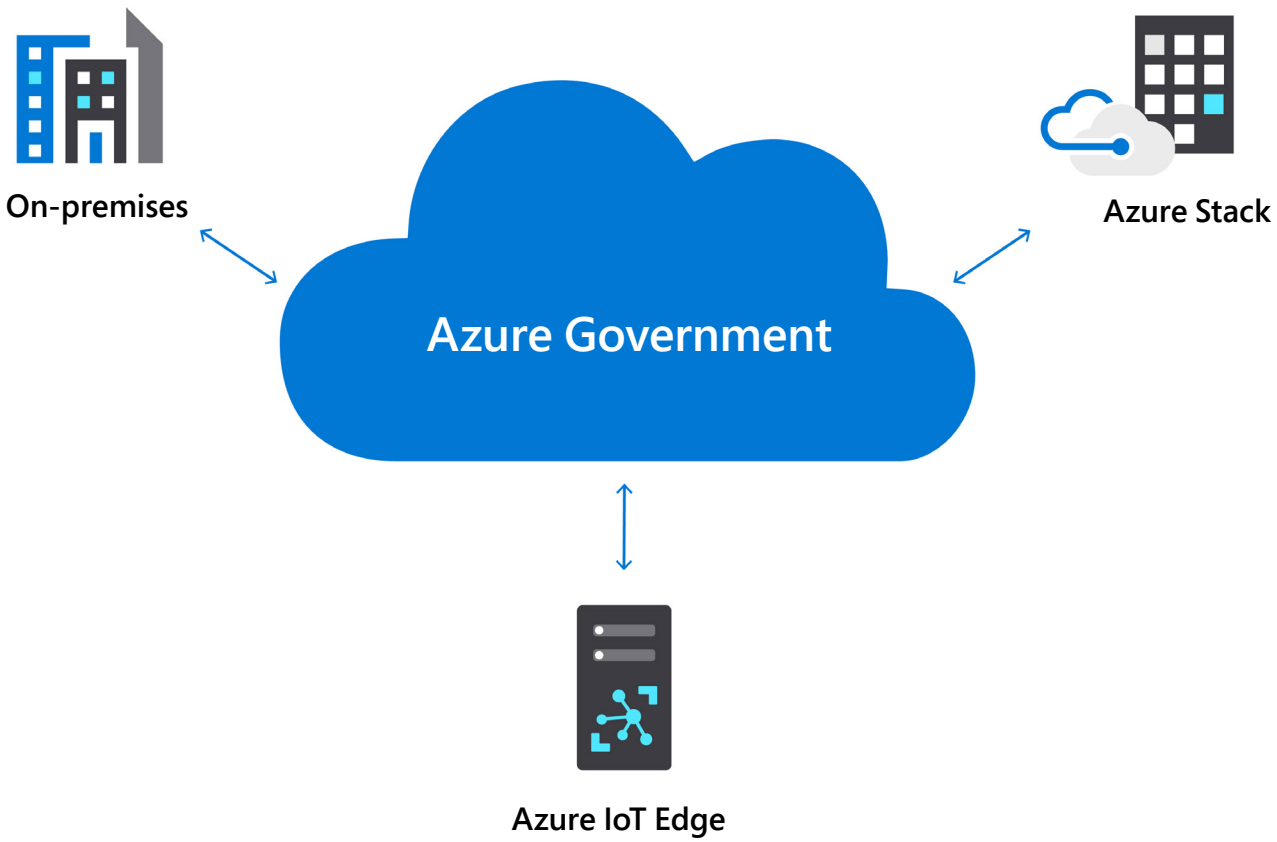
02

Intelligent edge approach

Today, technology in government agencies is going through a transformation, unlocking new mission scenarios that were not possible before. Smart sensors are changing the way agencies approach problems, while new intelligent edge devices are extending the reach of agencies' computing and analytical capabilities past on-premises and cloud solutions.

These connected systems and devices can help government agencies across a huge array of mission goals, such as tracking water quality, improving emergency responses, speeding maintenance of vital equipment, and bringing insight into complex real-world logistics problems. For example, using modern edge devices to better collect, store, and act on data, state and local government agencies can create “smart cities” that enable autonomous cars to make real-time decisions based on traffic and road conditions.

Increasingly, computing and data processing will be happening at the network edge, where devices and users are located. This enables government agencies to analyze relevant data in near real-time. When we take the power of the cloud down to the device—the edge—we provide the ability to respond, reason, and act in real-time and in areas with limited or no connectivity. As an extension of your agency's infrastructure, the intelligent edge brings AI, apps, and analysis closer to those who need it, wherever they're located.



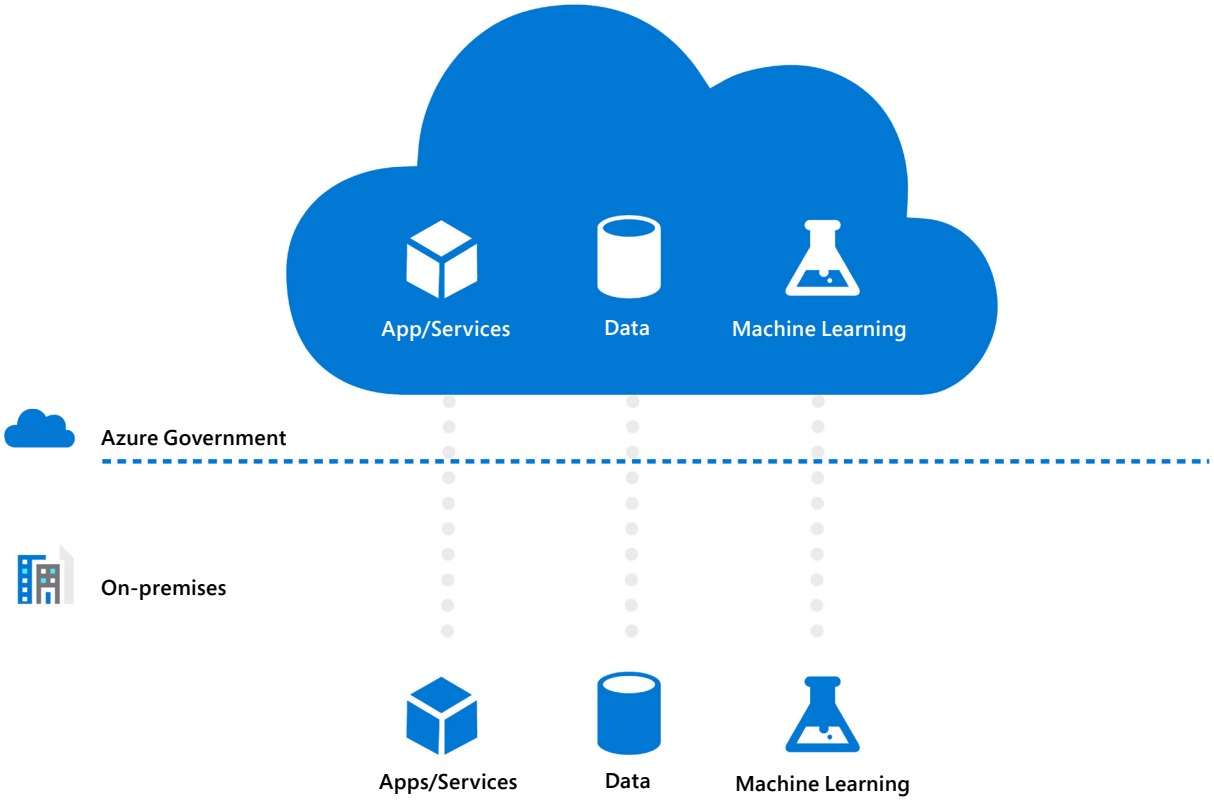
Hybrid cloud

Hybrid cloud typically combines on-premises (accessible only within an agency's network) infrastructure with public cloud (accessible to the general public) services. You can choose a hybrid strategy for many reasons, such as the ability to help achieve greater flexibility, to meet regulatory requirements, or to take advantage of the public cloud while leveraging existing on-premises technology as an asset.

Hybrid cloud has evolved. From the integration of a data center with the public cloud, it has now become units of cloud computing available at the edge—including the world's most remote destinations. Using hybrid cloud with edge devices and AI, government agencies can accelerate the era of the intelligent edge solutions. The same patterns and principles of building cloud applications apply to hybrid and edge applications—the investments you make and the skill sets you develop are fully ubiquitous across any environment, reducing retraining and supporting costs. Microsoft hybrid cloud offerings also work seamlessly with existing on-premises networks to extend agency capabilities without requiring any additional hardware from your agency.

Governments are unique; they manage controlled and highly sensitive citizen data. As such, they require a solution to make hybrid cloud safe, secure, and compliant with all government regulations.

To help assist with these unique needs, Azure Government delivers a dedicated cloud that enables government agencies and their partners to transform mission critical workloads while continuing to uphold high standards for security, data protection, and compliance. Providing similar experiences and services as the Azure commercial cloud, Azure Government delivers a physically isolated environment created exclusively for DoD, federal, state, local, and tribal governments. Customers can choose from six government-only datacenter regions across the United States, including two regions granted an Impact Level 5 Provisional Authorization.



Azure Government also offers the most compliance certifications of any cloud provider, including:

- Criminal Justice Information Services (CJIS) Security Policy
- Defense Federal Acquisition Regulation Supplement (DFARS)
- US Department of Defense (DoD) Provisional Authorizations at Impact Levels 5, 4, and 2
- Federal Risk and Authorization Management Program (FedRAMP Moderate and High)
- Federal Information Processing Standard (FIPS) 140-2
- US Internal Revenue Service Publication 1075
- International Traffic in Arms Regulations (ITAR)
- National Institute of Standards and Technology (NIST) 800-171
- NIST Cybersecurity Framework (CSF)
- US Section 508 VPATS

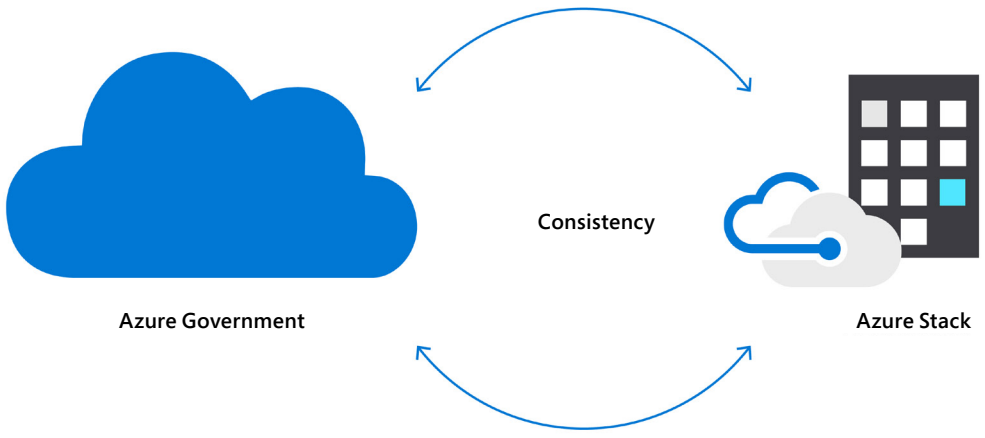
Implementing hybrid cloud with Azure Stack

When choosing cloud services, it's easy to get lost in the sea of product names and features. To assist with this, Microsoft took its best in class commercial cloud platform and devised a method to enable customers to physically locate it on their premises. Azure Stack, one of the key solutions powering hybrid scenarios, brings consistent infrastructure and services to the intelligent edge.

Today, a challenge for many government agencies is addressing the difference between on-premises systems and the public clouds they use. It can be difficult to move applications and data from one site to another, as the platforms they run on can be quite different. As a cornerstone of Microsoft's hybrid cloud approach, government agencies can deploy the same platform used in Microsoft's Azure cloud to their on-premises environment. This enables agencies to develop, deploy, and manage with a consistent set of tools, unlocking data and application portability. Azure Stack enables agencies to modernize their on-premises environments where localized infrastructure is required, or when public cloud connections can't be reliably achieved.

Azure Stack unlocks a wide range of hybrid cloud use cases for government agencies, including:

Decision making at the tactical edge
For government agencies and their field operations, speed is critical, and insights empower decisions. Azure Stack is an extension of Azure, and you can take advantage of these powerful hybrid capabilities to bring core and advanced cloud services to the edge—whether it's a field office, mobile command station, or remote location. With Azure Stack, it's possible to process data in the field without worrying about latency or internet connectivity, and then run aggregated analytics in Azure Government to get the most precise predictions and anomaly detections. In these scenarios, hybrid cloud extends from the enterprise to the tactical edge, which lets you bring Azure cloud to remote locations that can be connected, offline, or disconnected environments. Azure Stack can be used by first responder units or essential function teams, agencies, or departments that use satellite or other transient means of communication, providing the advantage that comes from immediate insight.



Solutions for meeting regulatory requirements

When embassies or offices in foreign countries aren't able to use local cloud services or applications because of data sovereignty laws, Azure Stack can help to meet regulatory requirements. You can use a combination of Azure Stack and Azure Government to support the full spectrum of unclassified and classified data, special access programs, and various data export policies. Azure Stack also meets requirements for FedRAMP Moderate.

Any solution for a modern government should ensure strict security measures that adhere to confidential, controlled, and high-impact data requirements, including compliance regulations. You can develop and deploy applications in Azure Government and then deploy those exact same applications to Azure Stack on-premises, all using a consistent set of tools.

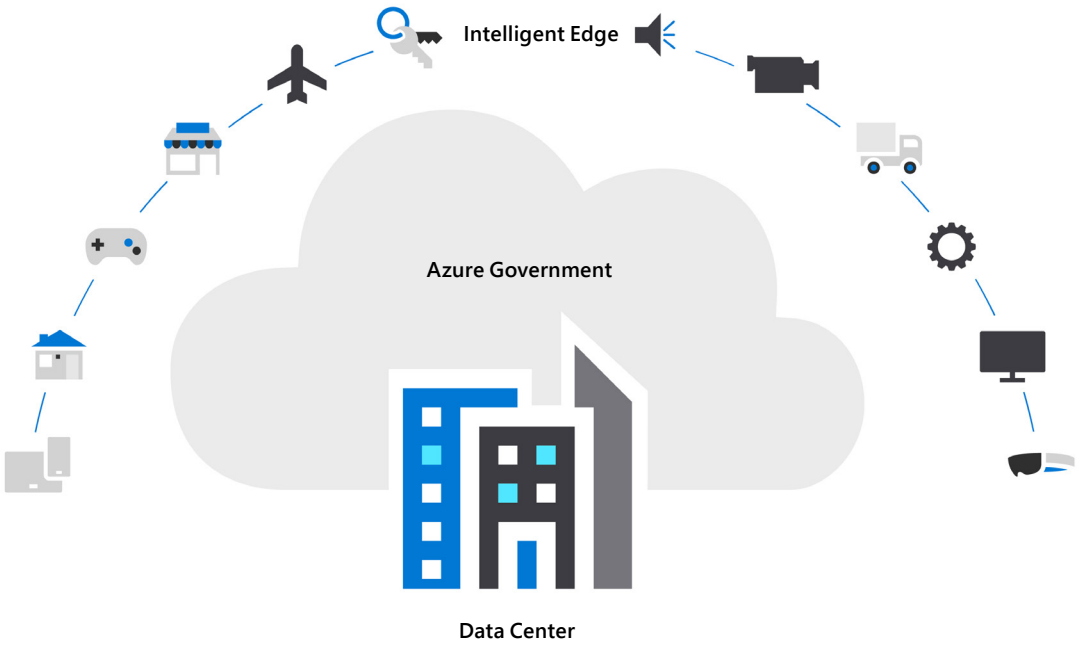
Solutions for modernization requirements

Many agencies feel blocked from modernizing their on-premises legacy applications, either because of security concerns or because they feel that the cost and effort of development for the cloud is too high. Azure Stack brings a core set of Azure services that enables your developers to easily port their applications to cloud services without significant changes or updates. With these services, you can take advantage of new security, management, and availability options that were previously unavailable on older on-premises environments. Over time, you can move these applications to Azure without making any changes to code, DevOps tools, processes, or skill sets.

Bring cloud intelligence where it's needed

Cloud services enable intelligent analytics to drive faster, more informed decision making. With Azure Stack, you can now also drive the same public cloud experiences to remote and isolated locations. But what if you want to go one step further? What if you want a device or sensor to act intelligently? To be able to utilize machine learning and take action even when isolated from control? The explosion of the Internet of Things (IoT) has enabled a plethora of connected devices and sensors everywhere. Now you can bring the same analytical, learning, and decision-making intelligence directly to your IoT devices with Azure.

Azure IoT Edge enables government agencies to bring cloud intelligence to the edge and act immediately on real-time data, whether it be a drone in a city recognizing a traffic jam and updating traffic apps to reroute, or a device predicting equipment failure and redistributing system load before it happens. IoT Edge also brings AI and cloud analytics in cases where poor or no connectivity, high latency, or high costs would have prevented direct connection to government cloud services.



AI and analytics

IoT Edge allows you to deploy complex event processing, machine learning, image recognition, and other high-value AI solutions directly to the field or to remotely located devices. The same machine learning models that agencies use in their Azure Government subscriptions can be deployed to the edge, enabling on-site analysis and insight generation. AI is only as good as the dataset running it—and to have a truly automated and intelligent edge system, your platform must have exposure to many real-world and contextual insights. Your Azure edge devices constantly gather real-world data that is collected and analyzed, driving updates and new machine learning models. Models are continually distributed across your edge devices, making them more intuitive to their mission.

Offline operability

With IoT Edge, your edge devices operate reliably and securely even when they're offline or have intermittent connectivity to the cloud. Azure IoT device management automatically syncs the latest state of devices once they're reconnected to ensure seamless operability.

Security

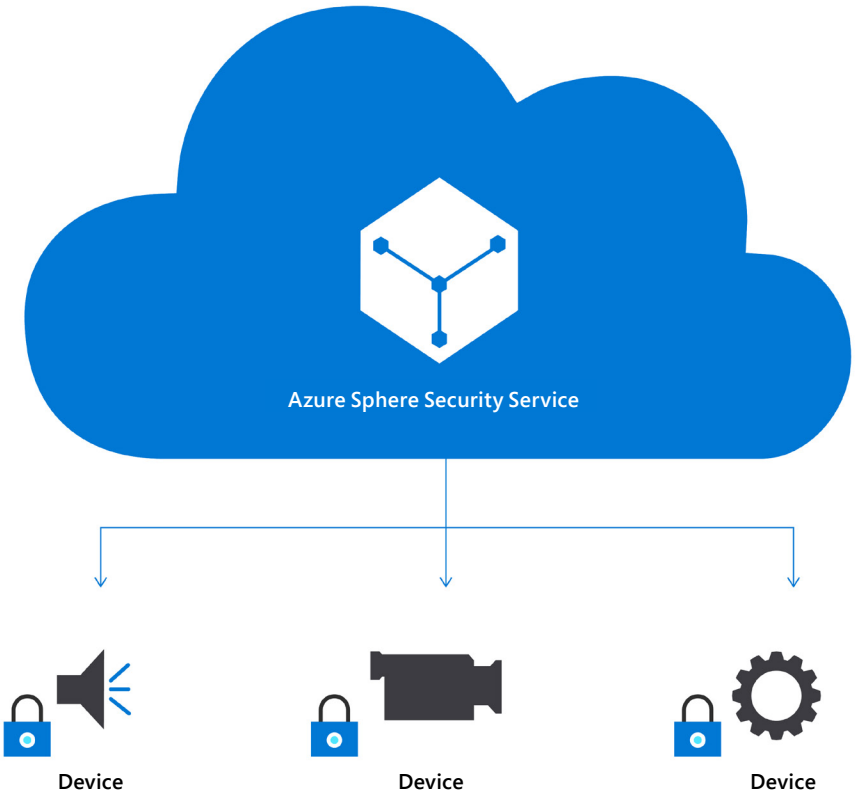
As government agencies are highly visible and usually very connected to citizens, any security issue can reduce trust. Intelligent edge devices have to be part of any agency's security planning. They are much "smarter" than most IoT devices; in contrast to the common sensors and actuators class of IoT devices, they both collect and analyze sensitive data. Many intelligent edge devices have the capability to operate mechanisms like engines, valves, switches, and more—mechanisms that can cause personal, property, and financial damage if they were to be maliciously operated.

With security in mind, Microsoft designed Azure IoT Edge with a solid foundation of security principles. The security framework was created from industry-proven security protocols and designed to be extensible to various risk profiles and deployment scenarios. Authorization operates on the principle of least privilege—meaning devices and modules can access data and resources only within the limits of permission scope and architecture allowances. This ensures that captured devices can't be used to piggy-back into the larger systems or introduce malware to other devices or users.

Secure devices for a safer network

Today we see government agencies using more and more connected edge devices. Many devices are powered by microcontrollers—low cost, single chip computers. This connectivity may be evolutionary, but also can create vulnerabilities. To protect data wherever it lives, security needs to be baked in from the silicon to the cloud. This has been one of the central design principles of Microsoft's intelligent edge products and services.

Azure Sphere is Microsoft's intelligent edge solution to power and protect these connected microcontroller devices. Security is built right into the silicon, and is constantly renewed by Azure Spheres cloud services, identifying threats and brokering trust among devices, the cloud, and other endpoints.



03

Scenario: disaster relief with the Microsoft intelligent edge

The Federal Emergency Management Agency (FEMA) defines continuity of operations (COOP) as "the activities of individual departments and agencies and their sub compartments to ensure that their essential functions are performed." [1] The activities associated with COOP include testing and training that ensure COOP capability as well as plans and procedures to ensure that essential functions are performed.

Microsoft intelligent edge solutions have much to offer initiatives like COOP, providing secure, resilient, and robust technologies and services for every phase of the relief operation, regardless of any lack of connectivity or infrastructure. Let's return to the emergency response team for the hurricane from Chapter 1 and look at how they take advantage of these solutions.

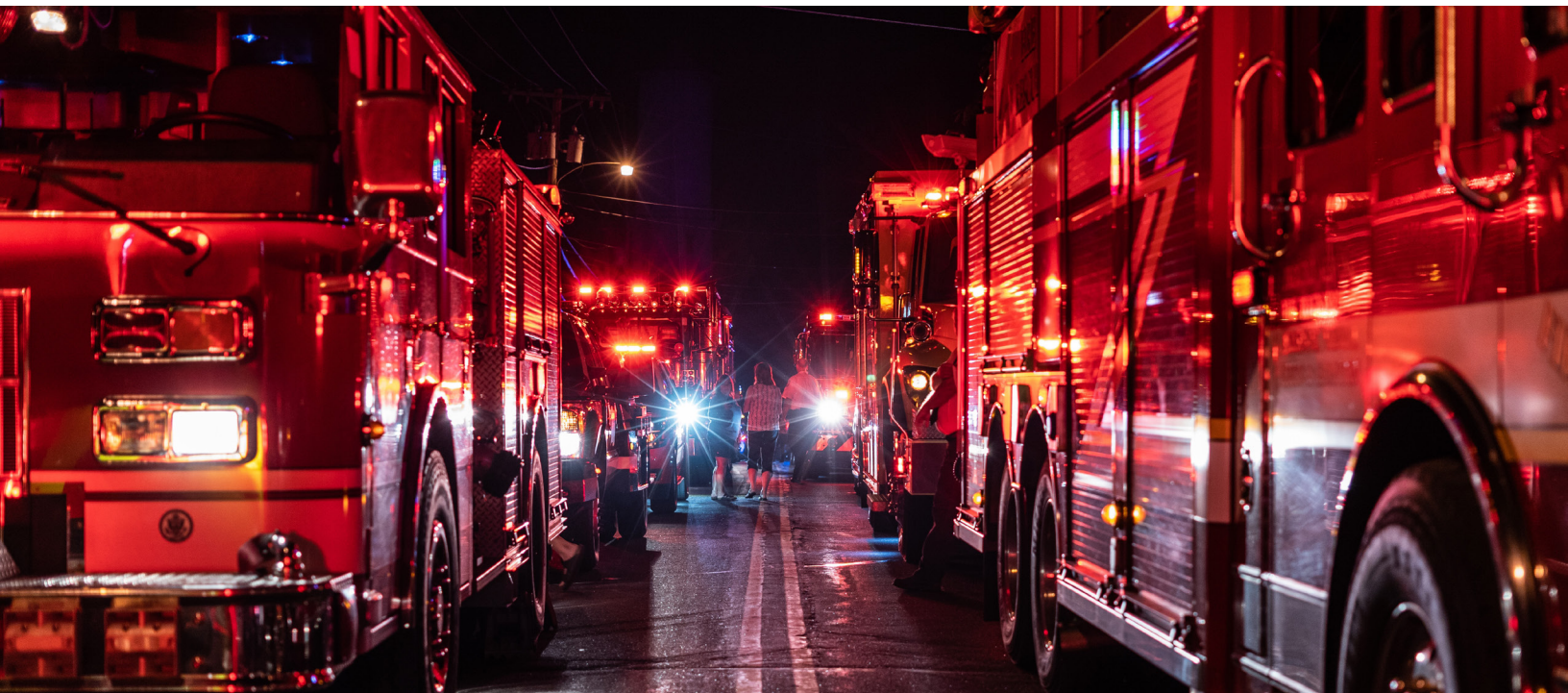
1 https://www.fema.gov/pdf/about/org/ncp/coop_brochure.pdf

Phase I: readiness and preparedness

In the initial stage of planning, the response team looks at their data and infrastructure architecture. They answer questions such as: how many citizens live in this area? What is the layout of the area and are there any geographical challenges? Additionally, the response team evaluates its essential functions and resource requirements to address the situation. What are the operating needs to complete their tasks? Is a hybrid cloud solution sufficient for these needs? What are their requirements for infrastructure in a remote or disconnected location?

These questions help guide the evaluation of their essential functions, which will, in turn, help them determine how much autonomy they need in this situation.

A mobile hybrid cloud deployment is capable of providing critical network infrastructure and services in an area with limited or no connectivity to the internet. If there's an area in the field that has an unreliable signal and contains IoT devices, the team can rely on their offline operability to ensure that data collection will continue during an emergency. By deploying trained and intelligent modules in the field, they can ensure that these systems can perform analysis and draw insights independently, forwarding data and insights when connectivity is available. With intelligent edge technologies, the key teams of support members, as well as IT staff supporting the systems, spend less time getting set up and more time focusing on the relief effort.



Phase II: activation and deployment

Indicators from weather sensors have caught onto some high winds and heavy rain rolling through. The pattern is unpredictable—and shaping up to be a large concern. As an incident on the pass causes the last-mile internet service to go down, it's evident to the agency that it's only a matter of hours before the surrounding community will be affected. The response team is aware of the problem and has already met several times to talk about deploying sensors to monitor more detailed weather patterns, road conditions, power, and communications.

Once the plan is in place, the team quickly begins to organize and pack essential gear, including the intelligent edge devices and systems to be deployed onsite. These monitoring systems are interconnected, enabling the team to receive comprehensive reports on the situation as it develops. As the event continues to build in severity, the team is called to a press conference. A state of emergency is announced.

Phase III: operations in the field

Before operations begin, the team needs to establish a base of operations. They'll also need a means of collecting data from the area of operation to assist both in the relief effort and in gathering up-to-the-minute information on weather and road conditions.

The question is, how will they do this? While FEMA can establish communications via satellite, there are limitations on bandwidth and latency. This can create issues if data, apps, and analytics are on-premises or cloud-based and need to compete with critical communications or information gathering. Microsoft intelligent edge solutions provides the key capability needed to save lives and properly support emergency teams.

Hybrid Cloud capability: using Azure Stack in the operations center

With its hybrid cloud capability, the operations center is the beginning of the local intelligent edge. The deployed implementation becomes the cloud connection for local client devices, including computers and laptops, tablets, and mobile devices—offering the same infrastructure and app services as the Azure Government cloud. Azure Stack gives the

operation center the capacity to operate as an ad-hoc onsite cloud, able to use internet connectivity as available but also capable of sustaining the entire relief effort.

Remote monitoring and analysis: using Azure IoT Edge

Critical infrastructure is down, but the relief team needs real-time information to do their jobs and stay safe. With the advent of the network-connected sensor and IoT devices, they can gather data and monitor the situation closely. Emergency services can gain access to real-time insights with IoT Edge devices—even if internet connectivity can't be established. Edge devices don't just forward data for analysis or manage sensors and machinery by collecting data; these devices can use machine learning to perform deep analysis, make weighted decisions, and even execute functions. For example, an IoT Edge device monitoring pressure in a flood dump valve will not simply report the pressure back to command—it will make calculated decisions about when to open the valve and relieve pressure without human intervention. Best of all, it is in communication with other IoT devices, so they can work in unison to react to unexpected changes and minimize impact.

Security: using Azure Sphere

At the core of these devices is the latest in IoT device security: Azure Sphere. The last thing the emergency team needs when focused on saving lives and property is to succumb to malicious cyber-attacks. With Azure Sphere, the team can place a mesh of sensors and actuators that are highly resistant to side-channel attacks. The single-purpose hardware is immune to reuse by attackers and can detect and mitigate against physical attacks. When used to protect secrets and device correctness, the hardware provides a solid foundation of trust with which rich software functionality can be implemented securely and safely. If a device fails, the Azure Sphere automatically collects failure reports and sends them to an analysis system, alerting the team of potential attacks to the infrastructure. This enhanced security helps alleviate concerns that malicious activity could compromise the relief effort.

Phase IV: reconstitution

As they round out an exhausting month of relief operations and recovery assessments, the team starts preparing to get back to operations as normal and examining the overall performance of the COOP plan. Azure Government continues to play a critical role, as edge devices and the hybrid cloud deployment have collected and analyzed data throughout the entire mission. The reports and insights generated from this data provide clear, unbiased evidence of the events of the past few weeks.

When the mission is completed, all aggregated data can be fed to the machine learning models that the rescue teams use, made available across agencies and enriching current predictive models. The intelligent edge continues to improve, helping the relief team—and the agency as a whole— become better prepared and more efficient when dealing with future events.

04

Accomplish your missions with intelligent edge

With advances in hybrid cloud and intelligent edge capabilities, government agencies and departments are able to embrace digital transformation to accomplish their missions in increasingly effective ways. The Microsoft commitment to empowering every person and every organization on the planet to achieve more continues to drive industry change in every sector—including government agencies.

The hybrid cloud capabilities of Azure Government coupled with secure intelligent edge solutions provide trusted, scalable, and secure infrastructure and services to your agency. Integrate advanced intelligent apps and tools that operate seamlessly across your agency compute fabric, enabling your teams to focus on mission success regardless of where your agency's mission takes you.

Next Steps

Request a free trial
Have Microsoft contact you about Azure Government
Learn more about Microsoft in government
Additional resources

Resources

Azure Government

Azure Government website

Azure Government enables digital transformation | US Veterans Affairs

Hybrid cloud

Creating order when data is everywhere

Harnessing the intelligent cloud for defense

The only consistent hybrid cloud

Azure Stack

Azure Stack brings Microsoft's cloud outside Microsoft data centers

How Azure Stack helps Microsoft deliver the promise of intelligent cloud and edge

Announcing Azure Stack for Azure Government customers to enable IT modernization and tactical edge scenarios

Announcing Azure Stack integration with Azure Government

IoT

Azure IoT Edge

Microsoft Azure IoT Edge—extending cloud intelligence to edge devices

What is Azure IoT Edge?

Azure IoT Edge: a breakthrough platform and service running cloud intelligence on any device

Azure Sphere

Azure Sphere overview

Azure Sphere news

Detailed information about Azure Sphere

FEMA

FEMA 2017 hurricane season after-action report