

Digital Solutions
Hardware Solutions

Deploying IoT solutions with Avantor

A guide to ensure IoT solutions work as you want



Gathering data about your business or research facility has become a critical component of success in the 21st century. One of the most valuable categories of data collection tools are smart devices. They are part of an Internet of Things (IoT) solution. Smart devices are designed to monitor their environment through sensors and transmit sensor data over a network so it can be aggregated, analyzed, and acted upon.



“The core advantage of data is that it tells you something about the world that you didn’t know before. As your competitors learn more, you’ll need to learn, too.”

– Hillary Mason, data scientist and founder of Fast Forward Labs

Avantor’s commitment to the digital lab and innovation, has resulted in the development of a data collection methodology that uses a variety of smart devices that enable our customers to understand their (lab) activities better, increase their efficiency, and proactively identify opportunities for improvement in processes, sustainability and efficiency based on data and metrics.



Deep lens camera



RFID scanner



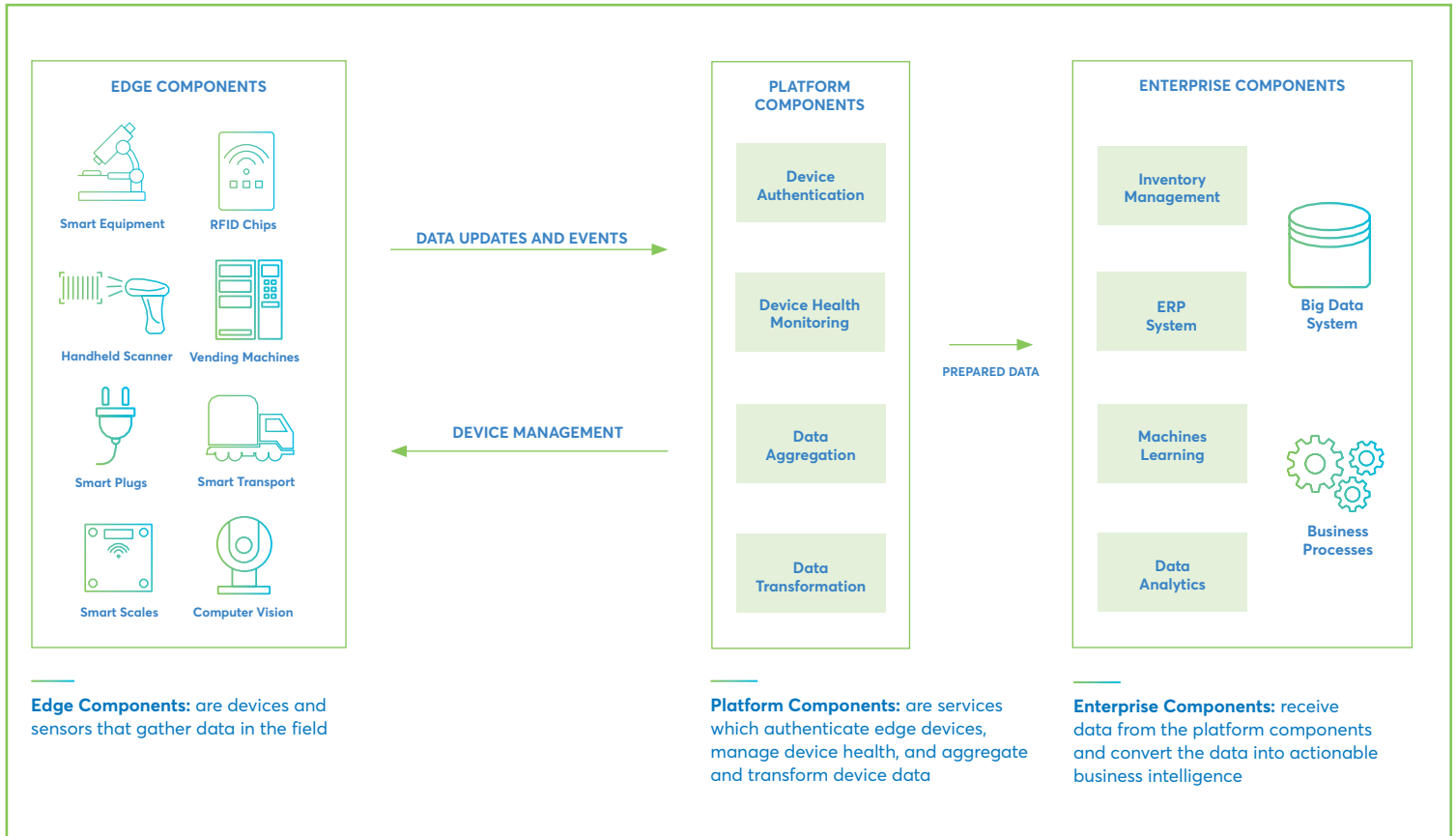
Smart button



Smart shelves

COMPONENTS OF AN IoT SOLUTION

IoT solutions consist of many components, from the sensors which capture data to the enterprise systems which convert information into actions.



EDGE COMPONENTS

As the name indicates, the edge components in an IoT platform comprise the sensors and devices which are deployed in the field to gather data. Although there is wide variation in device type and deployment environments, the essential functions of an edge component include:

- Capturing data points or events
- Communicating captured data to platform components
- Reporting status and health information to platform components

TYPES OF EDGE COMPONENTS

Avantor's IoT platform utilizes a variety of edge devices and connectivity options (see table to the right).

	Common use cases	Supported network connectivity options	Power requirements
Vending Machine	Provides access to products and tracks usages	Ethernet, Cellular	AC power supply
RFID Kiosk	Tracks consumption of products based in RFID tags	Ethernet, WiFi	AC power supply
Tablets	Tracks stock levels and consumption via manual entry in mobile application	Wifi, Cellular	Rechargeable battery
Handheld Scanners	Scanning barcodes to set stock levels or track consumption	Wifi	Rechargeable battery
Load Cell Sensors / Scales	Tracks weight of containers to determine current stock levels	Wifi, Ethernet	Rechargeable battery, AC power supply
Cameras	Use computer vision to track stock levels and outages	Wifi, Ethernet	AC power supply
Smart Plugs	Track electrical usage of appliances and equipment to determine utilization	Wifi	AC power supply

IMPORTANT PLATFORM CONSIDERATIONS

When deploying edge components, Avantor recommends that the following important topics are discussed:

Limit Network Connectivity

IoT devices need to be connected to transmit data and events to the platform components. However, their access should be extremely limited as this protects your organization's security and also reduces the impact if one or more devices starts to consume too much bandwidth or cause network issues.

You should limit connectivity by:

- Installing IoT devices on a separate network or completely segregated network segment
- Limiting outbound connectivity to specific platform component addresses/networks
- Limiting inbound connectivity to platform components that manage devices
- Separating devices from different vendors on their own networks (if possible)

Limit Security Risk Exposure

Edge devices are a potential security risk and IoT solutions should account for this. Integrating third-party devices into your network means you need to take additional precautions to account for the increased risk.

You can mitigate security risk exposure by:

- Following the limited network connectivity guidelines listed above
- Encrypting all communications from edge devices with modern, secure encryption protocols
- Installing patches and firmware updates as they are made available
- Always changing default password, usernames, and device names (if applicable)

- Routinely inspecting network traffic and data to validate that it matches expectations
- Ensuring that devices only capture the necessary data (e.g., correct camera placement)
- Processing sensitive data in edge components rather than transmitting it to the platform components

Limit Data Loss

IoT edge devices often have to function in less-than-ideal conditions. Dealing with connectivity issues, device failures, and data capture outages should be an integral part of your IoT solution.

Many data loss issues can be addressed with measures like:

- Implementing device monitoring to detect outages as soon as possible
- Monitoring network connectivity to ensure devices can communicate with platform components
- Designing IoT solutions which can store collected data locally in case of temporary connection problems
- Preferring AC power sources (either direct or daisy chained) with battery backup
- Deploying uninterruptible power supplies for devices and network components
- Using redundant devices to capture and verify critical data events

Implementing IoT solutions successfully can be a challenging and potentially risky endeavor. It is important to partner with IoT providers who have wide experience with IoT platforms and are able to adapt their solutions to your specific needs. Through their services programs and IoT solution portfolio, Avantor is focused on helping customers safely capture data and convert it to competitive advantage.

Do you need help with digital solutions to streamline your workflows?

Visit avantorsciences.com/digital-solutions or email services@avantorsciences.com for more information.

Avantor Services helps scientific organizations solve complex challenges, resulting in improved productivity, increased efficiency, and accelerated innovation.