

# When to use Azure Sphere

5 minutes

In this section, we'll discuss how you can decide whether Azure Sphere is the right product for securing your IoT devices end to end. We'll list some criteria that indicate whether Azure Sphere will meet IoT Security and Analytics requirements. You should consider using Azure Sphere for IoT solutions based on the following criteria.

## Security

Provision of End-to-End security at a low cost is the primary goal of the Azure Sphere platform. Specifically, Azure Sphere targets restricted, price sensitive microcontroller units that are connected to the Internet. If you're connected microcontroller devices, then Azure Sphere is the ideal choice to provide end-to-end security. The Azure Sphere platform is designed around the [seven properties of highly secured devices](#) . This design ensures that your products are secured in a holistic way.

## Productivity

The next consideration is Productivity. Once data is captured over secured and authenticated connections in the field, it can be used to detect anomalies from individual devices. Based on the insights from operational data, you can identify devices where maintenance is needed.

## Opportunity

The final consideration is Opportunity. Support and Engineering personnel can visualize the data and run analytics on it to understand long-term trends.

We can apply these considerations to the scenario above. Azure Sphere provides security to both new and legacy solar panels in the field. If the solar panels are damaged, the condition is reported to the support team who can undertake measures to fix it. By analyzing all the data from the devices over a period of time, the engineering team can plan new products and services for the future.

---

## Next unit: Knowledge check

Continue >

---