100 XP

How Azure Sphere works

6 minutes

The three components of the Azure Sphere platform work together to provide end-to-end security for an IoT solution.

The hardware architecture provides a secured computing as a device level

The software architecture enables you to provide a secure solution allowing you to focus your efforts on value-added features.

The Azure Sphere Security Service supports authentication, software update, and failure reporting.

Also, Azure Sphere also includes support for legacy IoT devices through **Guardian modules.** Guardian Modules are implemented as a hardware solution and support connections to the Azure Sphere Security Service for security checks and automated patching. They also connect to Brownfield devices through device-specific protocols.

> **Note**
>
> Brownfield devices are typically legacy IoT devices already deployed in the field but without internet connectivity.

Below we demonstrate how these components interact to address the scenario outlined above.

Azure Sphere Security service: Microsoft releases updates for the Azure Sphere OS through the Azure Sphere Security Service. The product engineering team then releases updates to individual solar panels through the Azure Sphere Security Service.

Support and services: Error reporting data is captured from the solar panels. If the solar panels are damaged or need cleaning, this information is captured from the sensors on the panel and relayed back to support services group.

Product Engineering: The product engineering team receives data from solar panels in the field that they can visualize. The data can be used to improve the solution or create new solutions

Support for legacy devices: Many of the solar panels in the field are old and not connected to the Internet. The use of Guardian modules helps to connect these panels and capture data from them.

Next unit: When to use Azure Sphere

Continue >