¿Qué es Azure Sphere?

Artículo • 02/12/2022 • Tiempo de lectura: 15 minutos

Azure Sphere es una plataforma segura de aplicaciones de alto nivel con características de seguridad y comunicación integradas para dispositivos conectados a Internet. Incluye una unidad de microcontrolador (MCU) segura, conectada y conectada, un sistema operativo personalizado basado en Linux y un servicio de seguridad basado en la nube que proporciona seguridad continua y renovable.

Azure Sphere MCU integra capacidades de procesamiento en tiempo real con la capacidad de ejecutar un sistema operativo de alto nivel. Un MCU Azure Sphere, junto con su sistema operativo y plataforma de aplicaciones, permite la creación de dispositivos protegidos conectados a Internet que pueden actualizarse, controlarse, supervisarse y mantenerse de forma remota. Un dispositivo conectado que incluye un MCU azure Sphere, ya sea junto o en lugar de un MCU existente, proporciona mayor seguridad, productividad y oportunidad. Por ejemplo:

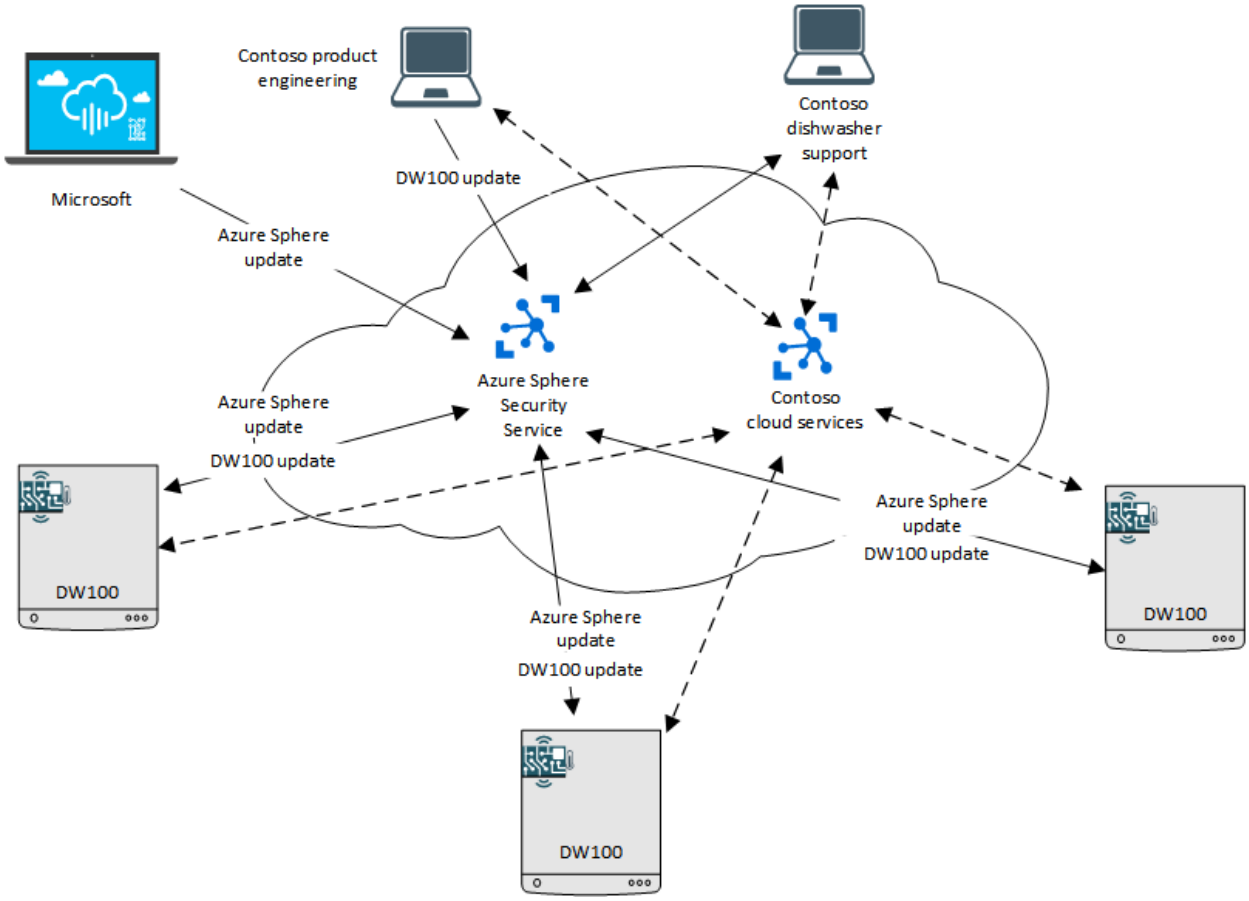
- Un entorno de aplicaciones seguras, conexiones autenticadas y uso opt-in de periféricos minimiza los riesgos de seguridad debido a suplantación de identidad, software fraudulento o ataques de denegación de servicio, entre otros.
- Las actualizaciones de software se pueden implementar automáticamente desde la nube en cualquier dispositivo conectado para solucionar problemas, proporcionar nuevas funciones o contrarrestar los métodos emergentes de ataque, lo que mejora la productividad del personal de soporte técnico.
- Los datos de uso de productos se pueden notificar a la nube a través de una conexión segura para ayudar a diagnosticar problemas y diseñar nuevos productos, lo que aumenta la oportunidad de servicio de productos, interacciones positivas del cliente y desarrollo futuro.

Azure Sphere Security Service es un aspecto integral de Azure Sphere. Con este servicio, los MCU de Azure Sphere se conectan de forma segura a la nube y a la web. El servicio garantiza que el dispositivo arranque solo con una versión autorizada de software original aprobado. Además, proporciona un canal seguro a través del cual los Microsoft pueden descargar e instalar automáticamente actualizaciones del sistema operativo en dispositivos implementados en el campo para mitigar problemas de seguridad. No se requiere intervención del fabricante ni del usuario final, por lo que se cierra un agujero de seguridad común.

Escenario Azure Sphere

Para comprender cómo funciona Azure Sphere en una configuración del mundo real, considere este escenario.

Contoso, Ltd., es un fabricante de productos de productos blancos que inserta un MCU Azure Sphere en sus lavavajillas. El lavavajillas DW100 acopla el MCU con varios sensores y una aplicación de alto nivel que se ejecuta en la MCU Azure Sphere. La aplicación se comunica con el Servicio de seguridad Azure Sphere y con los servicios en la nube de Contoso. El siguiente diagrama ilustra este escenario:



los lavavajillas conectados a la red contoso del inquilino en la nube del fabricante

Empezando desde la parte superior izquierda y moviéndose en el sentido de las agujas del reloj:

- Microsoft publica actualizaciones para el SO Azure Sphere a través del Servicio de seguridad de Azure Sphere.
- La ingeniería de productos de Contoso publica actualizaciones en su aplicación DW100 a través del Servicio de seguridad azure Sphere.
- El servicio de seguridad Azure Sphere implementa de forma segura el sistema operativo actualizado y el software de aplicación Contoso DW100 en los lavavajillas de las ubicaciones del usuario final.

- El soporte para lavavajillas de Contoso se comunica con el Servicio de seguridad de Azure Sphere para determinar qué versión del software Azure Sphere y el software de la aplicación DW100 deben ejecutarse en cada dispositivo de usuario final y para recoger los datos de informes de errores que se han notificado al servicio. La compatibilidad con lavavajillas de Contoso también se comunica con el servicio en la nube de Contoso para obtener información adicional.

- Los servicios en la nube de Contoso admiten aplicaciones de solución de problemas, análisis de datos e interacción con los clientes. Los servicios en la nube de Contoso pueden hospedarse en Microsoft Azure, en el servicio en la nube de otro proveedor o en la propia nube de Contoso.

- Los modelos DW100 de Contoso en las ubicaciones del usuario final descargan software de aplicación y sistema operativo actualizado a través de su conexión al Servicio de Seguridad de Azure Sphere. También pueden comunicarse con la aplicación de servicio en la nube de Contoso para informar de datos adicionales.

Por ejemplo, los sensores del lavavajillas pueden supervisar la temperatura del agua, la temperatura de secado y el nivel del agente de enjuague y cargar estos datos en los servicios en la nube de Contoso, donde una aplicación de servicio en la nube los analiza en busca de posibles problemas. Si la temperatura de secado parece inusualmente caliente o fría ,lo que podría indicar una parte que falla, Contoso ejecuta diagnósticos remotamente y notifica al cliente que las reparaciones son necesarias. Si el lavavajillas está bajo garantía, la aplicación de servicio en la nube también podría asegurarse de que el taller de reparación local del cliente tiene la parte de reemplazo, lo que reduce las visitas de mantenimiento y los requisitos de inventario. Del mismo modo, si el agente de enjuague es bajo, el lavavajillas podría indicar al cliente que compre más enjuagado directamente al fabricante.

Todas las comunicaciones tienen lugar a través de conexiones protegidas y autenticadas. El personal de soporte técnico e ingeniería de Contoso puede visualizar los datos mediante el servicio Azure Sphere Security, las características de Microsoft Azure o una aplicación de servicio en la nube específica de Contoso. Contoso también puede proporcionar aplicaciones web y móviles orientadas a clientes, con las que los propietarios de lavavajillas pueden solicitar servicio, supervisar el uso de recursos de lavavajillas o interactuar con la empresa.

Con las herramientas de implementación de Azure Sphere, Contoso se centra en cada actualización de software de aplicación al modelo de lavavajillas adecuado y el Servicio de seguridad de Azure Sphere distribuye las actualizaciones de software a los dispositivos correctos. Solo se pueden instalar actualizaciones de software firmadas y verificadas en los lavavajillas.

Azure Sphere y las siete propiedades de dispositivos altamente protegidos

Un objetivo principal de la plataforma Azure Sphere es proporcionar seguridad de alto valor a un bajo costo, para que los dispositivos con tecnología de microcontrolador sensibles a precios puedan conectarse a Internet de forma segura y confiable. A medida que los juguetes conectados a la red, los dispositivos y otros dispositivos de consumo se vuelven comunes, la seguridad es de suma importancia. No solo debe protegerse el hardware del dispositivo, sino que también debe protegerse su software y sus conexiones en la nube. Un fallo de seguridad en cualquier lugar del entorno operativo pone en peligro todo el producto y, potencialmente, cualquier cosa o cualquier persona cercana.

Basándose en Microsoft décadas de experiencia con la seguridad de Internet, el equipo de Azure Sphere ha identificado siete propiedades de dispositivos altamente protegidos. La plataforma Azure Sphere se ha diseñado en torno a estas siete propiedades:

Raíz de confianza basada en hardware. Una raíz de confianza basada en hardware garantiza que el dispositivo y su identidad no se puedan separar, lo que evita la falsificación o suplantación de identidad del dispositivo. Cada MCU de Azure Sphere se identifica mediante una clave criptográfica imprevisible generada y protegida por el hardware del subsistema de seguridad Plutón diseñado Microsoft. Esto garantiza una raíz de confianza segura y resistente a alteraciones de fábrica para el usuario final.

Defensa en profundidad. Defensa en profundidad proporciona múltiples capas de seguridad y, por lo tanto, múltiples mitigaciones contra cada amenaza. Cada capa de software de la plataforma Azure Sphere comprueba que la capa superior está protegida.

Pequeña base informática de confianza. La mayor parte del software del dispositivo permanece fuera de la base informática de confianza, lo que reduce el área de superficie para ataques. Solo el Monitor de seguridad seguro, el tiempo de ejecución de Plutón y el subsistema de Plutón,todos los cuales proporciona Microsoft, se ejecutan en la base de computación de confianza.

Compartimentos dinámicos. Los compartimentos dinámicos limitan el alcance de un solo error. Los MCU de Azure Sphere contienen contadores de placas, incluidos firewalls de hardware, para evitar que una infracción de seguridad de un componente se propague a otros componentes. Un entorno en tiempo de ejecución "aislado" restringido impide que las aplicaciones dañen el código o los datos protegidos.

Autenticación sin contraseña. El uso de certificados firmados, validados por una clave criptográfica imprevisible, proporciona una autenticación mucho más segura que las contraseñas. La plataforma Azure Sphere requiere que se firme cada elemento de software. Las comunicaciones de dispositivo a nube y nube a dispositivo requieren más autenticación, lo que se consigue con certificados.

Informe de errores. Los errores de software o hardware del dispositivo son típicos de los ataques de seguridad emergentes; errores de dispositivo que constituyen un ataque de denegación de servicio. La comunicación dispositivo a nube proporciona una alerta temprana de posibles errores. Los dispositivos Azure Sphere pueden informar automáticamente de datos operativos y errores a un sistema de análisis basado en la nube, y las actualizaciones y mantenimiento se pueden realizar de forma remota.

Seguridad renovable. El software del dispositivo se actualiza automáticamente para corregir vulnerabilidades conocidas o infracciones de seguridad, sin que sea necesaria la intervención del fabricante del producto ni del usuario final. El Servicio de seguridad de Azure Sphere actualiza automáticamente el sistema operativo Azure Sphere y sus aplicaciones.

Arquitectura Azure Sphere

Al trabajar conjuntamente, el hardware, el software y el servicio de seguridad de Azure Sphere permiten enfoques únicos e integrados para el mantenimiento, el control y la seguridad del dispositivo.

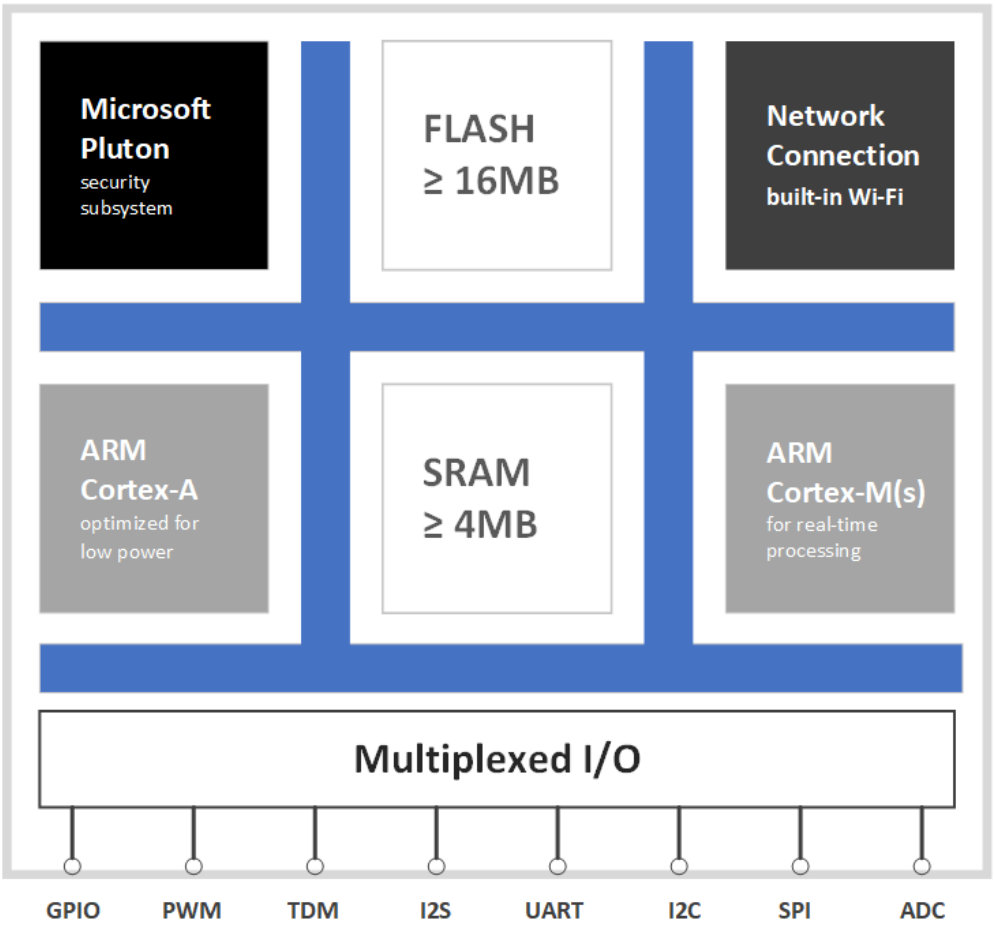
La arquitectura de hardware proporciona una base informática fundamentalmente segura para los dispositivos conectados, lo que le permite centrarse en su producto.

La arquitectura de software, con un kernel de SO personalizado protegido que se ejecuta sobre el monitor de seguridad escrito Microsoft, le permite concentrar sus esfuerzos de software en características específicas del dispositivo y ioT de valor añadido.

El servicio de seguridad Azure Sphere admite autenticación, actualizaciones de software e informes de errores a través de canales seguros de nube a dispositivo y de dispositivo a nube. El resultado es una infraestructura de comunicaciones segura que garantiza que sus productos ejecuten el sistema operativo Azure Sphere más actualizado. Para obtener diagramas de arquitectura y ejemplos de arquitecturas de nube, consulte Examinar arquitecturas de Azure.

Arquitectura de hardware

Una MCU cruzada azure Sphere consiste en varios núcleos en un solo troquel, como se muestra en la figura siguiente.



hardware de Azure Sphere MCU

Cada núcleo, y su subsistema asociado, está en un dominio de confianza diferente. La raíz de la confianza reside en el subsistema de seguridad plutón. Cada capa de la arquitectura supone que la capa superior puede estar comprometida. Dentro de cada capa, el aislamiento de recursos y los compartimentos dinámicos proporcionan mayor seguridad.

Microsoft subsistema de seguridad de Plutón

El subsistema de seguridad de Plutón es la raíz segura de confianza de Azure Sphere basada en hardware (en silicon). Incluye un núcleo de procesador de seguridad, motores criptográficos, un generador de números aleatorios de hardware, generación de claves públicas/privadas, cifrado asimétrico y simétrico, compatibilidad con la verificación del algoritmo de firma digital de curva elíptica (ECDSA) para arranque seguro y arranque medido en placas de silicon para admitir la atestación remota con un servicio en la nube, así como varias medidas contra alteraciones, incluida una unidad de detección de entropía.

Como parte del proceso de arranque seguro, el subsistema de Plutón arranca varios componentes de software. También proporciona servicios de tiempo de ejecución, procesa solicitudes de otros componentes del dispositivo y administra componentes críticos para otras partes del dispositivo.

Núcleo de aplicación de alto nivel

El núcleo de aplicación de alto nivel cuenta con un subsistema ARM Cortex-A que tiene una unidad de gestión de memoria completa (MMU). Permite la compartición basada en hardware de los procesos mediante el uso de la funcionalidad de zona de confianza y es responsable de ejecutar el sistema operativo, las aplicaciones de alto nivel y los servicios. Soporta dos entornos operativos: Normal World (NW), que ejecuta el código en modo de usuario y modo supervisor, y Secure World (SW), que ejecuta solamente el monitor de seguridad suministrado por Microsoft. Sus aplicaciones de alto nivel se ejecutan en modo de usuario NW.

Núcleos en tiempo real

Los núcleos en tiempo real incluyen un subsistema de E/S cortex-M ARM que puede ejecutar aplicaciones compatibles en tiempo real como código bare-metal o un sistema operativo en tiempo real (RTOS). Estas aplicaciones pueden asignar periféricos y comunicarse con aplicaciones de alto nivel, pero no pueden acceder a Internet directamente.

Conectividad y comunicaciones

El primer MCU Azure Sphere proporciona una radio de 802,11 b/g/n Wi-Fi que funciona tanto a 2,4 GHz como a 5 GHz. Las aplicaciones de alto nivel pueden configurar, usar y consultar el subsistema de comunicaciones inalámbricas, pero no pueden programarlo directamente. Además de o en lugar de usar Wi-Fi, los dispositivos Azure Sphere que están correctamente equipados pueden comunicarse en una red Ethernet.

E/S multiplexada

La plataforma Azure Sphere admite una variedad de capacidades de E/S, para que pueda configurar dispositivos incrustados para satisfacer los requisitos del mercado y del producto. Los periféricos de E/S se pueden asignar al núcleo de aplicaciones de alto nivel o a un núcleo en tiempo real.

firewalls de Microsoft

Los firewalls de hardware son contramedidas de placas que proporcionan protección de "espacio aislado" para garantizar que los periféricos de E/S sean accesibles solo al núcleo al que se asignan. Los firewalls imponen compartimentación, lo que impide que una amenaza de seguridad localizada en el núcleo de aplicación de alto nivel afecte al acceso de los núcleos en tiempo real a sus periféricos.

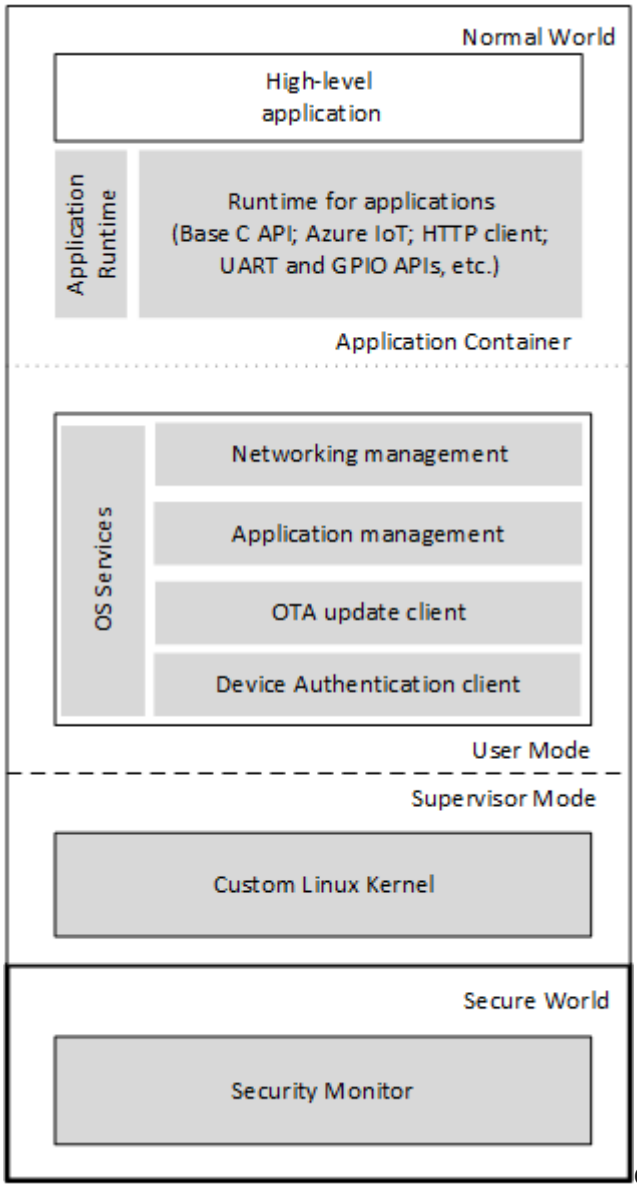
MEMORIA RAM integrada y flash

Los MU Azure Sphere incluyen un mínimo de 4 MB de RAM integrada y 16 MB de memoria flash integrada.

Arquitectura de software y sistema operativo

La plataforma de aplicación de alto nivel ejecuta Azure Sphere OS junto con una aplicación de alto nivel específica del dispositivo que puede comunicarse tanto con Internet como con aplicaciones compatibles con tiempo real que se ejecutan en los núcleos en tiempo real. La figura siguiente muestra los elementos de esta plataforma.

Microsoft elementos suministrados se muestran en gris.



de aplicaciones de alto nivel de plataforma de aplicaciones

Microsoft proporciona y mantiene todo el software excepto las aplicaciones específicas del dispositivo. Todo el software que se ejecuta en el dispositivo, incluida la aplicación de alto nivel, está firmado por la Microsoft entidad emisora de certificados (CA). Las actualizaciones de aplicaciones se entregan a través de la canalización de Microsoft de confianza y se comprueba la compatibilidad de cada actualización con el hardware del dispositivo Azure Sphere antes de la instalación.

Tiempo de ejecución de aplicaciones

El tiempo de ejecución de la aplicación proporcionado por Microsoft se basa en un subconjunto del estándar POSIX. Se compone de bibliotecas y servicios de tiempo de ejecución que se ejecutan en modo de usuario NW. Este entorno es compatible con las aplicaciones de alto nivel que se crean.

Las bibliotecas de aplicaciones admiten funciones de redes, almacenamiento y comunicaciones necesarias para aplicaciones de alto nivel, pero que no admiten el

acceso directo de E/S de archivo genérico o shell, entre otras restricciones. Estas restricciones garantizan que la plataforma permanezca protegida y que Microsoft pueda proporcionar actualizaciones de seguridad y mantenimiento. Además, las bibliotecas restringidas proporcionan una superficie de API estable a largo plazo para que el software del sistema se pueda actualizar para mejorar la seguridad y mantener la compatibilidad binaria para aplicaciones.

Servicios del sistema operativo

Los servicios del sistema operativo hospedan el contenedor de aplicaciones de alto nivel y son responsables de la comunicación con el Servicio de seguridad de Azure Sphere. Administran la autenticación de red y el firewall de red para todo el tráfico saliente. Durante el desarrollo, los servicios del sistema operativo también se comunican con un equipo conectado y con la aplicación que se va a depurar.

Kernel de Linux personalizado

El kernel personalizado basado en Linux se ejecuta en modo supervisor, junto con un cargador de arranque. El kernel se ajusta cuidadosamente para la huella de flash y RAM de la MCU Azure Sphere. Proporciona una superficie para la ejecución preventiva de procesos de espacio de usuario en espacios de direcciones virtuales independientes. El modelo de controlador expone periféricos MCU a aplicaciones y servicios del sistema operativo. Los controladores de Azure Sphere incluyen Wi-Fi (que incluye una pila de redes TCP/IP), UART, SPI, I2C y GPIO, entre otros.

Monitor de seguridad

El monitor de seguridad suministrado por Microsoft se ejecuta en SW. Es responsable de proteger el hardware sensible a la seguridad, como memoria, flash y otros recursos de MCU compartidos, y de exponer de forma segura el acceso limitado a estos recursos. Los agentes de Seguridad Monitor y puertas de acceso al subsistema de seguridad de Plutón y la raíz hardware de confianza y actúan como un perro de vigilancia para el entorno NW. Inicia el cargador de arranque, expone los servicios en tiempo de ejecución a NW y administra los firewalls de hardware y otros componentes de placa de seguridad que no son accesibles a NW.

Servicio de seguridad Azure Sphere

El Servicio de seguridad Azure Sphere consta de tres componentes: autenticación, actualización e informes de errores sin contraseña.

- **Autenticación sin contraseña.** El componente de autenticación proporciona atestación remota y autenticación sin contraseña. El servicio de atestación remota se conecta a través de un protocolo de respuesta de desafío que utiliza la función de arranque medida en el subsistema de Plutón. Comprueba no sólo que el dispositivo arrancado con el software correcto, sino con la versión correcta de ese software.

  Después de que la atestación tenga éxito, el servicio de autenticación se hace cargo. El servicio de autenticación se comunica a través de una conexión TLS segura y emite un certificado que el dispositivo puede presentar a un servicio web, como Microsoft Azure o la nube privada de una empresa. El servicio web valida la cadena de certificados, verificando así que el dispositivo sea original, que su software esté actualizado y que Microsoft sea su origen. A continuación, el dispositivo puede conectarse de forma segura con el servicio en línea.

- **Actualizar.** El servicio de actualización distribuye las actualizaciones automáticas para Azure Sphere OS y para las aplicaciones. El servicio de actualización garantiza el funcionamiento continuo y habilita el mantenimiento remoto y la actualización del software de la aplicación.

- **Informe de errores**. El servicio de informes de errores proporciona informes de bloqueos sencillos para el software implementado. Para obtener datos más completos, use las características de informes y análisis que se incluyen con una suscripción de Microsoft Azure.

Todos los datos almacenados con el Servicio azure Sphere Security se cifran en reposo de forma predeterminada. El servicio de seguridad almacena datos en Azure Storage, Azure Cosmos DB y Azure Key Vault, con el cifrado de datos en reposo para cada servicio.