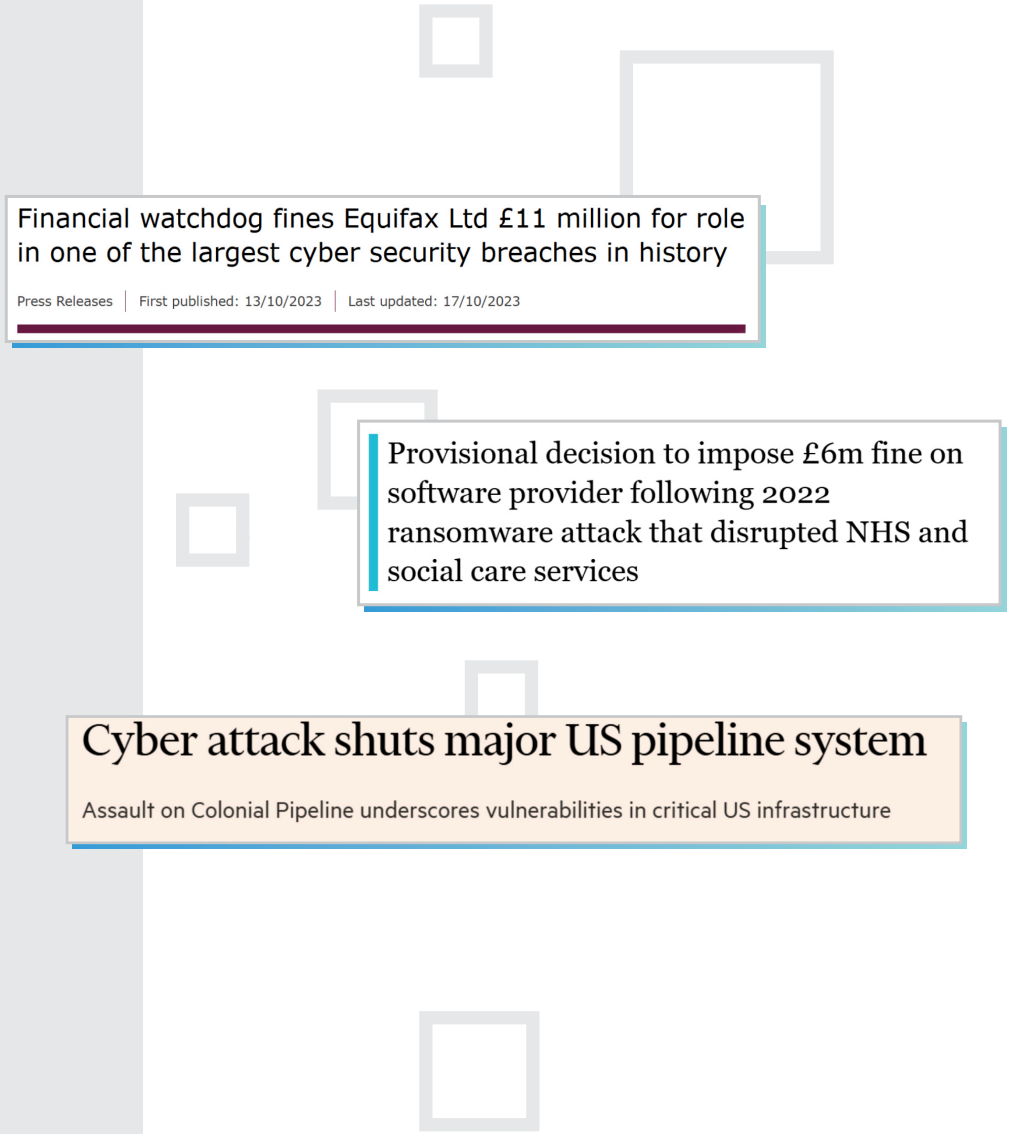
Raspberry Pi

Secure embedded computing with Raspberry Pi

The right choice for your secure embedded computing needs

In the world of embedded computing, security is paramount. Choosing a platform that can guarantee the integrity and confidentiality of your data is crucial, especially in an increasingly interconnected world.

Raspberry Pi single-board computers and modules offer a combination of security features, performance, and affordability. Raspberry Pi computers continue to be used in industrial and critical infrastructure projects around the world, securely enabling the growth of Edge IoT.



Key takeaways

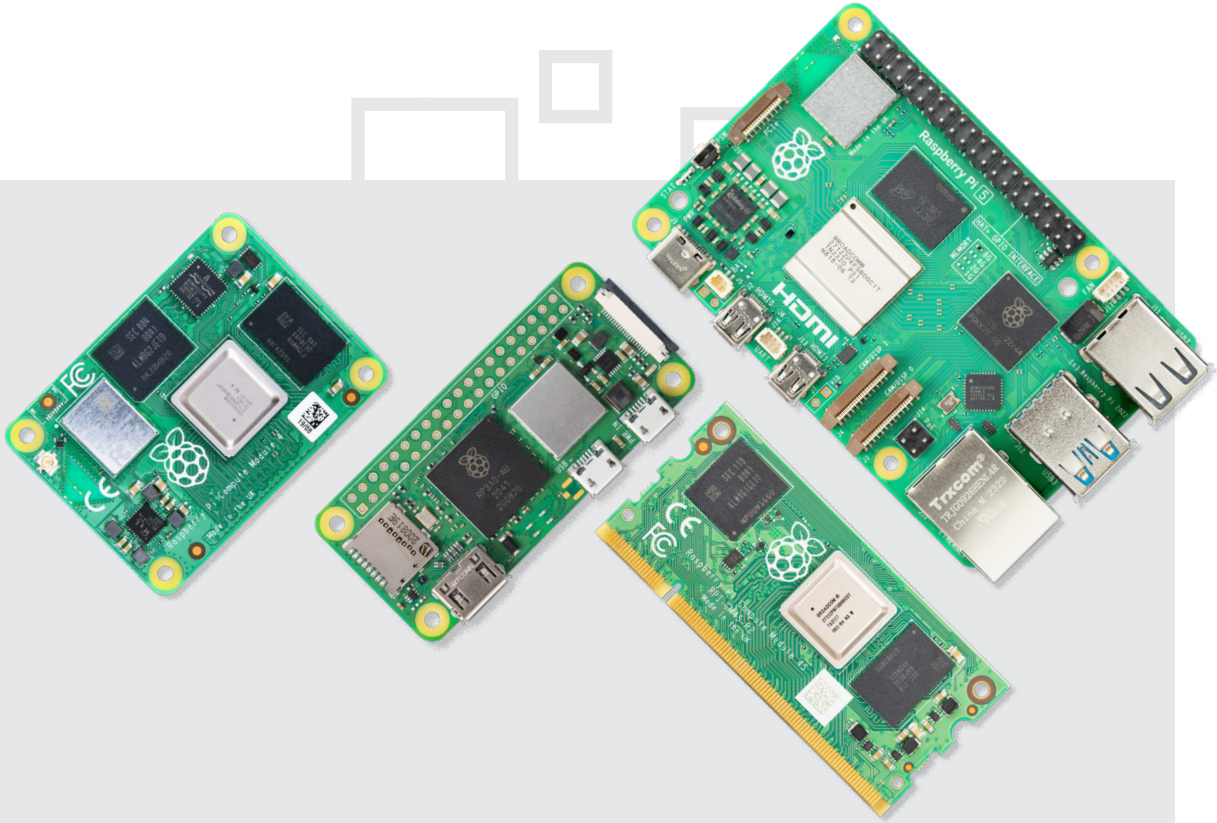
First embedded compute platform designed to be fully compliant to the EU's strict **ETSI EN 303 645 and EN 18031 cybersecurity standards,** with documentation and support for establishing levels of cybersecurity assurance, as defined by ISO 14508.

Designed and manufactured in the UK; the Country of Origin protects developers from potential trade and tariff instabilities.

Continuous, **free OS software support for all products,** supported by a dedicated in-house software engineering team.

Long-term lifetime commitments for products up to 2045, with OS backwards compatibility across all devices; products continue to benefit from security updates.

Hardware security features, including secure boot, full disk encryption on compute platforms, and Arm TrustZone on microcontrollers — **a robust set of tools enabling design engineers to address threats to IoT applications.**



Secure boot and encryption: building a chain of trust

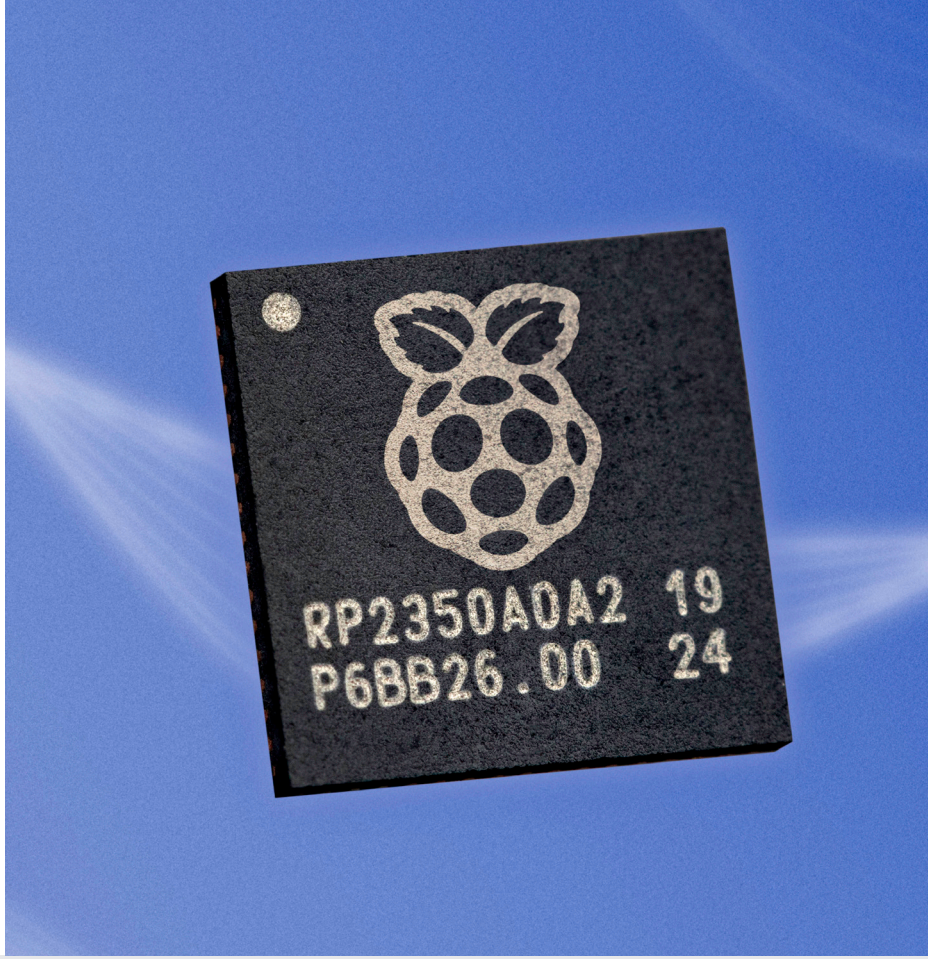
Signed boot ensures that only trusted software is executed when the device powers on, preventing malicious code from compromising the system. Raspberry Pi devices offer secure boot functionality, allowing you to cryptographically verify the authenticity of the bootloader and operating system. This mitigates the risk of unauthorised software manipulation and safeguards your device from boot-level attacks.

Raspberry Pi also supports full disk encryption, adding another layer of protection to your commercially sensitive data. By encrypting the entire filesystem, you ensure that the data remains inaccessible without the correct decryption keys — even if the device is physically compromised. This is particularly important in applications where data confidentiality is critical, such as industrial control systems, healthcare devices, and financial terminals.

These features enable Raspberry Pi products to meet the requirements of international cybersecurity standards, providing secure storage of sensitive security parameters, protection of personal data, secure communication, and best-practice encryption; Raspberry Pi ensures the integrity of the integrators' software and the security of their users' data.

Raspberry Pi microcontrollers

Raspberry Pi's new range of MCUs provide sophisticated security technologies, making them perfect for IoT applications. System designers have a duty to protect users' personal data, provide secure methods of data transmission, and ensure OTA updates can be conducted with confidence. RP2350 puts a tranche of security-focused tools at the fingertips of design engineers to achieve these goals.



Hardware-enabled protection: TrustZone and advanced security features

RP2350 arm TRUSTZONE

The RP2350 series of microcontrollers incorporates Arm's TrustZone technology. TrustZone creates a hardware-isolated secure world within the processor, separating security-critical operations from the main operating system. This isolation ensures that, even if the main OS is compromised, sensitive information and critical functions remain protected within the secure world. Side-channel attacks are mitigated through application code encryption and reference decryption software. This architecture is ideal for applications requiring secure key storage, secure firmware updates, and protection against runtime attacks. Later this year, Arm will deliver a PSA Certified Level 2 TF-M port to RP2350.

Intellectual Property

Security coprocessor (patent pending)
The redundancy coprocessor (RCP) is used in the RP2350 boot ROM to provide hardware-assisted mitigation against fault injection and return-oriented programming attacks.

Hardware random number generator
Generating truly random numbers is essential for cryptographic operations. Raspberry Pi computers include a dedicated hardware random number generator, providing a reliable source of entropy for secure key generation and other security-sensitive tasks.

Secure OTP (one-time programmable) memory This provides a secure, tamper-proof area for storing sensitive information like cryptographic keys or device-specific configurations. Once programmed, the data in OTP memory cannot be modified, ensuring its integrity.

Glitch detector
This hardware mechanism detects abnormal voltage fluctuations or clock glitches that could indicate an attempt to tamper with the device or inject malicious code. The glitch detector can trigger countermeasures to protect the system's integrity in such events.

Manufactured in the UK

A secure and stable supply chain

Geopolitical uncertainties and supply chain vulnerabilities mean the origin of your hardware matters. Raspberry Pi devices are manufactured in the UK, ensuring a stable and secure supply chain.

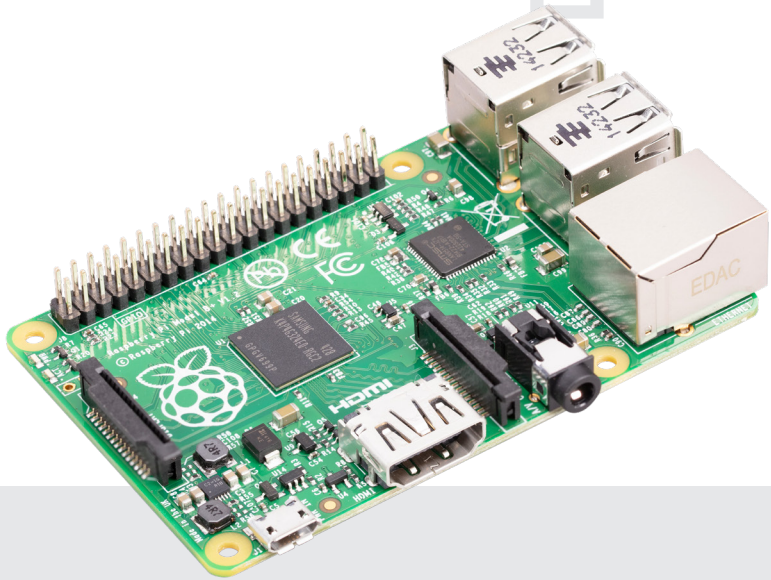
This minimises the risk of disruptions due to trade wars, tariffs, or political instability. Choosing Raspberry Pi means you can rely on a consistent supply of high-quality hardware, free from potential security concerns associated with manufacturing in certain regions.

Long product lifetimes

Raspberry Pi offers extended product lifetimes, ensuring that your devices remain supported with software updates and security patches for years to come. This long-term commitment provides peace of mind, and allows you to focus on your application development without worrying about frequent hardware upgrades or end-of-life issues.

Stable and updated software

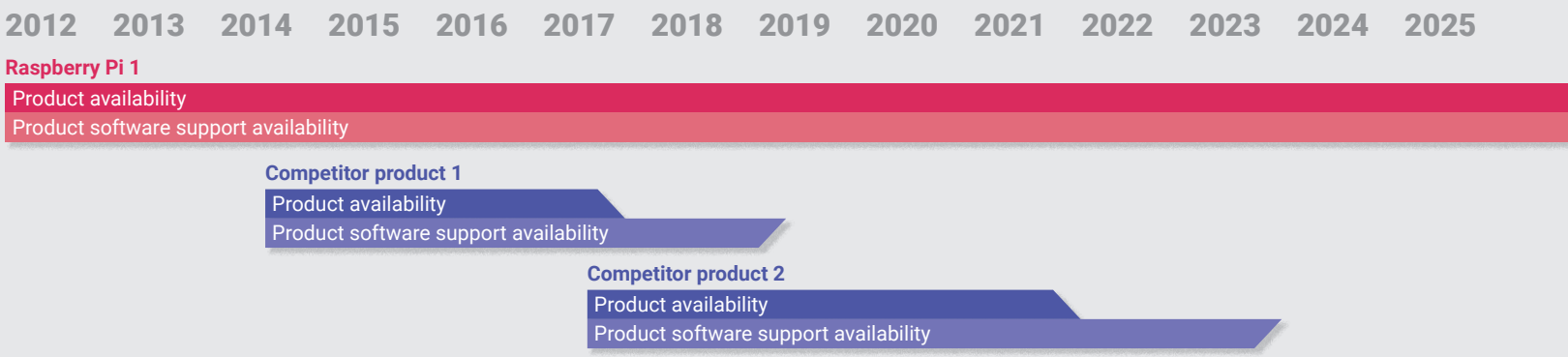
A secure embedded system relies on stable and regularly updated software; support for software update is an integral part of establishing cybersecurity compliance. Products based on the combination of Raspberry Pi hardware and software benefit from our commitment to update across all platforms.



Raspberry Pi 1 was launched in 2012, and is still supported in the latest Raspberry Pi OS release.

Software support is frequently cited as a reason why our OEM customers select Raspberry Pi over the competition

Long-term software support, alongside **long-term availability** of hardware, reduces treadmill costs for OEMs



Certification

EN 303 645 V2.1.1
Raspberry Pi is leading the way in embedded platform security. Its latest fourth- and fifth-generation compute platforms are some of the first to be fully compliant to the EU's strict cybersecurity standards (ETSI EN 303 645), ensuring enhanced security and privacy for users. This proactive approach puts Raspberry Pi ahead of the 2025 RED cybersecurity certification deadline, setting a new standard for the industry.

EN 18031
Though this standard has yet to be harmonised under the RED cybersecurity requirements, Raspberry Pi can already demonstrate proof-of-concept compliance with the new essential requirements for secure network connection, protection of personal data and privacy, and features to protect against fraud. Raspberry Pi supports module integrators in the use of its products in systems that require these protections to be demonstrated, creating an easy-to-integrate modular ecosystem.

Common Criteria ISO/IEC 15408
Through documentation, expertise, and technical features, Raspberry Pi ensures all its customers are able to comply with their cybersecurity requirements. This includes the assessment of systems under the Common Criteria defined by ISO/IEC 15408. Raspberry Pi is able to guide and inform customers who use its products as components in systems that have a target Evaluation Assurance Level (EAL), and provide documentation to prove their resilience to cybersecurity vulnerabilities.

UK Cybersecurity Act
In meeting the requirements of ESTI EN 303 645, Raspberry Pi is able to demonstrate full compliance with the Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023, the first regulation implemented under the Product Security and Telecommunications Infrastructure Act.

Raspberry Pi devices offer a combination of security features, high performance, and affordability, making them the right choice for secured embedded computing. Their secure boot functionality, encryption capabilities, TrustZone technology, and other hardware-enabled security features provide a robust foundation for protecting sensitive data and critical operations in deployed systems.

The familiar combination of software and hardware widely used and understood by engineers makes Raspberry Pi an ideal platform for developing and deploying secure embedded solutions. This familiarity reduces development time, simplifies integration, and ensures a robust and reliable security posture for critical applications.

Get in touch
industry@raspberrypi.com