intertrust®

Data Sheet

Platform

XPN™
Edge-to-cloud security for IoT devices

Intertrust Explicit Private Networking (XPN) provides end-to-end security for data at rest and data in transit—from the device to cloud and back. Your data is always protected and processed in a tamper-resistant, secure execution environment, with Intertrust XPN.

Persistent trust for IoT devices

Intertrust XPN gives you end-to-end, persistent and consistent trust and security for IoT devices and data, across zero- and full-trust environments, with a complete chain of trust.

Access a single pane of glass solution for trust and protection of IoT devices, data, and their operations, all within a secure data platform for mission critical data-driven applications.

Also preserve an auditable chain of trust for IoT data to demonstrate the provenance and veracity of IoT data across your device ecosystem. Prove that data transmission and authentication have not been altered for documenting trusted business transactions, regulatory requirements, or other record of governance operations.

Protect complex data operations and devices

Gaps in network security, incompatible key management systems, or competing data systems, can all put your devices at risk. Intertrust XPN eliminates the trust gaps, wherever devices and data are at risk, whether the data is at rest; unprotected on devices or in the cloud.

Transform diverse, existing IT infrastructure into a secure interoperable system that turns “zero trust” networks into “full trust” environments.

Make competing data operations systems and IoT devices work in secure, predictable, and controlled fashion.

Meet NIST 8259A baseline standards

The new NIST 8259A standard for IoT devices outlines numerous core security requirements. Device manufacturers can use XPN to meet many of these, including:

- **Device identification.** Ensure sensitive processing in IoT devices only occurs in secure environments
- **Device configuration.** Demonstrate that software on the device has not been changed in an unauthorized manner
- **Data protection.** Encrypt data and establish that it has not been tampered with after it was transmitted from the device
- **Logical access to interfaces.** Prevent unprotected network connections to vulnerable legacy devices
- **Software updates.** Protect software and underlying hardware during device software updates
- **Cybersecurity state awareness.** Indicate to applications and networks that attached devices are secure.

Features

Persistent data protection

Ensure that sensitive processing in IoT devices only occurs in secure environments. Data packages are digitally signed and optionally encrypted before they are transmitted. When received on the server side, the data is verified to assure its integrity and, upon confirmation, routed to its final destination, or processed in the Intertrust Platform's protected processing environment.

Entity attestation tokens

When an IoT device is introduced to an application, XPN issues a standards-compliant token attesting that the device posture can be trusted. The token is verified by Intertrust Platform to verify its trust state. The application can then determine to trust the device and data it transmits. It communicates this trust state to applications built on Intertrust Platform.

Enhanced auditing

Gain extensive auditing as part of its data governance capabilities of the Intertrust Platform. XPN expands this by adding information on IoT data used in transactions to the audit. This information can include timestamps and contextual metadata to prove provenance of data and protect against deep fakes. It also offers attestations on device and data integrity to provide further assurance of data trustworthiness. Organizations can use these enhanced audits for business, operations, and regulatory purposes.

Digital twin and firewall for legacy systems

Older connected devices, such as SCADA systems used in industrial applications, have limited or no hardware security capabilities. For these devices, XPN maintains a digital twin of the device. This digital twin acts as a firewall for the device so that any connection requests are first received by the digital twin and only route to the device if they are determined safe.

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035