intertrust®

Intertrust XPN™

Optimize your AI automation from edge to cloud

Intertrust XPN provides end-to-end security for data at rest and data in transit. XPN enables authorized commands from the cloud to the edge device, securely bridging the gap between IT and OT environments.

Industry

Industrial and residential IoT

Product

Intertrust XPN™

Security challenges of industrial and residential IoT networks

In the rapidly evolving landscape of industrial and commercial Internet of Things (IoT), legacy approaches to data security have proven to be fatally flawed. Whether it is the brittle 'eggshell' defense model of air gapping an operational network, or implementing virtual private networks (VPNs) or Transport Layer Security (TLS), they are not up to the task when faced with well-funded threat actors with deep expertise. Decentralization and digitalization trends are creating a unique set of challenges for operational technology (OT) and home IoT networks.

There are several security and operational concerns as data flows between edge devices, gateways, and clouds.

Lack of device authenticity
The rapid growth of connected devices has greatly increased the risk of compromise at the edge. It is necessary to secure large networks of IoT devices and assure the immutable and trusted cryptographic identity.

Untrusted networks
Data generated by sensors at the deep edge and commands traveling to actuators often must traverse untrusted and untrustable networks. Mesh networks, unprotected gateways, and other network components are often unsecured or unsecurable. They often operate beyond an organization's governance. And yet, many use cases in decentralized systems require transmitting sensitive data through these connections.

Regulatory compliance
Evolving regulation on the management and use of data creates increased risk and liability. Protecting personally identifiable information (PII) data persistently wherever it is sent or stored, is critical because privacy legislation such as California's Consumer Protection Act (CCPA) and Europe's General Data Protection Regulation (GDPR) have significant penalties for divulging PII.

Unprotected commands to IoT devices
System automation requires commands to be verified and accepted. Without securely communicating to IoT devices and using proper command authorization, organizations are unable to unify data analytics, prescriptive analytics, industrial automation, and artificial intelligence.

In the rapidly evolving landscape of industrial and commercial IoT, legacy approaches to data security have proven to be fatally flawed.

Zero trust and the deep edge

Today's networked "things" still rely on a secure perimeter in which they are "safe" yet the nature of the perimeter has changed with remote access, overlapping trust models, and governance. Zero trust principles have been widely adopted in the enterprise, particularly the notion of endpoint resilience and protection. Without such an approach, industrial and consumer systems will remain vulnerable to threat actors who can easily breach perimeters, escalate privileges, maintain persistence, and exploit the unprotected interior.

Don't trust that message

There have been many attacks from untrusted or compromised or overtly malicious devices. These attacks will send a malformed message to an unsuspecting recipient device. When it starts parsing the message, it will find an out-of-bounds data element resulting in a buffer overflow and quickly followed by an exploit code to attack and take over the receiving device.

This is a particular problem for IoT systems with many decentralized and automated devices enabling a malicious actor to spread quickly through a network.

IoT devices are often the softest of targets

Typically deployed with minimal or no security controls, maintaining the integrity and authenticity of IoT devices is challenging, as they are often susceptible to simple software-based exploits.

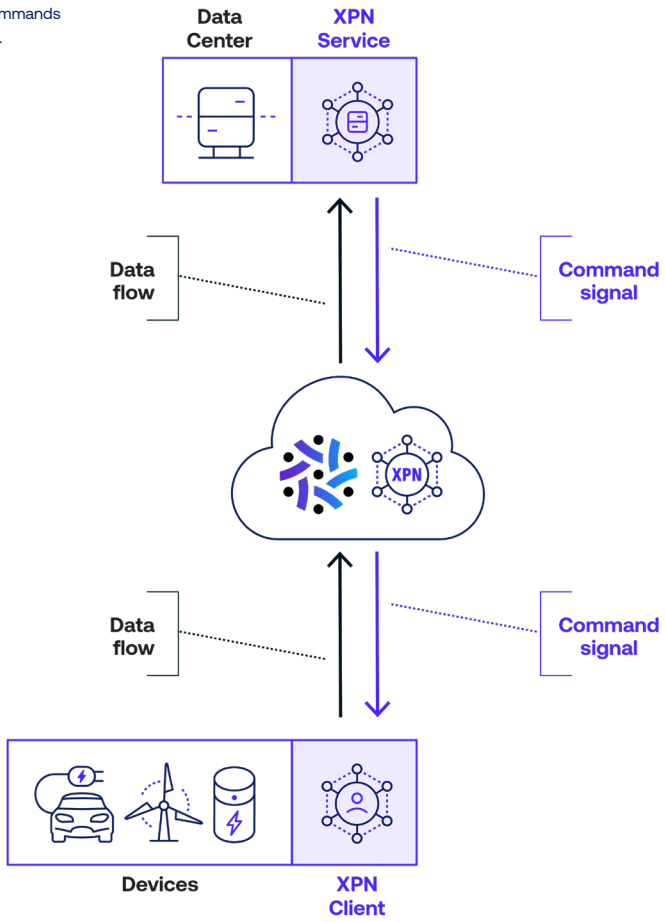
End-to-end trust for the IoT networks

Intertrust XPN (Explicit Private Networking) secures and authenticates the IoT edge devices or gateways in residential and industrial IoT applications. XPN protects data by assuring its authenticity, integrity, and secrecy. It does not rely on network security which can be intrinsically weak, poorly implemented, or insufficiently maintained.

The XPN protocol is an application layer protocol that protects IoT data from generation to consumption, both while in transit across untrusted network segments and at rest within a data store. It provides data integrity by cryptographically signing data at its source.

This signature can later be verified by an authorized recipient to ensure tampering or corruption has not occurred. Data packages can also be encrypted at the source to preserve data privacy, both while in transit and at rest. Lastly, it protects instructions sent from XPN-enabled applications to end devices, ensuring the authority and integrity of commands issued to actuators.

Intertrust XPN authorizes commands to devices at the deep edge.



Typically deployed with minimal or no security controls, maintaining the integrity and authenticity of IoT devices is challenging.

Intertrust XPN components

Intertrust XPN is designed with an architecture that includes three components to ensure secure and efficient operations across various platforms and devices.

XPN client SDK
The XPN Client SDK is a C/C++ source code that has been ported to FreeRTOS, Zephyr, Linux, Windows, MacOS and is easily ported to other packages that are portable to POSIX-compliant operating systems.

It enables the following actions and steps:

- Activation and initialization
- Data signing and encapsulation at the source within a protected processing environment
- Optional data encryption for privacy, if this option is not selected it allows intrusion detection systems to perform deep packet inspection and monitor data flows.

XPN Server
Establishes sessions to XPN devices running applications based on the XPN Client SDK Provides data connectors such as MQTT, HTTP, Kafka, SnowPipe for Snowflake databases, JDBC and APIs to easily store data from XPN Clients

iPKI
Intertrust PKI, or iPKI, is the public key infrastructure that provides the certificate provisioning service. It offers over-the-air certificate signing for field devices or batch generation and provisioning of key pairs.

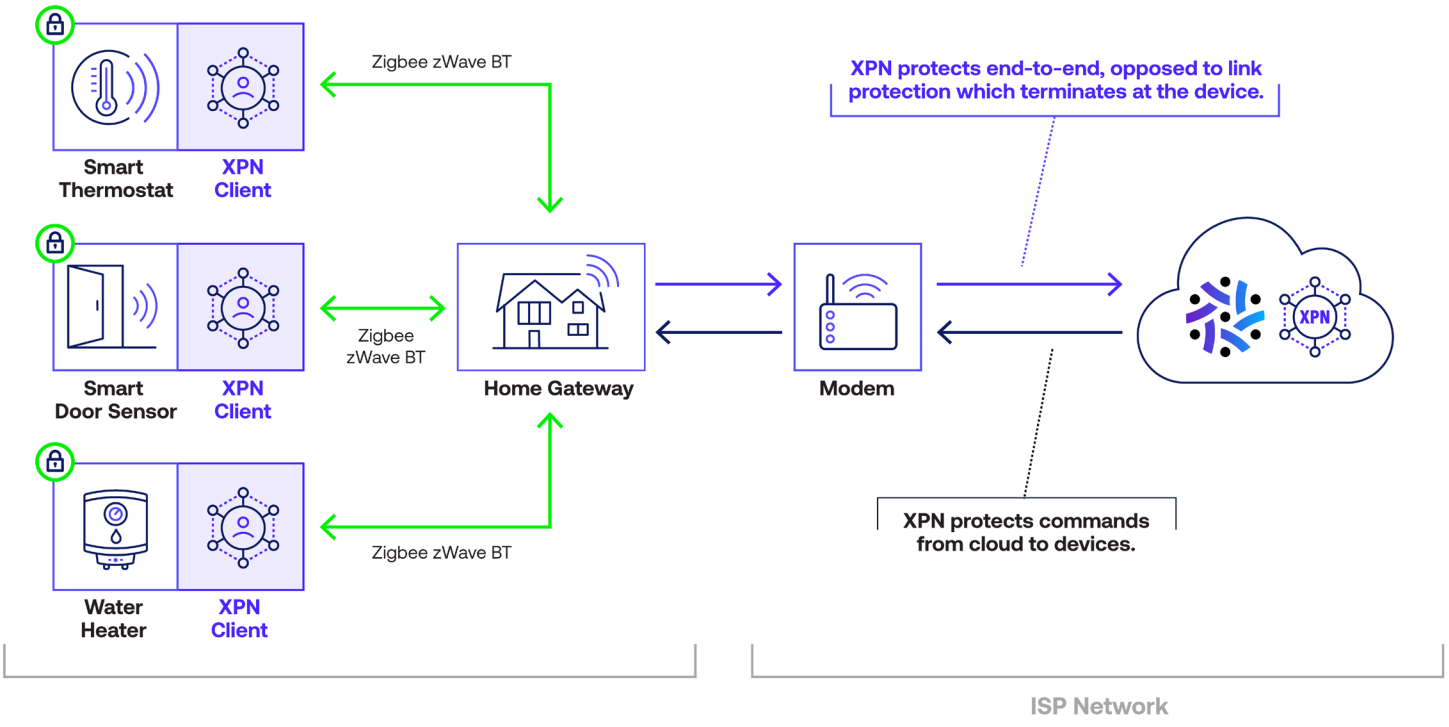
Enhancing security across networks with XPN

Persistent edge-to-cloud protection
To move data from a device to the cloud requires many steps:

- Smart home device (e.g., NEST thermostat or “open door” sensor)
- Local network (home network) using Wi-Fi, Zigbee, or Z-Wave
- Home router or hub
- Modem
- ISP network
- Cloud servers

Each of these steps come with their own link protections. XPN by contrast provides persistent protection throughout all of these links and devices. With XPN, data is protected whether at-rest or in-transit in these often hostile environments. Therefore, trust is maintained from when the device generates the data through its consumption in the cloud.

End-to-end authenticity and integrity with XPN at the application layer



Authorized commands
XPN enables secure control of assets through the authentication of devices, applications, and data streams. It also ensures that commands themselves can be verified and accepted procedurally. The command authorization framework is a key differentiator for XPN that enables secure systems automation.

Bridging across environments
XPN establishes trust between technologies in different environments including IT, OT, and residential IoT with a uniform trust model. In contrast to VPN and TLS protocols which heavily depend on the network stack and how it is implemented, XPN protects the actual data and is not dependent on the network 'pipe'. The data is never left unwrapped or vulnerable to man-in-the-middle attacks, data poisoning, or malicious malware embedding. With XPN, data is truly secure end-to-end independent of any unprotected devices, attackers, or changes in the environment.

Tunneling through insecure protocols
Many protocols, in particular mesh and serial protocols such as Zigbee/AMI and Modbus/SCADA, either implement a limited TCP/IP stack which results in a weak TLS protocol or don't implement it at all. In contrast, XPN establishes secure links through existing industry network standards. XPN has native support for communication protocols including AMI, Bluetooth, Zigbee, and ZWave as well as messaging protocols such as MQTT and HTTP.

PSA certified device support

PSA certification is one of the leading regimes for certifiable trust in IoT devices. It includes three security levels, starting with Level 1, ensuring a security design is reviewed and approved. Level 2 requires pen testing in a lab by an authorized certification company and must pass software-based attacks. Level 3 requires the device to be resilient in the face of hardware- based side channel attacks.

The XPN Client SDK is integrated with the PSA certified API, providing a simple means for a software developer to root their application to the certified hardware implementations of secure boot, secure storage, and secure execution offered in these devices.

Entity Attestation Token

IoT devices face many threats from other devices, so XPN incorporates the IETF RATS EAT protocol: The IETF RATS (Remote Attestation Procedures) Working Group's Entity Attestation Token (EAT) is a standardized format for conveying the security posture of a device. EATs are designed to provide verifiable claims about a device's identity, integrity, and operational state.

These tokens are typically used in IoT environments to ensure that devices can be trusted before they are allowed to communicate with other devices or networks. By providing cryptographic proof of a device's attributes, EATs help mitigate risks such as unauthorized access, tampering, and firmware attacks, thereby enhancing the overall security of the IoT ecosystem.

Strategic impact of XPN vs. residential and industrial controls security

Intertrust XPN delivers a scalable, and end-to-end solution. The below table compares different features of XPN with industrial control systems security solutions.

Feature	Current OT and residential IoT protocols	XPN
Protocol type	Connection-oriented	Message-oriented
Security type	Point-to-point security	End-to-end security
Network context	Works best in unified, single-entity controlled networks.	Applicable to large-scale, distributed networks of networks, such as VPPs and distributed energy generation.
Security & trust model	Legacy protocol with support for systems with minimal security. Leaves security implementation open. No core trust model.	Built for modern, dynamic systems and uncontrolled environments incorporating a robust trust model.
Data storage security	Only encrypts data in transit, not at rest. Leaves intermediate data collector security to implementers.	Provides persistently encrypted data, securing stored data in intermediate systems.
Adaptability to zero-tust environments	Predates zero-trust thinking and is not well-adapted for such environments.	Built from the ground up for dynamic systems and uncontrolled environments, aligning with zero-trust principles.
PKI and authentication	Tightly coupled with PKI and certificate-based security for device authentication.	Supports evolution to more scalable key management systems.
Interoperability & standards complexity	Covers a wide range of topics, leaving many options to implementers, complicating interoperability in systems of systems.	Much simpler, by design. Fewer specific requirements to become and remain compliant.
Approach to system security	Allows insecure profiles, relies on implementations for security. Challenged in securing intermediate data collectors.	Starts with a modern approach to security, inherently designed for dynamic and uncontrolled environments where zero-trust concepts underpin all data transactions and storage.

intertrust®

Building trust for a connected world.

Learn more at: intertrust.com/xpn
Contact us at: energy@intertrust.com
+1 408 616 1600