intertrust®

End-to-end data security in zero-trust environments

Businesses are being reshaped to take advantage of their most valuable asset: information. The cloud, secure devices at the edge, and trusted data management environments are not optional for businesses that seek to maintain a competitive advantage.

To protect information at the core of any operation, the data must be trusted and secure. This is especially true in the modern data supply chain, with distributed devices and disparate data stores operating on premises and in the cloud.

Today, organizations rely more than ever on information for their operations and are under pressure to use their data to reduce operational costs, enhance user experience and make it easier to collaborate with partners and third parties. Data flows from and to edge devices are increasing in their importance, especially for industrial organizations such as utilities and manufacturers. The corresponding rapid growth of connected devices has greatly increased the risk of compromise at the edge. Companies need to secure and authenticate large networks of IoT devices and ensure their identity throughout their lifecycle.

Yet, the inclusion of edge devices greatly increases the difficulty of protecting these data flows since quite often edge devices operate in insecure or zero-trust environments. Data and commands traveling both from and to devices on the edge traverse a series of untrusted networks. This places authenticity, data integrity, and privacy all at risk.

The cost of not using a zero-trust security solution?

The cost of doing nothing or not being prepared to protect data can be significant if a breach occurs, as the loss will spread across many areas of an organization, including diminished productivity, where data loss incidents impact day-to-do day operations and revenue.

Next is the response costs of dealing with the compromise: software and hardware has to be taken offline and addressed so the vulnerability that permitted the breach is fixed. Infected systems also need to be purged or replaced.

Since operational technology is increasingly used for critical systems, if these are compromised it can lead to a lot of risk and exposure well beyond a typical breach. If these systems are corrupted or intentionally altered they run the risk of not only adversely affecting OT operations, they could lead to loss of property or even life.

Of course, regulatory action is also a possibility if the breach is related to data or regulatory compliance. But, least quantifiable but perhaps most widespread damage is the loss of reputation, credibility and competitive advantage. In any business model that operates with sensitive information, when that is compromised, existing customers and prospects alike will often look elsewhere for a more secure solution.

How to best protect your device in the data supply chain

Many IoT devices are installed in field environments where organizations can not practically control security. The networks connecting these devices are often plagued with weak security protocols, incomplete implementations, and badly configured gateways–providing easy access to malicious botnets and other malware.

What you should look to combat these issues are solutions that can maintain data integrity, authenticity, and privacy on a system level. The protection should be persistent, whether the data is at rest or in transit. It should offer app level security for zero trust architectures, including ones that contain unprotected or poorly protected legacy devices. Finally, the solution should offer an approach to ensure trust or attest trustworthiness.

Intertrust XPN for zero-to-full trust environments

Intertrust' Explicit Private Networking (XPN) is an innovative technology for use in zero-trust architecture environments that provides end-to-end security for data at rest as well as in transit from device to cloud and back.

XPN leverages flexible PKI (public key infrastructure) certificates, the latest standardized cryptographic techniques, attestation, and data governance to seamlessly assure the integrity, authenticity, and secrecy/security/privacy of IoT devices. XPN's protection persists from the origination device all the way through to cloud services that manage the data and final distribution to the end applications.

Unlike VPNs or other network-focused security measures that may only protect one network segment, XPN is specifically designed to be independent of any current or future networking technologies and offers:

- **Persistent data protection**
  Data packages are digitally signed and optionally encrypted before being transmitted. Data is verified/validated to ensure its integrity on the server side, and only routed upon confirmation.
- **Entity attestation tokens**
  XPN issues a standards-compliant token attesting that devices are secure and can be trusted. The token is verified by Intertrust Platform to validate its trust state
- **Enhanced auditing**
  Audit information on IoT data used in transactions, including timestamps and attestations on device and data integrity. Organizations can use these enhanced audits for business or regulatory purposes.
- **Digital twin and firewall for legacy devices and systems**
  Legacy devices with limited or no hardware security capabilities, XPN maintains a digital twin of the device. This acts as a firewall so any connection requests are first received by the digital twin and only routed to the device if determined safe.

Intertrust XPN offers trusted interoperability for data and devices–across the data supply chain of untrusted networks, devices services, data infrastructures, and data services–your information is always protected and secure.

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