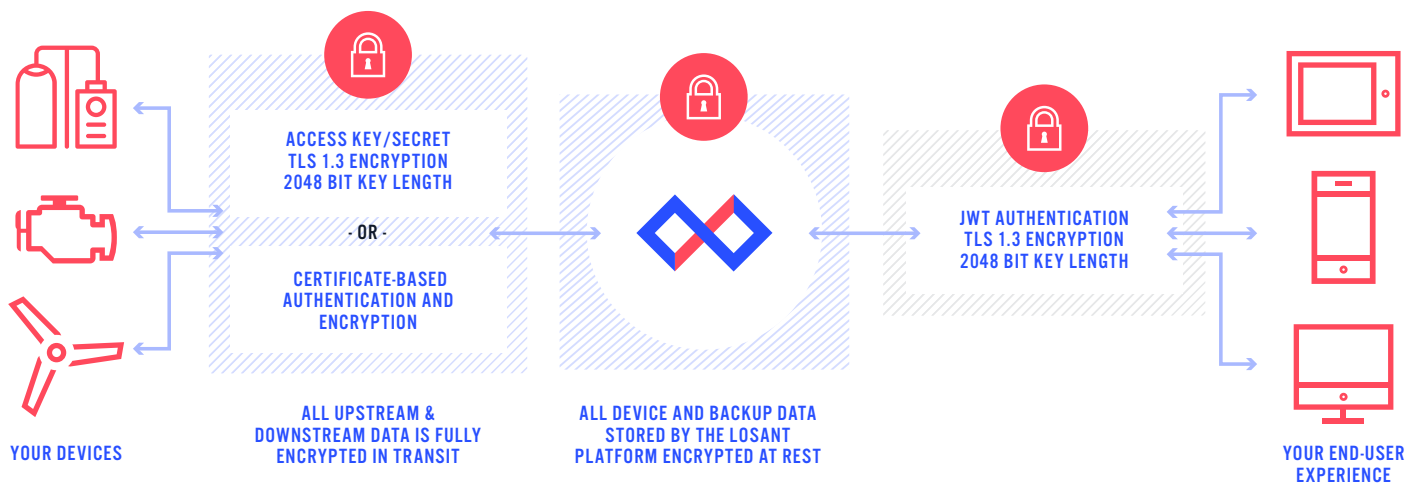# LOSANT

Securing Your Internet of Things

Ensure your information is safe at all times with Losant's security-first approach encompassing product, infrastructure, and architecture.

End-To-End Data Encryption

Confidently build and scale solutions for your enterprise using Losant. Data encryption practices combined with a set of other security controls promote peace of mind for your organization and your clients.

ACCESS KEY/SECRET TLS 1.3 ENCRYPTION 2048 BIT KEY LENGTH

- OR -

CERTIFICATE-BASED AUTHENTICATION AND ENCRYPTION

JWT AUTHENTICATION TLS 1.3 ENCRYPTION 2048 BIT KEY LENGTH

YOUR DEVICES

ALL UPSTREAM & DOWNSTREAM DATA IS FULLY ENCRYPTED IN TRANSIT

ALL DEVICE AND BACKUP DATA STORED BY THE LOSANT PLATFORM ENCRYPTED AT REST

YOUR END-USER EXPERIENCE

NEW IN 2023: SERVICE CREDENTIALS

A core feature of Losant's application enablement platform is its ability to easily connect with the managed services of Amazon Web Services, Microsoft Azure, and Google Cloud Platform. In most cases, usage of those services requires authentication, and the values that make up the auth request are considered highly sensitive. Service credentials are a more secure and user-friendly way to store authentication keys that connect your IoT applications with other elements of your company's cloud infrastructure. And most importantly, the sensitive portions of these credentials are never returned to the user after creation, greatly reducing the risk of unauthorized access to your data and processes.

WWW.LOSANT.COM

How Does Losant Secure Your Internet of Things?

Granular Access Control with Full Audit Logging

Losant's multi-level permissions system provides fine-grained control over your users and their access rights. With built-in audit logging, Losant makes it easy to investigate user behavior and activity.

Independent Third-Party Security Audits

In addition to Losant's internal security testing, each year Losant undergoes comprehensive white-box and black-box testing with an independent third-party security firm.

Industry-Standard Best Practices

- Two-factor authentication
- Minimum password complexity requirements
- Automatic account lockout on failed log-in attempts
- JWT specification for authentication tokens
- Per-device and revocable authentication keys

- TLS 1.3 with 2048 bit key length encryption in transit
- AES 256 encryption at rest
- Hosted on GCP for ISO and SOC compliant infrastructure
- On-premises and dedicated cloud deployment options
- 24-48 hour response time for critical security patches

SOC 2 Compliant

Losant undergoes a regular third-party audit to certify our enterprise platform against the SOC 2 compliant standards. SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC).

The report evaluates information systems relevant to security, availability, processing integrity, confidentiality, and privacy.

ISO 27001 Certified

Losant is proud to be ISO 27001 Certified, a process we are audited for and recertified on an annual basis.

ISO certification speaks to our commitment to manage our users' data – as well as their IoT application data – safely and securely.

We regularly audit our internal processes and employee data access to ensure that we follow the guidelines set forth by the ISO standard.

WWW.LOSANT.COM

© LOSANT IoT, 2023

LOSANT IoT, INC. | **1100 SYCAMORE STREET** | **7ᵀᴴ FLOOR** | **CINCINNATI, OH 45202** | **UNITED STATES of AMERICA**