Datasheet

# IronCore Labs SaaS Shield + Thales CipherTrust Manager Integration

SaaS companies are responding to the data sovereignty requirements of their global customers by upgrading data security with developer-proof application-layer encryption and privacy preserving key management.

IRONCORE LABS

VERIFIED SOLUTION
THALES

# ADDRESSING THE DATA SOVEREIGNTY DILEMMA

### A Flexible Technical Solution to Address Privacy Regulations

Data sovereignty is an urgently growing concern for companies and their customers who must comply with regional data privacy laws like GDPR, which only allows transfers to third countries with adequate privacy protections. The United States and China, among others, are deemed inadequate to hold the personal data of EU citizens.

That's where the IronCore Labs SaaS Shield platform and the Thales CipherTrust Manager come into play. Encrypt your customers' sensitive data at the application layer, before it goes to the data store, and place the keys under the jurisdiction of the appropriate country. **For B2B SaaS companies, customers can even hold their own keys or leverage a partner that offers the Thales CipherTrust Manager as a service.**

The integration makes it easy for SaaS companies to protect their data, preserve the privacy of personal information they hold, and address data sovereignty concerns using advanced encryption and key management.

# THE POWER OF SAAS SHIELD BY IRONCORE LABS

### What is SaaS Shield and ALE?

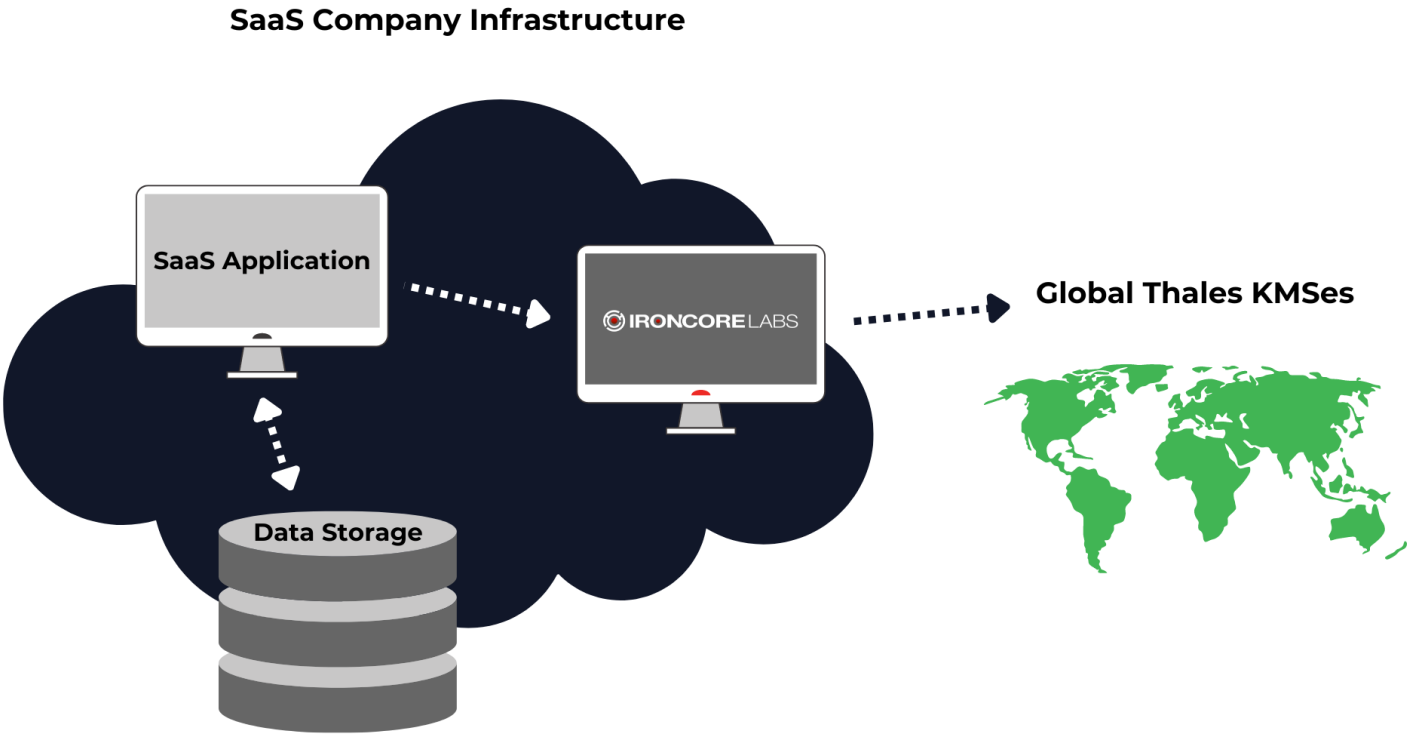
SaaS Shield by IronCore Labs makes it easy for companies to adopt application-layer encryption (ALE). ALE is an architectural approach where companies encrypt data before sending it to a data store. If it's compromised, the encrypted data remains safe.

SaaS Shield lives inside the SaaS provider's infrastructure but calls out to local and/or remote key management servers as necessary with different KMSes possible for different segments of data. For example, in a B2B SaaS application, each customer using the app could have their own key, which makes wholesale compromise and cross-customer attacks less feasible.

### Features of SaaS Shield:

- Advanced application-layer encryption
- Cloud-native
- Multi-tenant support
- Developer-proof
- Data isolation with per-tenant keys
- Audit trails and security logs
- Hold Your Own Keys (HYOK)
- Crypto-agile (algorithm choices, key sizes, etc., are dynamically configurable)
- Key leasing with fast revocation
- Bring your own storage

Integration with the Thales CipherTrust Key manager allows companies to better control their data by keeping their keys outside of the SaaS vendor's infrastructure.




## What is the Thales CipherTrust Manager?

CipherTrust Manager offers an industry-leading enterprise key management solution that enables organizations to centrally manage encryption keys, provide granular access control and configure security policies. CipherTrust Manager is the central management point for the CipherTrust Data Security Platform. It manages key lifecycle tasks including generation, rotation, destruction, import, export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers a developer friendly REST API.

**When combined with IronCore Labs, the Thales CipherTrust Manager creates and holds keys that it never shares.**

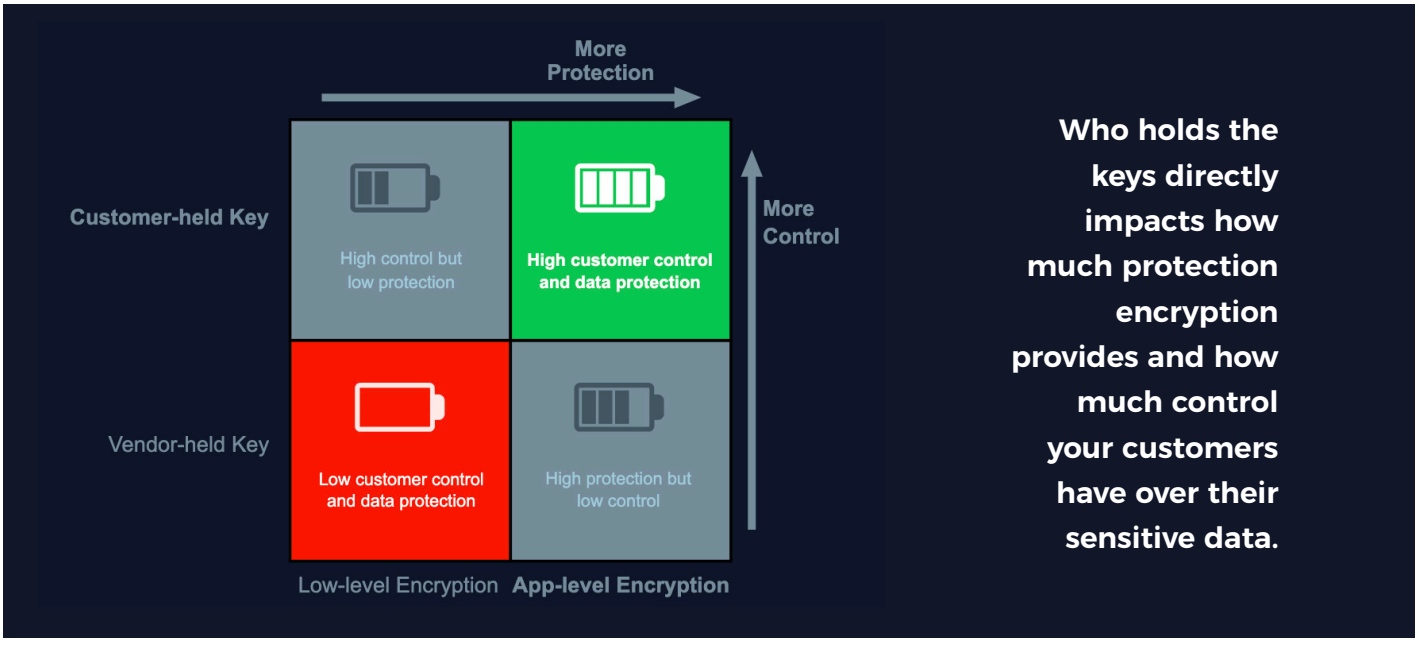
Access to keys (and therefore the data they protect) can be revoked at any time by simply changing permissions on the keys. Keys can be rotated and managed according to company policy.

CipherTrust Manager is available in both virtual and physical appliances that integrates with FIPS 140-2 compliant Thales Luna or third-party Hardware Security Modules (HSMs) for storing keys using a highly secure root of trust. These appliances can be deployed on-premises in physical or virtualized infrastructures and in public cloud environments. Select Thales partners also deploy cloud-based options. These allow customers to efficiently address compliance requirements, regulatory mandates and industry best practices for data security.

# KEY ORCHESTRATION PATTERNS

With SaaS Shield by IronCore Labs, you decide who holds the keys and where, which is one of the most vital aspects of application-layer encryption. Here are several options you have with SaaS Shield.

- **Regional vendor-held keys** means the SaaS provider also controls the KMS or KMSes and the keys on behalf of their customers. This provides strong protection for the data but can be problematic for data sovereignty if, for example, a U.S. company receives a U.S. subpoena for the keys they hold in a different region.
- **Regional partner-held keys**: multiple KMSes and the keys for a given customer or individual are held in the related region. Trusted partners are subject to the laws of the given region and those laws will determine how a government can access keys. This is a technical solution that preserves privacy and can meet international transfer and data sovereignty requirements.
- **Regional Customer-held keys** puts the control of the keys outside of the vendor's infrastructure and optionally into a different jurisdiction for data sovereignty purposes. This gives customers, generally in B2B scenarios, the ability to offer strong control, data protection, access transparency, and revocation capabilities.
- **Hybrid solutions** allow you to pick and choose the strategy per data segment based on region, customer, service levels, customer type, data subject nationality, or anything else.



## BENEFITS OF SAAS SHIELD + CIPHERTRUST

- Reduce risk by protecting data at the **application layer**
- Highly **performant** and secure
- **Developer-proof** integration
- Allow users to scale up **customer-managed keys** for enterprise customers
- Give users a technical solution to comply with **data privacy laws** and regulations
- Helps users safeguard data with future-proof and **quantum-ready** cryptography
- Built-in **audit logs** for visibility into data access and updates
- Sell into new markets to security-conscious prospects and **differentiate** from competitors
- Satisfy customer requests for higher levels of **security and control**
- Meet **data privacy and data sovereignty** needs around the world
- Add on Cloaked Search by IronCore Labs to **search over encrypted data** in Elasticsearch and OpenSearch

IRONCORE LABS

## ABOUT IRONCORE LABS

IronCore Labs is a data security platform for application-layer encryption and customer managed keys (CMK). We enable software developers and businesses to rapidly build enterprise applications with strong data control. Data owners decide who can access their data, monitor how it's used, when, where, and by whom, and can revoke that access at any time. IronCore Labs is the fastest and easiest way to control data in multi-cloud and SaaS environments.

THALES

## ABOUT THALES

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

**IronCore Labs**
1750 30th Street #500
Boulder, CO 80301, USA

**Inquiries**
Email: info@ironcorelabs.com
Phone: +1.415.968.9607

CONNECT WITH US

- ironcorelabs.com/blog
- linkedin.com/company/ironcore-labs
- twitter.com/ironcorelabs
- ironcorelabs.com