

Strengthening Data Privacy and Security with OpenText and Thales Luna HSM

Strengthening Data Privacy and Security with OpenText and Thales Luna HSM

Sensitive data is essential to business operations, but it is also one of the organization's greatest sources of risk as data breaches become more frequent and severe. AI's rapid adoption is expanding this risk by increasing the volume of sensitive data collected, accelerating cyberattacks, and enabling more sophisticated threats, while emerging quantum computing capabilities are raising concerns about the long-term effectiveness of traditional encryption. Personal, financial, payment, and regulated data are now distributed across databases, applications, cloud services, analytics pipelines, and AI environments. Perimeter security alone is insufficient for these large, distributed architectures, yet many complementary data protection methods can be complex, costly, or reduce the utility of protected data to the business.

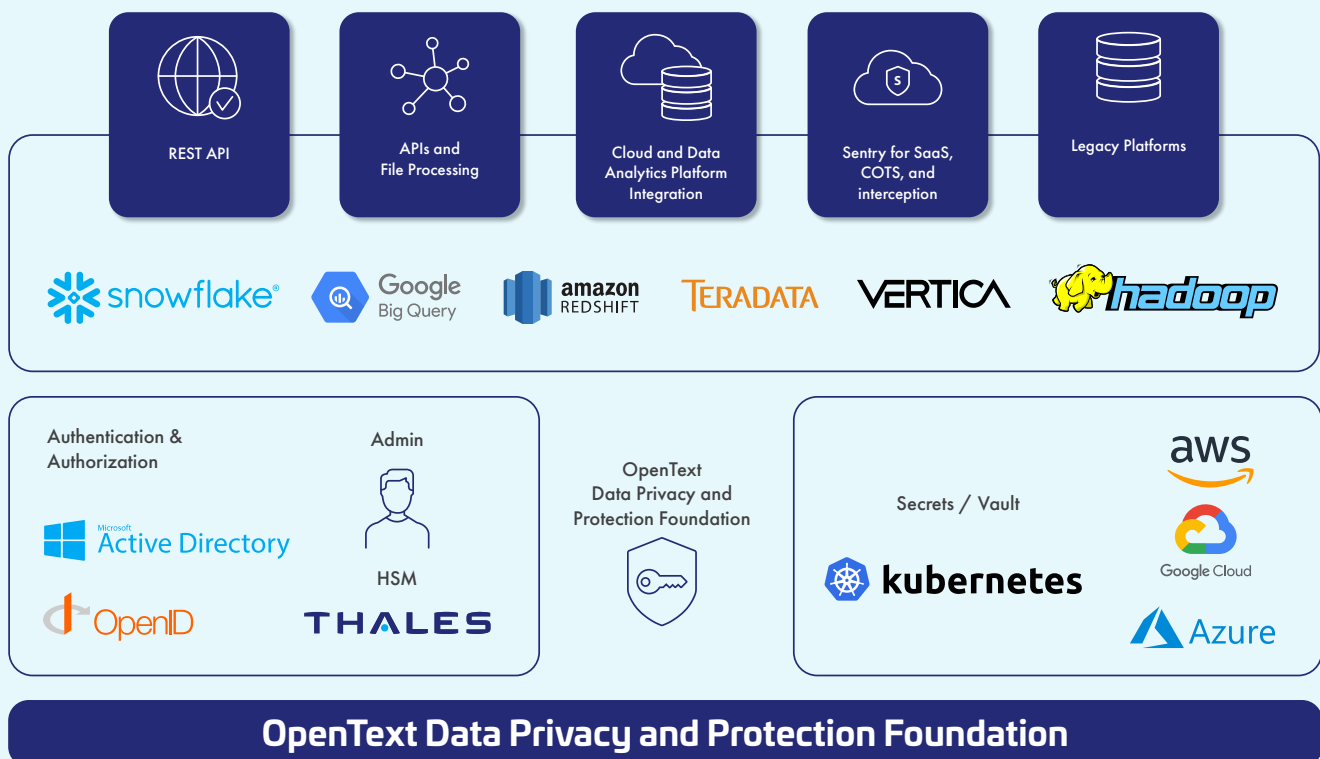
Organizations face not only growing risks to sensitive data but also increasing pressure to meet stringent compliance and sovereignty requirements. They need to protect and control sensitive data wherever it resides, across applications, databases, analytics environments, and hybrid cloud infrastructure without compromising

its business utility or running afoul of regulatory obligations. For most organizations, that is a significant challenge.

Fortunately, OpenText and Thales have teamed up to help organizations address these concerns and turn security into a business enabler.

The Combined Solution: OpenText Data Privacy and Protection with Thales Luna HSM

OpenText Data Privacy and Protection's (DPP) approach secures sensitive data while preserving its value to business operations. Unlike traditional encryption approaches that often require applications to decrypt data before use, OpenText DPP enables organizations to protect sensitive information while preserving format, referential integrity, and operational usability. This allows applications, analytics platforms, and business processes to continue operating with protected data, reducing exposure while minimizing disruption. Organizations can process transactions and analyze data without ever having to return it to its original format. This approach keeps data safer for longer without affecting the ability of the business to operate.



OpenText DPP uses Thales Luna HSMs to securely generate, protect, and manage cryptographic secrets within the tamper-resistant confines of a dedicated HSM. Sensitive cryptographic operations – such as DPP’s encryption key derivation – are done without exposing key material outside the physical and logical protections of the HSM’s trusted boundary. As a result, organizations strengthen their overall OpenText DPP security posture, reduce key exposure risk, and maintain tighter control over sensitive cryptographic processes. Together, the two solutions reduce exposure to a wide variety of risks without forcing organizations to modify applications, redesign workflows or disrupt day-to-day operations.

Solution Component	Role in the Combined Solution
OpenText DPP	Protects sensitive data in use through tokenization, encryption, and data-centric controls while preserving compatibility with applications, databases, and workflows.
Thales Luna HSM	Protects master secrets in tamper-resistant hardware and provides the root of trust for cryptographic operations under enterprise control.
Combined Value	Helps reduce exposure, preserve data usability, strengthen compliance readiness, and improve control over encryption infrastructure.

Key Benefits of the Combined OpenText and Thales Solution

Protect Sensitive Data with Hardware-Backed Cryptographic Secrets

OpenText reduces data exposure through tokenization and format-preserving encryption, while Thales protects the cryptographic secrets that secure those controls. Software-stored keys are more vulnerable to theft, misuse, and compromise. Luna HSM keeps sensitive key material inside purpose-built FIPS 140-3 validated tamper-resistant hardware to mitigate a wide range of security risks. Knowing that keys never leave the secure HSM boundary in plaintext gives organizations confidence in their infrastructure’s cryptographic foundation. Together, organizations have a crypto-agile architecture that confidently secures them today while helping them prepare for PQC standards.

Trusted Crypto Operations and Compliance Readiness

With Luna HSM as the root of trust, organizations can be confident that their encryption and tokenization processes are backed by hardware protection. Since secrets remain protected within the Luna HSM and are never exposed in plaintext outside the HSM boundary it is easier for customers to demonstrate control of their cryptography by demonstrating control of their physical HSM appliance. Organizations have full auditable visibility for how keys are accessed and used to simplify reporting.

Combined, OpenText DPP and Thales Luna HSM strengthen security controls for regulated data while simplifying audit, compliance, and risk management efforts. De-identifying or pseudonymizing sensitive data and providing secure key management with detailed audit logging helps organizations reduce compliance scope and ease the burdens of addressing their regulatory reporting requirements.

Scale Securely Across Hybrid and Cloud Environments

The use of HSMs for key protection is a recommended best practice for cloud deployments. HSMs provide critical protection against key derivation when configuration backups are compromised. Configurable with up to 100 cryptographically isolated partitions, a single Luna HSM can act as the root of trust for hundreds of independent applications, providing customers with the scalability, flexibility and security necessary for virtual and cloud environments.

Build a Stronger Foundation for Data-Centric Security

For enterprises, protecting sensitive data requires a layered approach that combines strong encryption with complementary controls to reduce risk exposure, preserve data usability, and ensure the cryptography involved is trusted and beyond reproach.

OpenText Data Privacy and Protection and Thales Luna HSM come together so organizations can adopt such a data-centric security model—one that helps organizations reduce risks to sensitive data while making sure it is available and usable across IT environments.

By combining strong key protection with crypto agility, this approach provides a certified foundation of trust that helps organizations stay secure into the future and adapt to evolving threats over time.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.