SOLUTION BROCHURE

Data-Centric Security With OpenText Data Protection Platform (DPP)/Voltage SecureData and Entrust nShield HSMs

ENTRUST

SECURING A WORLD IN MOTION

Using hardware-protected key management to strengthen OpenText data protection, privacy, and compliance outcomes

Executive Summary

Modern organizations manage large volumes of sensitive information, including payment data, regulated personal information, healthcare records, financial data, and intellectual property. As cyber threats and regulatory requirements continue to increase, organizations need security controls that protect the data itself rather than relying solely on network boundaries. OpenText Data Protection Platform (DPP)/Voltage SecureData provides a data-centric security approach that protects sensitive information while preserving business functionality.

OpenText DPP/Voltage SecureData combines Format Preserving Encryption (FPE), Secure Stateless Tokenization (SST), Format Preserving Hashing (FPH), data masking, and stateless key management to protect sensitive information without requiring extensive application redesign. Protected data can remain usable for reporting, analytics, operational workflows, and business processes while significantly reducing exposure risk. Stateless key management derives keys from protected root secrets rather than maintaining large key repositories, reducing operational complexity and attack surface.

Entrust nShield HSMs complement the OpenText architecture by providing a hardware-based root of trust for cryptographic root secrets. Using FIPS 140-3 Level 3 validated hardware, organizations can strengthen governance, key protection, and trust in the broader OpenText data protection architecture. Together, OpenText and Entrust help organizations reduce breach impact, simplify compliance, support cloud adoption, and enable secure use of data in analytics and AI initiatives.

Introduction: The Case for Data-Centric Security

Organizations operate in increasingly distributed environments spanning data centers, public cloud services, private cloud platforms, business partners, remote workers, and analytics environments. Sensitive information frequently moves between systems and users, making traditional perimeter-focused security insufficient as a standalone protection strategy.

Data-centric security addresses this challenge by protecting data at the field level through encryption, tokenization, hashing, and masking. Protected information remains protected as it moves between databases, applications, analytics platforms, backups, and cloud services. Even if unauthorized access occurs, exposed information is substantially less useful to an attacker.

Historically, broad encryption adoption was limited by operational and integration challenges. Traditional encryption can alter data format and structure, forcing application changes. Tokenization systems may require centralized repositories that create operational complexity. OpenText DPP/Voltage SecureData addresses these challenges through technologies specifically designed to preserve business usability while improving security.

OpenText Technologies That Enable Data-Centric Security

OpenText DPP/Voltage SecureData provides the policy-driven software layer that applies protection directly to sensitive information. Organizations can align protection techniques to specific business, compliance, and operational requirements while maintaining application functionality.

Hyper FPE, Hyper SST, FPH, and data masking provide flexibility for different data types and business requirements. A single organization may use encryption for regulated payment information, tokenization for customer identifiers, masking for operational workflows, and hashing for analytics use cases.

Stateless key management reduces dependence on persistent key repositories and simplifies operational management. Keys are derived when needed from protected root secrets, reducing the number of high-value repositories that must be secured, backed up, replicated, and monitored.

1. **Format Preserving Encryption protects sensitive values while retaining expected formats used by applications and databases.**
2. **Secure Stateless Tokenization replaces sensitive information with tokens without requiring traditional token vault architecture.**
3. **Format Preserving Hashing supports repeatable pseudonymization suitable for analytics, matching, and reporting workloads.**
4. **Data masking provides role-based visibility controls that limit access to sensitive information.**
5. **Stateless key management derives keys from protected root secrets rather than storing large inventories of operational keys.**

OpenText DPP/Voltage SecureData With Hardware-Protected Key Management

Entrust nShield HSMs protect the root secrets supporting the OpenText architecture. FIPS 140-3 Level 3 validated hardware provides a strong trust foundation for cryptographic operations. CodeSafe 5 integration further allows critical cryptographic logic to execute within the protected HSM environment.

Together, these technologies allow organizations to protect sensitive information while preserving application compatibility, operational workflows, and analytical value.

Cloud and Hybrid Deployment

OpenText supports deployment across on-premises, cloud, and hybrid environments. Because protection is applied directly to data, organizations can maintain consistent policies across infrastructure environments. This enables cloud migration initiatives without sacrificing security controls.

Entrust nShield deployments, including cloud-hosted options, provide flexibility for organizations that require hardware-protected key management while maintaining a consistent trust model across distributed environments.

Payment Data and PCI DSS

Payment processors, retailers, service providers, and financial institutions face significant obligations to protect cardholder data. OpenText FPE and SST help organizations secure payment information while maintaining compatibility with existing applications and business workflows.

By reducing the number of systems that store or process exposed payment card data, organizations can reduce compliance scope and lower operational risk. Protected values continue to support business processes while limiting exposure if systems are compromised.

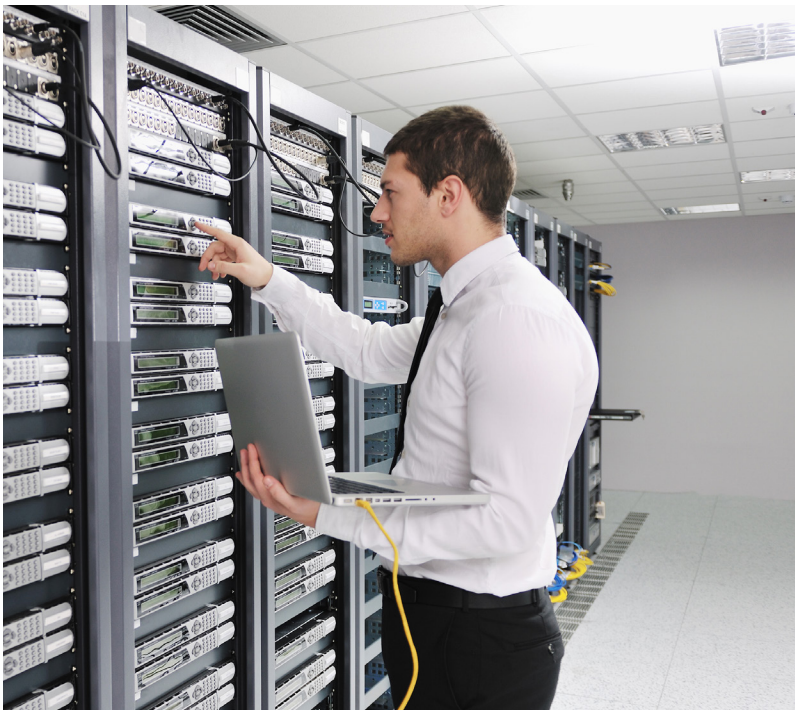
Entrust nShield HSMs strengthen this model by protecting the root secrets used to support OpenText stateless key management. This separation reinforces protection of payment environments and supports strong governance practices.

Personal Data, GDPR, and HIPAA

Organizations managing personal information and healthcare data must balance security, privacy, and operational usability. OpenText technologies allow personal and healthcare information to be encrypted, tokenized, hashed, or masked according to business requirements.

Healthcare organizations can continue supporting care delivery, research, analytics, and reporting while reducing exposure of personally identifiable information. Organizations operating under GDPR and related privacy frameworks benefit from stronger privacy controls and reduced exposure of sensitive information.

Hardware-protected key management complements these privacy controls by strengthening protection of cryptographic root secrets and supporting governance requirements around key access and administration.



Analytics, AI, and Machine Learning

Organizations increasingly rely on analytics, machine learning, and AI initiatives that require access to large data sets. Exposing raw sensitive information to these environments can create security, privacy, and compliance concerns.

OpenText data-centric protection technologies help organizations use realistic data while limiting exposure of sensitive values. Protected information can continue supporting analytics, fraud detection, business intelligence, research, and AI workloads.

This capability enables organizations to pursue innovation initiatives while maintaining appropriate protection of sensitive information. Protection remains tied to the data regardless of where the analytical workload resides.

Cloud Migration and Data Sovereignty

As organizations move applications and workloads to cloud platforms, they must maintain consistent control over how sensitive information is protected. OpenText applies protection directly to data, allowing governance, privacy, and security controls to remain consistent across on-premises, cloud, and hybrid environments.

Data sovereignty remains important for organizations operating across multiple jurisdictions. Regulatory requirements, regional privacy obligations, and data residency considerations increasingly influence security architecture decisions.

By protecting data at the field level and maintaining consistent protection policies across environments, OpenText helps organizations support sovereignty objectives while maintaining operational flexibility and supporting cloud adoption strategies.

Deployment and Operational Insights

Organizations can adopt OpenText incrementally, beginning with high-risk data domains and expanding over time. This phased approach reduces operational disruption and supports gradual expansion of protection policies.

Stateless key management supports large-scale deployments without dependence on centralized token vaults or extensive key repositories. The architecture is designed to support enterprise scale while reducing operational complexity.

Entrust nShield HSMs support governance, separation of duties, and controlled management of cryptographic root secrets. Together, OpenText and Entrust provide an architecture that balances operational usability with strong security controls.

Scalability and Availability

Large enterprises require architectures that can support high transaction volumes, broad deployment footprints, and diverse application environments. OpenText stateless key management reduces synchronization requirements associated with traditional key repositories and supports scalable operations.

HSM infrastructure can be deployed in highly available configurations that support enterprise resilience requirements. The result is a platform capable of supporting large-scale payment, healthcare, analytics, and customer-data workloads.

Compliance and Risk Reduction

Data-centric security helps organizations reduce the volume of exposed sensitive information across the enterprise. Protected information remains available for authorized use while limiting the value of data exposed through unauthorized access.

PCI DSS, GDPR, HIPAA, and other regulatory frameworks increasingly emphasize protection of sensitive information and reduction of exposure risk. OpenText technologies support these objectives through encryption, tokenization, hashing, masking, and governance controls.

Entrust nShield HSMs strengthen compliance initiatives by protecting cryptographic root secrets, supporting controlled access to key operations, and reinforcing separation-of-duties practices.

Future Readiness: AI, Cloud, Sovereignty, and Crypto-Agility

Organizations must prepare for continuing changes in threat landscapes, cloud adoption, data sovereignty requirements, AI initiatives, and cryptographic modernization.

OpenText provides a flexible platform that allows protection policies to remain consistent even as infrastructure, applications, and business requirements evolve. Because controls are tied directly to data, organizations can adapt more easily to infrastructure changes.

AI and Advanced Analytics

OpenText enables organizations to govern how sensitive information is used in analytics and AI environments. Protected information can continue supporting innovation initiatives while reducing unnecessary exposure of sensitive values.

Data Sovereignty

Organizations increasingly operate across multiple jurisdictions and regulatory frameworks. OpenText supports sovereignty objectives through field-level protection, consistent governance policies, and support for data residency requirements.

Post-Quantum and Cryptographic Agility

The transition to post-quantum cryptography will require coordinated updates across applications, protocols, infrastructure components, and cryptographic systems. OpenText centralizes protection policies and helps simplify modernization efforts.

Entrust nShield HSMs provide a trusted foundation for protecting root secrets and supporting future cryptographic migration strategies. HSM support alone does not complete post-quantum migration, but it remains an important component of a broader cryptographic modernization initiative.

Conclusion

OpenText DPP/Voltage SecureData enables organizations to implement a practical data-centric security strategy that protects sensitive information while preserving business value. Through FPE, SST, FPH, data masking, and stateless key management, organizations can reduce risk, simplify compliance, support cloud adoption, and enable secure analytics and AI initiatives.

Entrust nShield HSMs complement this architecture by providing a hardware-based root of trust using FIPS 140-3 validated technology. Together, OpenText and Entrust provide a scalable approach to protecting sensitive information, supporting regulatory obligations, and strengthening digital trust across modern enterprise environments.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION