SOLUTION BROCHURE

# OpenText™ and Entrust Solutions Deliver Data-Centric Information Protection

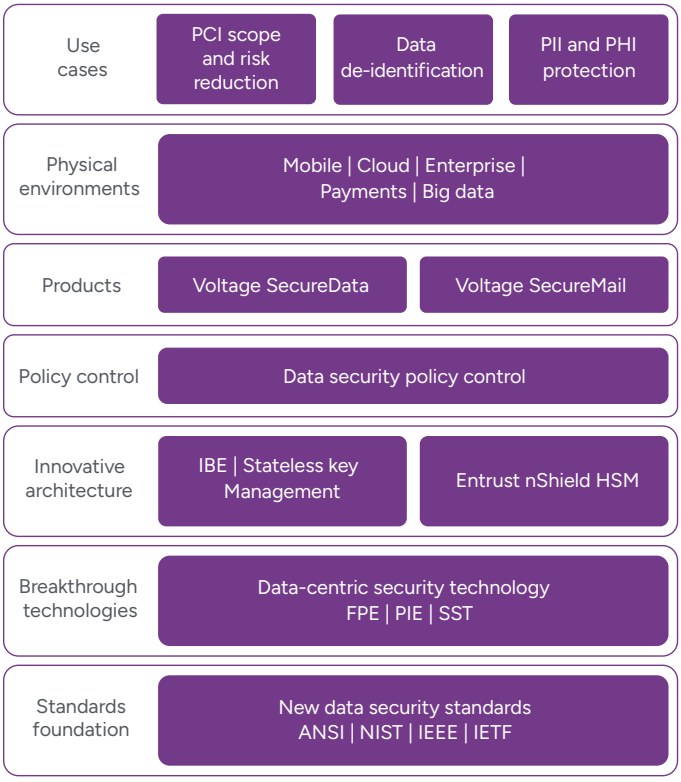
Achieve end-to-end data protection with OpenText Data Privacy and Protection (Voltage) and Entrust nShield hardware security modules

ENTRUST

SECURING A WORLD IN MOTION

## Sensitive data is at risk the moment it is created or captured

Organizations that process credit card payments and similar sensitive customer data such as Social Security numbers and other personal data all too often recognize the need for greater security only after a data breach or organizational misuse. This results in costly consequences under an array of data protection regulations and laws, including full incident disclosure. However, to reduce risk and demonstrate compliance, many organizations employ auditable data protection processes that render sensitive information useless to all but legitimate users. By protecting sensitive data, companies can likely reduce the scope of PCI DSS audits, enable privacy compliance, and help support safe harbor from data breach disclosure with data privacy laws.



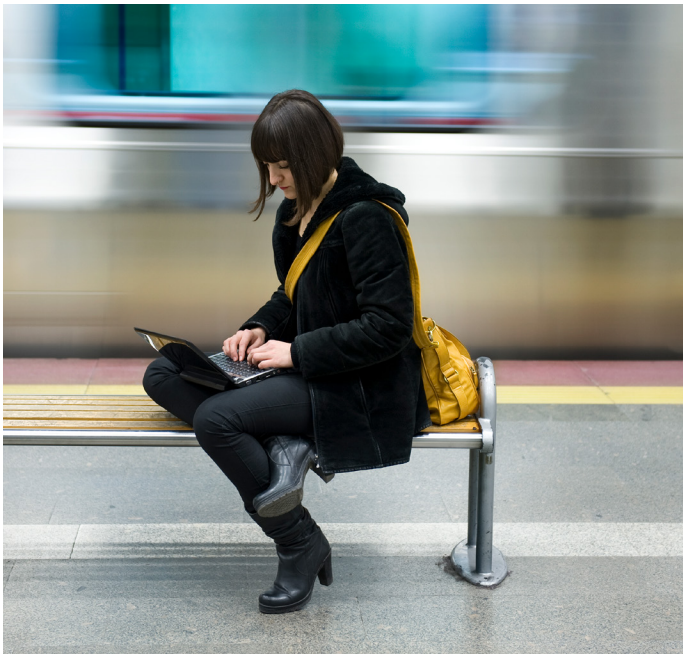

Entrust nShield HSMs safeguard and manage the secure root of trust associated with data-centric security technology within a FIPS 140 Level 3 security boundary. Entrust nShield can be deployed on premises or as a service.

## Highlights

- Delivers data-centric protection everywhere data is used, moved, and stored
- Reduces cost of compliance and simplifies audit scope
- Deploys quickly and easily
- Protects data without requiring change to applications or business processes
- Enables recoverability of sensitive data under secure policy

## Long-standing perception: Protecting sensitive data disrupts normal business operations

Historically, encryption, by its very design, protects sensitive data at rest and prevents it from being accessed by unauthorized applications and users. However, most encryption techniques render existing data processing systems and schemas unusable due to their inability to handle encrypted data. Add to this the cost and complexity of managing encryption keys, and it is no mystery why the perception persists that encryption makes data unusable and difficult to manage.



## The solution: OpenText and Entrust together help customers demonstrate privacy compliance, reduce PCI DSS audit scope, and neutralize breaches end-to-end

Innovative OpenText Data Privacy and Protection (Voltage) data protection resolves the issues of historical encryption methods. OpenText Data Privacy and Protection (Voltage) enables companies to neutralize the impact of data security breaches by preserving the format – and thus, usability – of data, while rendering the data valueless to cyber-attackers. Using breakthrough technologies, OpenText Data Privacy and Protection (Voltage) provides a comprehensive data-centric approach to enterprise data protection that addresses enterprise security and privacy needs not only for data at rest, but also for data in motion, and in use in business processes and analytics.

OpenText Stateless Key Management securely derives keys on-the-fly, significantly reducing IT costs and administrative staff burden by eliminating the need for a key database, key storage, replication, and backup. Stateless Key management delivers scalability for protection of today's massive high-value data feeds, enabling enterprises to focus on the business of data use, with protection and privacy compliance enabled.

Deployed on premises or as a service, nShield® hardware security modules (HSMs) integrate seamlessly with Stateless Key Management to host the master root key for the encryption key derivation function in a hardened device for trust assurance.

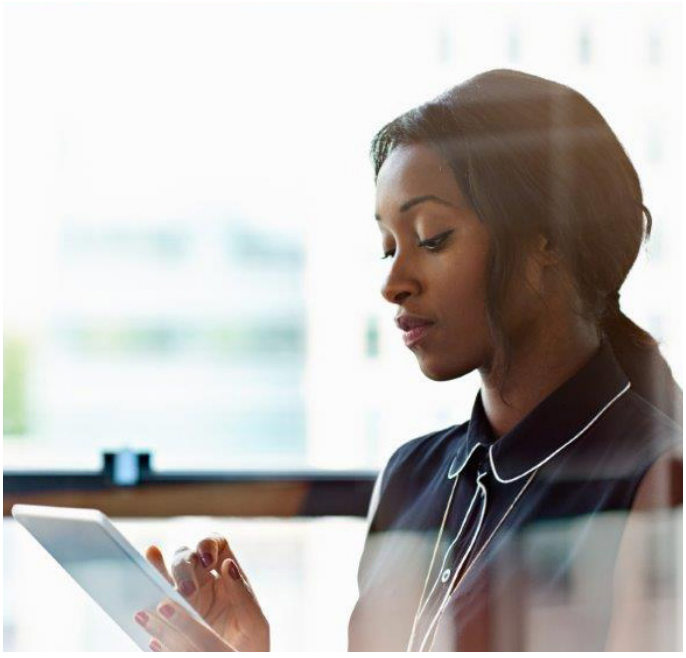
Critical encryption/decryption and key management processes are also performed within the secure boundary of the Entrust nShield HSM using CodeSafe, a unique capability that enables secure code execution inside the tamper-resistant environment. Within CodeSafe, keys and cryptographic processes are safeguarded and managed away from possible malware or insider attacks.

## Why use Entrust for enhanced security?

nShield HSMs provide high security available in a hardened, FIPS-validated physical device to protect critical information such as payment card data, personal information, applications, and business critical data, and are specifically designed for cryptographic processing. Critical keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attacks that can lead to disclosure of confidential information. HSM use rose to 55% of respondents from a baseline of 47 in 2019[1].

**Entrust nShield HSMs:**

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage, and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasingly demanding transaction rates
- Are available in several form-factors: as an appliance, PCIe, USB, and as a service



## Benefits of the combined solution

Entrust nShield HSMs integrate with OpenText Data Privacy and Protection (Voltage) to offer reductions in cost and time for privacy compliance. The combined capabilities provide comprehensive logical and physical protection that delivers a tangible and auditable method for enforcing security policies that underpin critical components of a data protection infrastructure. The data-centric approach mitigates data leakage and avoids disclosure from the outset, regardless of platform choice, outsourcing needs, scaling requirements, or IT processes. By providing a mechanism to enforce security policies and providing a secure tamper-resistant environment for encryption, key management, and code execution, this solution enables customers to demonstrate compliance and minimize the scope of security audits.

## OpenText

OpenText is an information management software company that helps companies organize, store, and protect their data. We provide integrated solutions in analytics, business networks, content services, cybersecurity, DevOps, IT management, and more. Our software is designed to propel businesses forward with cloud, security, and AI tools that facilitate enterprise-level growth and innovation.

For more information, please visit us at www.opentext.com

## Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

For more information, please visit entrust.com/HSM

1. Ponemon Institute 2024 State of Zero Trust Encryption Study, May 2024

## ABOUT ENTRUST

Entrust fights fraud and cyber threats with comprehensive identity-centric security that protects people, devices, and data. Our solutions help enterprises and governments safeguard critical systems from every angle, enabling secure onboarding and issuance, providing everyday identity protection, and empowering them with 360-degree visibility and orchestration across keys, secrets, and certificates so they can transact and grow with confidence. Building on our decades as a pioneer and innovator in establishing trust, 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