THALES

www.thales-esecurity.com

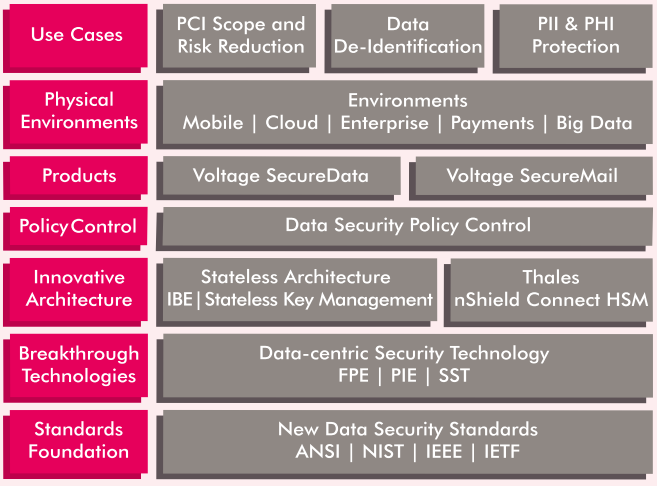
# ACHIEVE END-TO-END DATA PROTECTION WITH VOLTAGE SECURITY AND THALES HARDWARE SECURITY MODULES

- **Solution Benefits**
  - Protects data everywhere it goes
  - Reduces cost of compliance and audit
  - Deploys quickly and easily
  - Protects integrity of security processes
  - Guarantees recoverability of critical data

Voltage security

Thales e-Security

# Voltage Security and Thales Solutions Deliver Data-Centric Information Protection



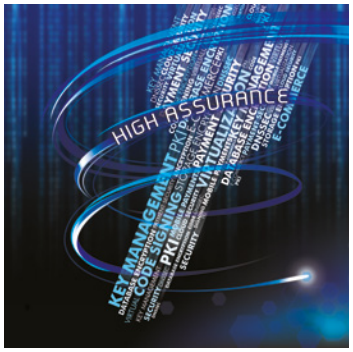

Thales nShield® HSMs safeguard and manage the system-level keys associated with data-centric security technology within a FIPS 140-2 Level 3 security boundary

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

Organizations that process credit card payments and other sensitive customer data such as social security numbers all too often recognize the need for greater security only after a data breach. This results in costly consequences under an array of data protection regulations and laws, including full incident disclosure. To reduce risk and demonstrate compliance, many organizations employ auditable data protection processes including file and email encryption that aim to render sensitive information useless to all but legitimate users. By encrypting sensitive data, companies can reduce the scope of PCI DSS audits and may achieve safe harbor from data breach disclosure and protection laws.

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

Encryption, by its very design, protects sensitive data wherever it goes and prevents it from being accessed or used by unauthorized applications and users. However, IT system architects and security administrators are often reluctant to implement needed changes due to the potential disruption caused by adding encryption to existing data processing systems and schema. Add this to the cost and complexity of managing keys and it is no mystery why this long-standing perception persists.




# VOLTAGE SECURITY AND THALES SOLUTIONS DELIVER DATA-CENTRIC INFORMATION PROTECTION

**The Solution: Voltage Security and Thales together help customers demonstrate compliance, reduce PCI DSS audit scope, and neutralize breaches end-to-end.**

Voltage Security provides a comprehensive data-centric approach to enterprise data protection that addresses the security and privacy needs for data at rest, in motion, and in use. Voltage enables companies to neutralize breaches and render data valueless using breakthrough technologies. Voltage Format-Preserving Encryption™ (FPE) enables sensitive data such as credit card and social security numbers to be encrypted while retaining their field length. Applications no longer need re-coding to process encrypted fields, maintaining referential integrity and avoiding costly database schema changes. Voltage Page-Integrated Encryption™ (PIE) encrypts payment and personal data in browser-based transactions from the moment they are entered into the browser all the way to the trusted host. Voltage Secure Stateless Tokenization™ (SST) eliminates token databases and removes high-value targets for hackers. Voltage Identity-Based Encryption™ (IBE) uses stateless key management to derive keys on-demand and regenerate them from existing credentials. Using these technologies, Voltage SecureData™ and Voltage SecureMail™ products delivers comprehensive data security.

Thales nShield hardware security modules (HSMs) integrate seamlessly with Voltage SecureData and Voltage SecureMail to protect the underpinning cryptographic keys used for data encryption, de-identification, and masking. Thales nShield HSMs manage the system level keys used for key derivation within a hardened device, significantly reducing the risk of compromise. Critical encryption/decryption and key management processes are also performed within the secure boundary of the Thales 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 Thales HSMs for enhanced security?

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. HSMs are the only proven and auditable way to secure valuable cryptographic material.
Thales 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

## Benefits of the combined solution

Thales nShield HSMs integrate with Voltage SecureData 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 secure tamper-resistant environment for encryption, key management and code execution, customers can demonstrate compliance and minimize the scope of security audits.

## Thales e-Security

Thales e-Security, Inc. is a global leader in trusted cryptographic solutions. Thales nShield HSMs provide a hardened, tamper-resistant environment for encryption and key management. nShield HSMs eliminate traditional deployment and scalability issues, enabling strict enforcement of security policies and separation of critical functions from administrative tasks. For more information, please visit www.thales-esecurity.com

## Voltage Security

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, powerful data protection solutions from Voltage allow any company to seamlessly secure all types of sensitive corporate and customer information wherever it resides, while efficiently meeting regulatory compliance and privacy requirements. For more information, please visit www.voltage.com

**Follow us on:**



**Americas –** Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
**Asia Pacific –** Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
**Europe, Middle East, Africa –** Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com