Micro Focus Voltage and Entrust solutions deliver data-centric information protection

Achieve end-to-end data protection with Micro Focus Voltage and Entrust nShield hardware security modules

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

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

Use cases	PCI scope and risk reduction	Data de-identification	PII and PHI protection
Physical environments	Mobile | Cloud | Enterprise | Payments | Big data		
Products	Voltage SecureData	Voltage SecureMail	
Policy control	Data security policy control		
Innovative architecture	IBE | Stateless key Management	Entrust nShield Connect HSM	
Breakthrough technologies	Data-centric security technology FPE | PIE | SST		
Standards foundation	New data security standards ANSI | NIST | IEEE | IETF		

Entrust nShield HSMs safeguard and manage the secure root of trust associated with data-centric security technology within a FIPS 140-2 Level 3 security boundary. Entrust nShield can be deployed on-premises or as a service.

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.

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: Micro Focus Voltage and Entrust together help customers demonstrate privacy compliance, reduce PCI DSS audit scope, and neutralize breaches end-to-end

Innovative Micro Focus Voltage data protection resolves the issues of historical encryption methods. Micro Focus 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, Voltage SecureData 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.

Voltage SecureData includes next-generation technologies: Hyper Format-Preserving Encryption (FPE), Hyper Secure Stateless Tokenization (SST), Format-Preserving Hash (FPH), Stateless Key Management, and data masking. Voltage SecureData “de-identifies” data, while maintaining referential integrity for data processes, applications, and services. Voltage 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, Entrust nShield® hardware security modules (HSMs) integrate seamlessly with Micro Focus Voltage 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.

Delivering data-centric information protection

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 is 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. The use of HSMs as part of an enterprise encryption and/or key management strategy has been steadily increasing over the last six years.[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 Micro Focus 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 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.

Micro Focus Voltage

Micro Focus is a global software company with 40 years' experience delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. Micro Focus® Voltage data security solutions enable advanced Hyper Format-Preserving Encryption, Hyper Secure Stateless Tokenization, Stateless Key Management and data masking to protect high-value regulated data in enterprise applications, data processing infrastructure, hybrid IT/cloud, payment ecosystems, mission-critical systems, storage, and big data/IoT analytics platforms.

For more information, please visit us at **www.microfocus.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, Global Encryption Trends Study, 2020

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com