MICRO FOCUS

Data Sheet
Security

# Voltage SecureData Payments

In today's environment of heightened regulatory requirements and increasing risk of cardholder data breach, it is critical to protect payment data anywhere it moves, anywhere it resides, and however it is used. Micro Focus® Voltage SecureData Payments protects payment data at all points, from swipe/dip through to the payment processor, end-to-end.

## Product Highlights

Voltage SecureData Payments is a complete payment transaction protection framework built on a flexible and highly scalable architecture, including a common back-end infrastructure that protects system and device payment transactions for ecommerce (mcommerce), mobile payments, card on file (CNP), and the associated PII payment stream data. Voltage SecureData Payments protects the full payment stream—beyond just the credit card number—and the associated PII payment stream information, including payment data from POS devices, terminals, browsers, and mobile devices.

By protecting the data itself, Voltage SecureData Payments eliminates security gaps that exist between networks, databases, and applications when protected with point security solutions. It removes the traditional complexities associated with payment device key injection, key management, payment application changes, and enables a true end-to-end architecture that can be rapidly deployed even in the most complex environments.

## Key Benefits

- Diminishes the liability exposure of a breach while meeting card (PCI) requirements.
- Complies with the Payment Card Industry Data Security Standard (PCI DSS and PCI P2PE) and data privacy laws.
- Easily expands to accommodate new payment methods transparent to the user.
- Enables seamless omni-channel business with complete control over end-to-end payment security, independent of the payment or service provider solution.
- Ensures customer cardholder data is never in the clear at any point in the transaction flow (from the dip, swipe, keyed, or NFC) through to the protected backend.
- Flexible, scalable architecture with common backend infrastructure that protects payment transactions and associated PII/PHI payment stream data.

## SecureData at a Glance

- **Scalable big data security:** SecureData for Hadoop and IoT delivers scalable protection for data streaming into big data lakes, enabling analytic insights while lowering exposure to data misuse or breach.
- **Privacy compliance:** Micro Focus Data Privacy Manager addresses data privacy governance from discovery and classification to protection and reporting. Data is de-identified using a standards-based approach that can meet GDPR mandate requirements.
- **Cloud data security:** Voltage SecureData Sentry delivers transparent protection for data in the cloud in a platform-agnostic approach. SecureData Cloud provides cloud-native data protection for application workloads.

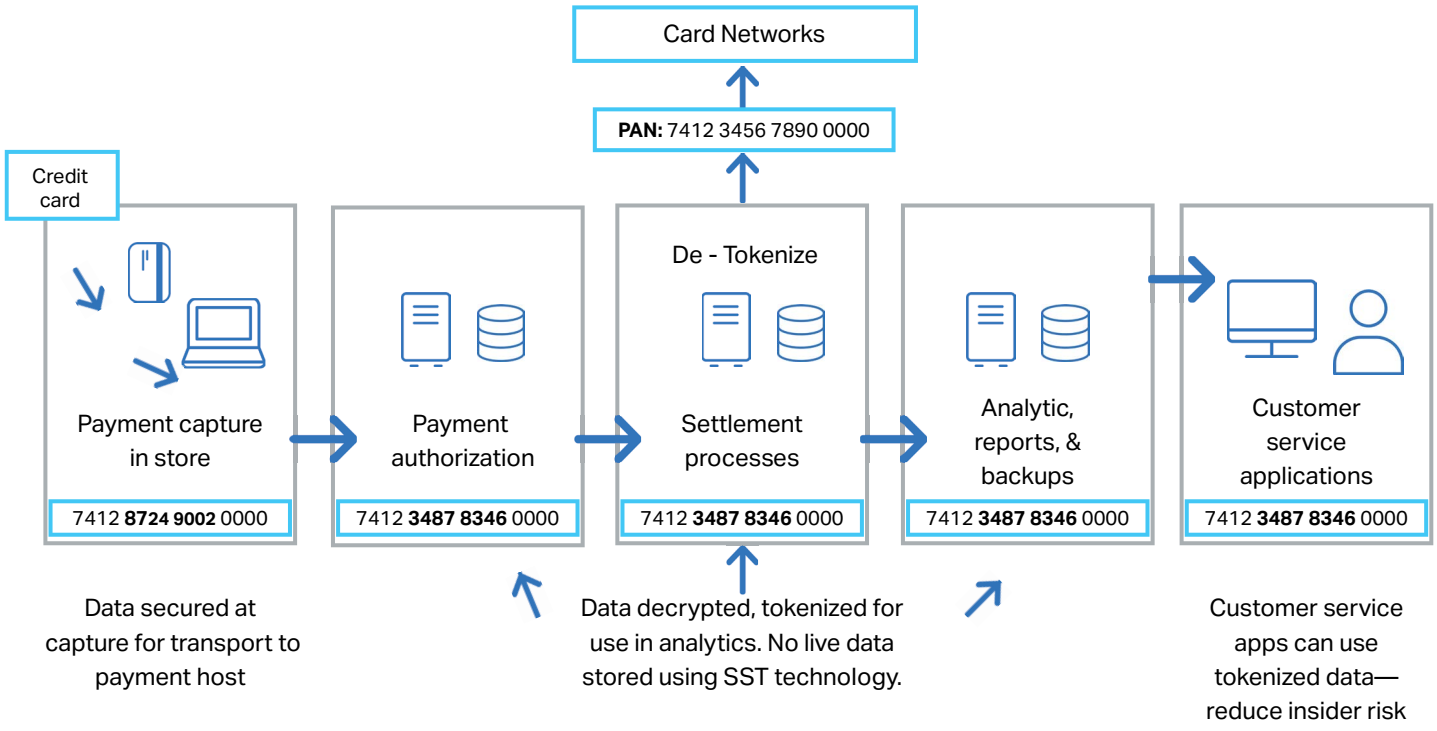


**Figure 1.** Securing Credit Card Payments with Data-centric Security

## Key Features

Voltage SecureData Payments is a complete payment transaction protection framework, built on two breakthrough technologies encompassing encryption and key management: Format-Preserving Encryption (FPE) and Identity-Based Encryption (IBE). These two technologies combine to provide a unique architecture that addresses the complexity of retail environments with high transaction volume.

### PCI Compliance Alignment

Voltage SecureData Payments can reduce the cost of complying with PCI DSS—a direct result of reducing the number of changes necessary to implement payment data protection while eliminating payment data from databases and applications. By incorporating Voltage Secure Stateless Tokenization with Voltage SecureData Payments, service providers, merchants, and enterprises are able to secure backend data, removing data from PCI audit scope while complying with the latest PCI DSS requirements for cardholder data protection. Voltage Secure Stateless Tokenization maintains token schemes across regions with no communication between them, eliminating the need for a central key management database as well as database replication. By tokenizing card numbers immediately at the source, clear data is eliminated from the transaction process.

### Voltage Format-Preserving Encryption

With Voltage Format-Preserving Encryption (FPE), credit card numbers and other types of structured information are protected without the need to change the data format or structure. In addition, data properties are maintained, such as a checksum, and portions of the data can remain in the clear. This aids in preserving existing processes such as BIN routing or use of the last four digits of the card in customer service scenarios.


**Figure 2.** Format Preserving Encryption

### Voltage Identity-Based Encryption

Voltage Identity-Based Encryption (IBE) is a breakthrough in key management that eliminates the complexity of traditional Public Key Infrastructure (PKI) systems and symmetric key systems. In other words, no digital certificates or keys are required to be injected or synchronized. IBE also enables end-to-end encryption from swipe-to-processor and swipe-to-trustedmerchant applications.

With point-of-sale (POS) solutions that use legacy symmetric encryption, encryption keys must be reset annually for each POS device through a process called key injection. This procedure is expensive and cumbersome, because merchants must take POS devices offline while new keys are injected. With Voltage SecureData Payments, because encryption keys are securely generated on demand and not stored, POS devices are not subject to key injection and key rotation. This function happens systematically, eliminating labor-intensive key management processes and costs.

### Voltage Secure Data Payments Compatibility

- **Robust host side capabilities and broad platform support:** Voltage SecureData Payments Host SDK can be deployed on a wide variety of platforms including HPE NonStop, Windows, Linux, UNIX, z/OS, and Stratus. It is the only data protection solution available that natively runs on Nonstop (OSS and Guardium) and Stratus VOS, enabling maximum protection and efficiency.
- **Unified, complete end-to-end data security:** Voltage SecureData Payments enables merchants and service providers to protect their entire payment stream and reduce PCI audit scope from the end user to backend systems by offering a variety data protection needs for m-commerce (in-app) payment data (mobile), e-commerce/in-browser payment data, device-based encryption of payments data (P2PE), and protect PCI data stored for post-authorization needs.
- **Stateless key management:** Voltage SecureData Payments does not require digital certificates or keys to be injected or synchronized with the host. Because encryption keys are securely generated on demand, POS devices sufficiently protect card data without the need for key injection or key rotation, which can be labor-intensive and expensive to administer.
- **Integrated with an industry-leading pioneer:** Voltage SecureData Payments is the only off-the-shelf integrated solution with a PCI-HSM and FIPS validated secure root of trust (Atalla HSM) to protect payment data, payment authorization and fraud prevention. The integrated solution extends end-to-end data protection through the combined, integrated solutions of Voltage SecureData Payments and Atalla Hardware Security Module (HSM). By joining data-centric data protection with a tamper-reactive hardware security module, companies are able to neutralize data breaches by protecting data, rendering it useless to attackers.
- **Multiple integration options:** Processors and merchants can choose to integrate using SDKs, Web services, and/or command line tools for quick and simple deployment. End-to-end encryption can easily be combined with Voltage Secure Stateless Tokenization (SST) to provide merchants with a complete solution for PCI audit scope by protecting data stored for post-authorization needs.
- **Integrated POS systems:** Voltage SecureData Payments solution is integrated into a variety of payment terminal devices and platforms, giving organizations the flexibility to select one or more payment vendor(s) for the required business needs. For a complete list of payment partners, visit voltage.com/partners.
- **Scalability and performance:** Flexible, scalable architecture that handles quickly scales eliminating the need for merchants to self-manage payment transactions. The platform delivers complete control over end-to-end payment security stream for the omni-channel business requirements.

Contact us at:
**www.microfocus.com**

Like what you read? Share it.

### How Secure Is Secure?

To ensure compliance with PCI DSS best practices and requirements, Coalfire, a well-known cyber risk management and compliance organization, conducted independent technical assessments of Voltage SecureData Payments to verify that it meets the current PCI DSS standards.

Learn more at
**www.microfocus.com/data-security-encryption**