

# Voltage SecureData Mobile

Voltage SecureData Mobile provides security for sensitive data submitted through a mobile endpoint. It enables end-to-end sensitive data protection within native mobile iOS and Android applications through the entire enterprise data lifecycle and payment transaction flow. Data is secured from the point of capture to the trusted host.

## Product Highlights

With the increase in mobile applications and a surge in data breaches, securing sensitive data in the mobile environment is more important than ever. Sensitive cardholder information in mobile payment applications, and Personally Identifiable Information (PII) and Protected Health Information (PHI) in other mobile applications, should be protected end-to-end. The need to safeguard sensitive data in motion captured on mobile endpoints becomes critical to ensure end-to-end data protection. Voltage SecureData Mobile protects sensitive data in native mobile apps while safeguarding the data end-to-end.

## Key Benefits

### Data Security for In-App Mobile Purchases

Voltage SecureData Mobile by OpenText leverages Voltage Format-Preserving Encryption (FPE) by OpenText to provide data security for in-app mobile purchases. It encrypts sensitive customer information such as PANs (credit card numbers) and the CVV/CVC (3-digit security code) when a customer makes a purchase through a merchant mobile application. The merchant environment has no access to PCI data in-the-clear or encryption keys because the PAN and CVV fields are encrypted in the mobile application before the data reaches the merchant's web services. Decryption happens at the host end so that transaction

## Quick View

- Enables consumer confidence to safely interact with the business through mobile devices
- Simplifies PCI compliance and provides scope reduction
- Enables PII and PHI compliance
- Protects sensitive data at every level of the omnichannel and unified commerce experience
- Recognized format-preserving encryption standard (NIST SP800-38G)
- Developer friendly—simple native libraries, easy to incorporate into iOS and Android apps
- Voltage Stateless Key Management eliminates operational complexity

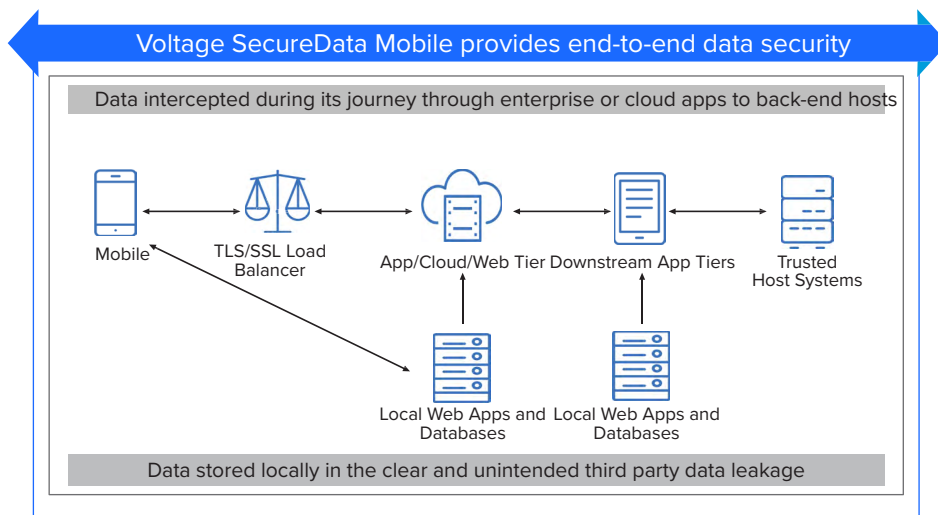


Figure 1. Voltage SecureData Mobile provides end-to-end data security

authorization can be completed. Voltage SecureData Mobile simplifies compliance and reduces PCI audit scope.

**Data Security for Personal Sensitive Information**

Voltage SecureData Mobile also provides data security for personal sensitive information such as PII and PHI, and enables companies to meet PII and PHI compliance requirements. Sensitive PII and PHI information such as name, address, social security number, birthdate, health information, and more is protected. In the healthcare industry, HIPAA and HITECH require and enforce the encryption of all PII and PHI data. Healthcare organizations can no longer afford to expose sensitive personal information in mobile environments, especially when more consumers are frequently using mobile apps to access test and lab reports, medical records, and billing services.

**Sensitive Data Safeguarded as It Moves through the Enterprise and Beyond**

In the financial services industry, the combination of new state privacy regulations with consumer demand for faster, more convenient banking and mobile wallet services has also driven the need for companies to secure sensitive data in mobile applications. In a 2015 Forrester report, the findings show consumers are more willing than ever to walk away from the business if it fails to protect their data and privacy.\* Voltage SecureData Mobile protects sensitive PII and PHI personal data in the mobile applications by encrypting the data so that it can be used safely throughout its lifecycle. Because live data exposure is removed from insecure systems, compliance to privacy regulation is also streamlined. Voltage SecureData Mobile safeguards sensitive data as it moves through the enterprise and beyond.

**Safe, Seamless Digital Purchasing Transactions**

With the growing popularity of digital shopping, the retail industry is rapidly embracing the omni-channel strategy that enables customers to have a seamless


shopping experience regardless of the channel, whether online, mobile, or in store. Because of this multichannel approach, it is critical for retailers to reduce fraud and protect consumer data at every touch point to deliver a transformative and secure customer experience. Given the recent number of high-impact retail breaches, and the rapid increase in mobile wallets, payment applications, and other mobile-based applications, retailers need to increase the protection of PII and PHI data so that consumers can safely interact with the business through their mobile devices. Voltage SecureData Mobile transparently secures the consumer’s submission of sensitive data through mobile applications, which gives retailers more control in the customer experience and how store associates interact with customers via mobile devices.

**Key Features**

**Highly Scalable, Reliable and Developer-Friendly Data Protection Solution That Leverages Voltage FPE, a Breakthrough Technology**

Voltage FPE is a mode of AES, a recognized encryption standard by NIST (NIST SP800-38G). The result of a standards-based encryption scheme allows for encryption with minimal modifications to the existing applications. Because Voltage FPE maintains the format of the data being encrypted, no database schema changes are required and only minimal application changes are required.

Connect with Us  
www.CyberRes.com



**Simple, Native Libraries to Easily Incorporate into Native Mobile Applications**

This enables the application code to retrieve a one-time-use cryptographic key for encrypting sensitive data. Voltage SecureData Mobile supports two mobile client platforms: iOS and Android.

**Support for Voltage State Key Management Architecture**

This architecture enables on-demand key generation and re-generation without the need for an ever-growing key store. The result is a system that can be infinitely scaled across distributed physical and logical locations for a low operational and infrastructure cost.

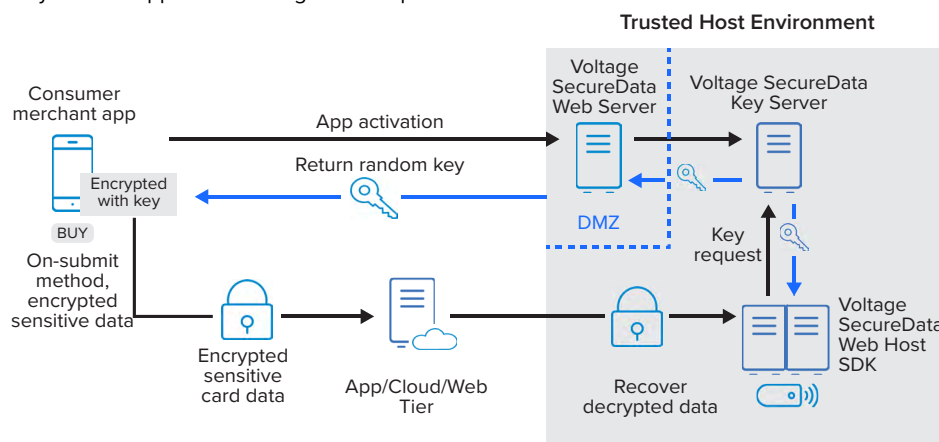


Figure 2. How It Works