Voltage security

DATA SHEET
Voltage SecureData Web

End-to-end Encryption for Payment Card and Personal Data at the Web Browser

SIGNIFICANTLY LOWERS RISK AND CUTS COMPLIANCE COSTS

Voltage SecureData Web delivers groundbreaking technology for securing payment and personal data in browser-based transactions. Voltage SecureData Web protects data from the moment of capture at the browser and keeps it protected all the way through the web tier, the application tier, cloud infrastructure, and upstream IT systems and networks to the trusted host destination.

The Challenge – Data Streams Must be Protected End-to-end

Today, many organizations are using the internet to collect sensitive data from their users such as payment data for e-commerce transactions, personal information for electronic medical records (EMR) and user credentials for access to systems and services. When sensitive data is entered into a browser, security gaps exist between systems, networks, and applications. These security gaps present opportunities for hackers to steal data. In browsers on desktop and mobile devices, the sensitive data can be protected while in transit between systems by Secure Socket Layer (SSL), but data remains in the clear in application servers, back office systems and databases. Point solutions such as database encryption can be used to protect data at rest, but information is still exposed as it enters and leaves each system. Without protecting the data from the browser all the way to the trusted host destination, hackers have more vulnerabilities to target, and compliance costs and risk of data theft rise. This problem will intensify as e-commerce, cloud computing, and mobile applications grow in popularity and use.

The Solution – Voltage SecureData Web

Voltage SecureData Web protects sensitive data at the browser and keeps it protected all the way to the trusted destination where it can be decrypted. This shields data from theft in front-end and intermediate systems, and also reduces audit footprint. E-commerce merchants required to comply with the PCI DSS can significantly reduce compliance costs and scope as systems and applications that previously handled payment data no longer have access to payment data. Voltage SecureData Web also protects Personally Identifiable Information (PII) typed into the browser, so PII and Primary Account Number (PAN) data is protected from the point of capture through the data life-cycle of processing, use and storage.

Benefits:

- **Protects sensitive data end-to-end** - Sensitive data is encrypted when the user enters data at the browser, and decrypted only at the trusted host destination. The data is thus no longer unprotected when it leaves an SSL tunnel during data transmission.
- **Eliminates PCI DSS compliance scope** - By removing access to sensitive data in merchant systems when properly implemented, as validated by Coalfire Systems. Read the Coalfire Systems Report at **http://www.voltage.com/resources/#PaymentSecurity**.
- **Enables a seamless user experience** – Alternative solutions, which use redirects or embedded iframes, disrupt the user experience and obscure web tracking data.

Page-Integrated Encryption

Voltage SecureData Web uses Voltage's Page-Integrated Encryption (PIE) technology to encrypt data in the browser at the moment of capture. PIE technology uses Voltage Format-Preserving Encryption (FPE) to protect data in the most transparent manner possible, allowing for quick deployment with minimal change to existing applications. Voltage Format-Preserving Encryption encrypts structured data like credit card numbers without changing the format or length, minimizing change to the associated applications, databases and other systems. The encryption employs a unique single-use key, and the data is decrypted only at the trusted host destination. Voltage SecureData Web works without user interaction and without compromising user experience. It is designed to work in any major mobile or desktop browser, without add-ons or plug-ins.

Data Security That Starts in the Browser

Voltage SecureData Web uses standard browser features for compatibility across systems including mobile and desktop. Browsers must be SSL-capable and have JavaScript enabled. The static JavaScript performing the encryption is provisioned to the browser via SSL from a trusted site, such as a secure server in your environment, and is invoked with just a few lines of HTML on the web page.

Voltage SecureData Web allows full control of user interaction and avoids third-party handoffs. The user experience is seamless, without complex iframes or redirects. Every step of the transaction can be monitored for analytic purposes without disruption. Users have the same improved experience on mobile device browsers as on conventional desktop browsers.

Most important, front-end and intermediate systems no longer handle sensitive data in the clear. Sensitive data stays encrypted from the beginning to the end of the transaction, substantially reducing compliance costs and risk.

The end-to-end protection provided by Voltage SecureData Web is unique in the industry. It provides an elegant and easily delivered solution to a pressing and escalating security challenge in e-commerce.

> *"A properly designed and deployed Voltage SecureData Web with PIE Technology-integrated e-commerce application can significantly reduce PCI DSS scope and validation requirements similar to merchants implementing a hosted payment page solution."*
>
> *— Voltage SecureData Web with Page-Integrated Encryption (PIE) Technology Security Review,* ***Coalfire Systems, Inc.***

Voltage SecureData Web includes:

- **Voltage Key Management Server:** Generates and manages single-time keys; supports key management across the Voltage SecureData suite; optionally supports FIPS 140-2 hardware key management through hardware security modules
- **Voltage SecureData Web Front End Server:** Delivers the key, key ID, and associated JavaScript to browsers
- **Voltage SecureData Host SDK:** Decrypts payment and PII data in backend hosts; supports HP-UX, HP NonStop, Solaris, Linux, AIX, Windows, Stratus, and z/OS operating systems
- **Voltage SecureData Management Console:** Built into the Voltage Key Management Server; enforces centrally defined policies and audits usage; provides robust and flexible authentication via centralized role-based control system, including dual controls.

ABOUT VOLTAGE SECURITY

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions 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.**

v05012013

Voltage Security, Inc. US Tel: +1 (408) 886-3200 EUR Tel: +44 (0) 203 468 0559 www.voltage.com/contact