opentext™ | Cybersecurity

Data Sheet

Voltage SecureData Web

Voltage SecureData Enterprise provides end-to-end encryption for payment card and personal data at the web browser.

Product Highlights

Security Gaps Leave Organizations and Their Customers at Risk
Today, more and more organizations are using the Internet to collect sensitive data from their customers such as payment data for ecommerce transactions, personal information for electronic medical records (EMR) and user credentials for access to systems and services. While sensitive data can be protected in transit between systems by Secure Socket Layer (SSL) / Transport Layer Security (TLS), significant security gaps remain as data remains in the clear in applications 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 vulnerable places to target. This problem only intensifies as e-commerce, cloud computing and mobile applications grow in popularity and use.

The Solution—Voltage SecureData Web
Voltage SecureData Enterprise for Web by OpenText protects sensitive data captured at the browser, from the point the customer enters their cardholder or personal data, and keeps it protected through the load balancing and web tier, the application tier, cloud infrastructure, and upstream IT systems and networks to the trusted host destination. Payment information, tax IDs, authentication credentials, or any structured field is protected from capture, only accessible by trusted systems even in sophisticated distributed web applications:

- For e-commerce payments subject to PCI DSS, Voltage SecureData Web helps merchants significantly reduce PCI DSS scope by up to 80% for the systems and applications that previously handled cardholder data.
- For both internal and external applications involving personally identifiable information (PII), personal health information (PHI) and electronic personal health information (ePHI).
- Voltage SecureData Web reduces the exposure of live information and simplifies compliance with privacy laws such as the EU's General Data Protection Regulation (GDPR), HIPAA, and state regulatory laws.

Key Benefits

- **Neutralize Breaches with End-to-End Datacentric Protection**—sensitive data is no longer exposed to hackers on web server infrastructure, networks and other systems between the browser and payment processor.
- **Deliver Rapid Compliance, Reduce PCI Audit Scope**—proven to reduce PCI scope by up to 80%. Voltage SecureData Web and Voltage SecureData Enterprise by OpenText require no token database, reducing scope, complexity, management and costs.

Voltage SecureData Enterprise

- **End-to-end data-centric security:** Voltage SecureData Enterprise neutralizes data breaches across the data lifecycle, securing data whether it is at rest, in motion or in use, by embedding protection in the data itself.
- **Data protection with usability:** Voltage SecureData Enterprise enables data protection while keeping da-ta usable for analytics and business processes. Data flows in its protected form without break-ing applications, databases, or hindering analytics.
- **Ease of implementation:** Voltage SecureData Enterprise provides a flexible range of native interfaces, REST and Simple APIs, to enable easy integration across applications and systems, from legacy databases to mobile, web, and IoT.

> **“Voltage Page-Integrated Encryption technology is a game changer. From an ecommerce standpoint, we would not have been able to become PCI–compliant without it unless we resorted to alternatives, which no one wanted to do from a usability or customer experience perspective.”**

Manager
System Security
U.S. Airline

Connect with Us
www.opentext.com

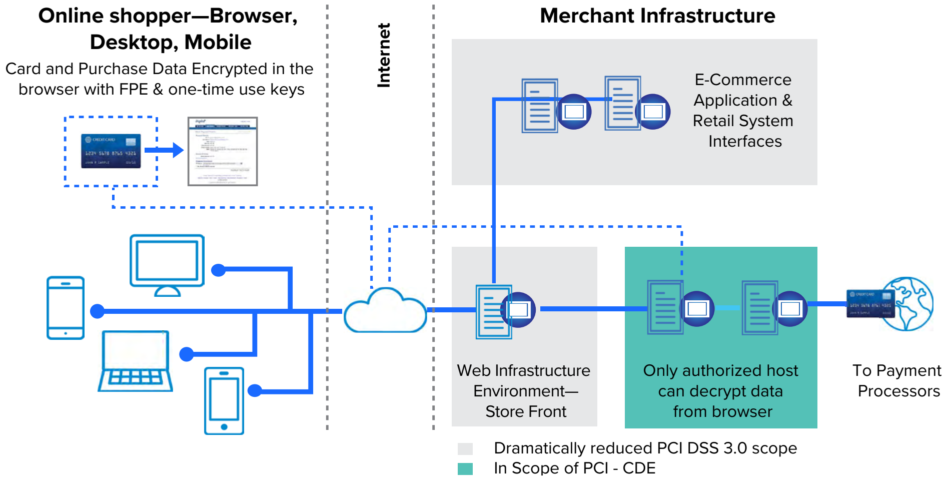
Online shopper—Browser, Desktop, Mobile
Card and Purchase Data Encrypted in the browser with FPE & one-time use keys
Internet
Merchant Infrastructure
E-Commerce Application & Retail System Interfaces
Web Infrastructure Environment—Store Front
Only authorized host can decrypt data from browser
To Payment Processors
Dramatically reduced PCI DSS 3.0 scope
In Scope of PCI - CDE

Figure 1. Online shopper through merchant infrastructure.

Key Features

- **Voltage Page-Integrated Encryption (PIE) by OpenText**—patented technology encrypts data directly in the browser the moment it is captured, using random single-use keys that are dynamically and transparently generated. Protected data can only be decrypted at the trusted host system at the destination.
- **Uncompromising security, seamless user experience**—designed to work in any browser whether on a laptop or a mobile phone, without browser add-ons or plug-ins. Data protection is transparent to end users, and eliminates page re-directs, disruption, or confusing workflows.
- **Preservation of data format and structure**—Voltage Format-Preserving Encryption (FPE) by OpenText permits policy information to be embedded into the encrypted data field while preserving the format and structure of the original data. For example, for credit card payments, this allows merchant access to the first 6 and/or last 4 digits of the credit card information for payment business processes, while protecting the sensitive digits from the browser to the payment processor.
- **Ease of deployment**—Deploys effortlessly, requiring as little as three lines of HTML code.

Learn more at
www.voltage.com

www.microfocus.com/data-encryption-security

opentext™ | Cybersecurity