

Voltage SecureData Enterprise

End-to-end data-centric security for the new data-driven economy



The Challenge in Data Security

The volume of data, the sophistication of ubiquitous computing and the borderless flow of data are outpacing the ability to understand how personal data is being used. In this data-driven economy, consumers find it hard to trust companies for a variety of reasons when it comes to the use of their personal data. For example, consumers' reaction to data misuse can cause them to reduce their spending with a company by about one-third.¹ Moreover, the number of cyber-attacks against enterprises and governments globally continues to grow in frequency and severity.

The findings in the Ponemon Institute Cyber Crime Study² suggest companies using encryption technologies are more efficient in detecting and containing cyber-attacks. According to the Ponemon Institute 2021 Cyber Crime Study² a typical data breach experienced by companies now costs \$4.24 million per incident when 1K–100K records are involved. That's the highest ever

recorded. So called “mega” breaches, when there's an exposure of 50M–65M records, now reach an average of \$401M to resolve.

However, according to the report, companies that employ security solutions based on artificial intelligence (AI), machine learning (ML), zero trust, analytics, and encryption all mitigated the potential cost of a breach. Organizations using high standard encryption (using at least 256 AES encryption, at rest and in motion), had an average total cost of a breach of \$3.62 million, compared to \$4.87 million at organizations using low standard or no encryption, a difference of \$1.25M or 29.4%.

Voltage SecureData Enterprise by OpenText offers an end-to-end data-centric approach to enterprise data protection. It is the only

1. Bridging the Trust Gap in Personal Data, BCG, March 2018
2. Cost of a Data Breach Report 2021, Ponemon Institute, July 2021

Highlights of Voltage SecureData Capabilities

- Protect ANY sensitive data, using an array of format-preserving data protection techniques to address compliance to privacy, payments standards and regulations, and data security needs
- FIPS 140-2 and Common Criteria validated solution; sensitive data is protected with NIST Standard FF1 mode of AES encryption, pioneered by OpenText
- Designed for compute-intensive demands and the explosion of data across multi-cloud, on-premises, and hybrid IT infrastructure
- Flexible range of interfaces including REST APIs, local client libraries, proxy and driver interceptors, and cloud-native functions for easier integration with broadest available range of databases, operating systems, applications, and platforms
- Integrations with services offered by all major cloud services providers such as Object Storage, Streaming services, Data Discovery, Data Warehouses, API Gateways, Serverless Compute (FaaS), managed Kubernetes services, KMS, Secrets Managers, and more.
- Highest availability and scalability with stateless software and HSM-based key derivation and management such as seamless key rotation, Bring Your Own Key (BYOK), etc.
- Integrated data discovery, analysis, and classification with Voltage Structured Data Manager by OpenText automates data protection and risk remediation

comprehensive data protection platform that enables you to protect data over its entire lifecycle—from the point at which it's captured, throughout its movement across your extended enterprise, all without exposing live information to high-risk, high-threat environments. That's the essence of data-centric security.

Voltage SecureData Enterprise provides a platform for protection of sensitive data at rest, in motion, and in use. Whether you implement one use case or hundreds, SecureData Enterprise can scale to meet any data protection requirement on premises and in multi-cloud hybrid IT. Voltage SecureData “de-identifies” data, rendering it useless to attackers, while maintaining its usability, usefulness, and referential integrity for data processes, applications, and services. Voltage SecureData Enterprise neutralizes data breaches by making your protected data absolutely worthless to an attacker, whether it is in production, analytic systems, or test/development systems, such as training and quality assurance.

A Unique Approach to End-to-End Data Protection

Voltage SecureData Enterprise is a unique, proven data-centric approach to protection—where the access policy travels with the data itself—by permitting data protection without changes to data format or integrity, and eliminating the cost and complexity of issuing and managing certificates and keys. As a result, leading companies in financial services, insurance, retail, healthcare, energy, transportation, telecoms, and other industries have achieved end-to-end data protection across the extended enterprise with success in as little as 60–90 days, because of the minimum, in most cases zero, impact to applications and database schemas.

Short Time to Success with Data Security

Most applications can operate using protected data without change. For those applications where sensitive data is first captured or live data is needed for controlled business purposes, Voltage SecureData

Enterprise can easily be used with virtually any system, ranging from decades-old custom applications to the latest enterprise programs. Powerful, centrally managed, policy-controlled APIs enable encryption and tokenization to occur on the widest variety of platforms, including but not limited to, OpenText™, Vertica™, NonStop, Teradata, IBM mainframe, Linux and other open systems, on-premises, hybrid, and all major clouds. APIs enable broad deployment into portfolios including ETL, databases and applications, network appliances, and API brokers, and Hadoop distributions. SIEM systems can take event data from Voltage SecureData for data governance reporting, activity monitoring, and audit.

Voltage SecureData Enterprise protects information in compliance with PCI DSS, HIPAA, GLBA, and global data privacy regulations including the GDPR, CCPA/CPRA, KVKK, POPI, and others. Voltage SecureData Enterprise is also compatible with PCI DSS requirements on Point-to-Point-Encryption (P2PE), enabling accelerated compliance and reduction in scope, time, and cost for PCI audits.

Key Benefits

Voltage SecureData Enterprise enables global organizations to manage risk, achieve regulatory compliance, and capture the benefits of digital transformation without increased exposure to a breach of sensitive data.

Industry Standard Format-Preserving Technologies

OpenText™ leads our industry as the patent holder and official licensor of the National Institute of Standards and Technology's (NIST) AES FF1 Format-Preserving Encryption (FPE) mode standard. The NIST standard provides an approved and proven data-centric encryption method for government agencies and has been adopted as the de-facto standard for global organizations. The NIST standard is critical in setting the bar to ensure organizations are maintaining regulatory and audit compliance, as well as using proven methods to protect against a data breach.

Voltage SecureData Enterprise is FIPS 140-2 and Common Criteria validated, and we continue to drive the industry forward with peer-reviewed work across numerous standards bodies and working groups.

The work OpenText™ Cybersecurity Voltage is doing with NIST, ANSI, IEEE, IETF, and independent security assessment specialists reflects our position of leader and trusted advisors to the world's largest financial services, banking and insurance organizations, retailers, manufacturers, telecoms providers, and payment processors.



STATELESS KEY MANAGEMENT: TRANSPARENT, DYNAMIC

Stateless Key Management securely derives keys on-the-fly as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. Stateless Key Management reduces IT costs and eases the administrative burden by:

- Eliminating the need for a key database, as well as the corresponding hardware, software, and IT processes required to protect the database continuously or the need to replicate or backup keys from site to site.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and via Web services.
- Maximizing the re-use of access policy infrastructure by integrating easily with identity and access management frameworks and dynamically enforcing data-level access to data fields by policy.

GDPR and similar privacy regulations are placing new pressure on global organizations to provide data-centric protection and policy as a service to their application and platform teams. Voltage SecureData de-identification and privacy protection of sensitive data including PII, PHI, and PCI, provides end-to-end data-centric security. Voltage SecureData delivers strong and flexible encryption to protect EU citizen's personal data and to follow pseudonymization guidance in the new GDPR.

Protecting high value data in government—Voltage SecureData has achieved the industry's first Federal Information Processing Standard FIPS 140-2, and Common Criteria, validation of Format-Preserving Encryption (FPE). Now, government agencies and private contractors serving government customers, can leverage the same powerful and proven technology that has transformed cybersecurity in the private sector.

ENCRYPTION AND TOKENIZATION

Traditional encryption approaches, such as AES 256 in CBC, GCM, CTR, etc., modes, have enormous impact on data structures, schemas and applications as shown in Figure 1. Voltage FPE is a tokenization method that uses the NIST-standard FF1 mode of the Advanced Encryption Standard (AES) algorithm, which encrypts sensitive data while preserving its original format without sacrificing encryption strength. Structured data such as Social Security Number, credit card, account, date of birth, salary fields, or email addresses can be protected without requiring changes to databases or impacting application functionality and performance.

Traditional encryption methods significantly alter the original format of data. For example, a 16-digit credit card number encrypted with AES produces a long alphanumeric string. As a result, database schema changes are required to facilitate this incompatible format. Voltage SecureData maintains the format of the data, so no database schema changes and minimal application changes are required. Tools for bulk encryption facilitate rapid de-identification of large



 Tax ID 934-72-2356		First name: Gunther Last name: Robertson SSN: 934-72-2356 DOB: 08-07-1966
FPE AES-FF1 mode	253-67-2356	First name: Uywjlqo Last name: Muwruwbp SSN: 253-67-2356 DOB: 08-07-1966
Regular AES-CBC mode	8juYE%Uks&dDFa2345^WFLERG	lja&3k24kQotugDF2390*32 0OWioNu2(*872weW Oiuqwriuweuwr%oLUOw1@

Figure 1. Format-Preserving Encryption (FPE) versus Regular AES Encryption

amounts of sensitive data in files and databases. Typically, whole systems can be rapidly protected in just days at a significantly reduced cost. Voltage SecureData allows accelerated encryption performance aligning to the high volume needs of big data, cloud analytics, and IoT, and supports virtually unlimited data types.

There are various types of tokenization:

- **Reversible**, which means a detokenization process exists (pseudonymization in privacy terminology)
 - **Cryptographic:** tokens generated from the data element using strong cryptography; the cleartext data element(s) are not stored, just the cryptographic key; Voltage SecureData offers Format-Preserving Encryption (FPE) for cryptographic tokenization
 - **Non-Cryptographic:** Stateless tokenization—randomly generated metadata containing data that is securely combined to build tokens; Voltage SecureData offers [Secure Stateless Tokenization \(SST\)](#) for non-cryptographic tokenization, offering high performance, security, and scalability
- Note:** Voltage doesn't offer a database vault-based tokenization, hence it eliminates the need for a token database or token vault, which is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. SST uses a set of static, pre-generated

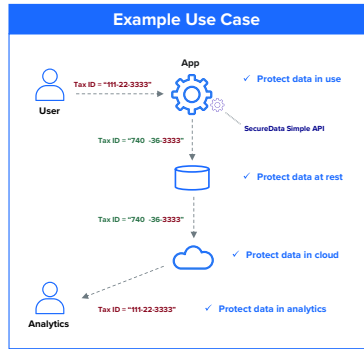
tables containing random numbers created using a FIPS random number generator. These static tables are used to consistently produce a unique, random token for each clear text PCI or PII input, resulting in a token that has no relationship to the original data. No token database is required with SST, thus improving the speed, scalability, security and manageability of the tokenization process over vault-based methods.

- **Irreversible**, which means it is not practical to convert the token back to the original value (anonymization in privacy terminology)
 - Tokens are created through a one-way function to anonymize data elements for third-party analytics, using production data in lower environments, etc.; Voltage SecureData offers Format-Preserving Hash (FPH) for irreversible tokenization

DATA ANONYMIZATION WITH VOLTAGE FORMAT-PRESERVING HASH

In specific use cases, such as click-stream analytics, the need to recover masked data may be an unnecessary risk, or may be explicitly undesired. Voltage Format-Preserving Hash (FPH) provides the same benefits as FPE—preserving the data's format and referential integrity—but with the added benefit of non-recovery of original data. This enables FPH to offer high-performance data usability—unlike traditional one-way transformation techniques, such as SHA-256—but in a non-disruptive and flexible approach.

Sensitive Data Types	Example Data in the Clear	Example Protected Data
Credit Card Number	1111-2222-3333-4444	1111-2287-9581-4444
Tax ID	111-22-3333	740-36-3333
Address	1234 Maple Street	7321 Uqhah Fbzir
Phone Number	415-555-1234	819-913-0471
Email Address	surfer1@mycompany.com	d8wLa2k@cPAzlu3la.8fq
Drivers License #	A1234567	P9162047
Date of Birth	20-12-1970	10-01-1956
Name	王秀英	樂魚扶的
IP Address	130.57.66.19	910.48.17.26
Geolocation	37.3974044, -121.9770816	81.7380129, -391.0193528
VIN	2W87Z7N139933	UV19PA07CBL13
Treatment Code	81082	81XXX



Connect with Us
www.opentext.com

Figure 2. SecureData protects the world's most sensitive data

SECURE AND COMPLIANT TEST DATA MANAGEMENT

For test data management use cases, Voltage SecureData de-identifies production data and creates structurally valid test data so developers or users can perform QA or conduct data analysis—all without exposing sensitive data. The Voltage SecureData Enterprise management console enables easy control of policy and provides audit capabilities. Voltage Structured Data Manager (SDM) enables complete management of structured data across its lifecycle. SDM can discover sensitive data in on-premises, cloud, or hybrid systems and classify in-scope data for disposition, defining archival, protection, deletion, or any other disposition based on company policy. The integration of Voltage SecureData Enterprise with Voltage SDM automates test data management, supports privacy compliance, and secures sensitive data in test and analytics use cases.

Note: OpenText Voltage Partners and Professional Services are available to help clients scope projects, combat advanced threats, reduce compliance burden, and quickly solve difficult data privacy challenges. **VOLTAGE SECUREDATA ARCHITECTURE** Voltage SecureData platform provides flexible deployment options to ensure high availability and performance across multi-cloud hybrid IT infrastructure. Whether you prefer to deploy virtual appliances, or cloud-native, containerized microservices running within Kubernetes clusters, you'll be able to scale SecureData to meet the most demanding enterprise requirements.

This enables Voltage SecureData Enterprise customers to choose an appropriate combination of techniques to address their use cases, across diverse environments, while avoiding the costs and complexities of deploying and managing multiple products.

“We are fully compliant with the latest financial services regulations and thanks to Voltage SecureData [Enterprise] we achieved this in a minimally invasive manner, without having to change our existing infrastructure. We protect our sensitive data very cost-effectively in a complex and distributed environment.”

Christian Stork
Head Strategic Projects
SIX

VOLTAGE SECUREDATA SENTRY—TRANSPARENT DEPLOYMENT ACCELERATES TIME-TO-VALUE With migration to hybrid IT and an increasing reliance on SaaS applications, organizations may not have the accessibility or development resources for API-level integration. Voltage SecureData Sentry by OpenText enables transparent data protection by intercepting sensitive data flowing through the network. Voltage SecureData Sentry simplifies hybrid IT migration, accelerates time to value by quickly enabling security compliance, and offers consistency for end-to-end data protection, without having to break open applications and extensively re-qualify IT architectures.

Learn more at www.microfocus.com/en-us/cyberres/data-privacy-protection/securedata-enterprise

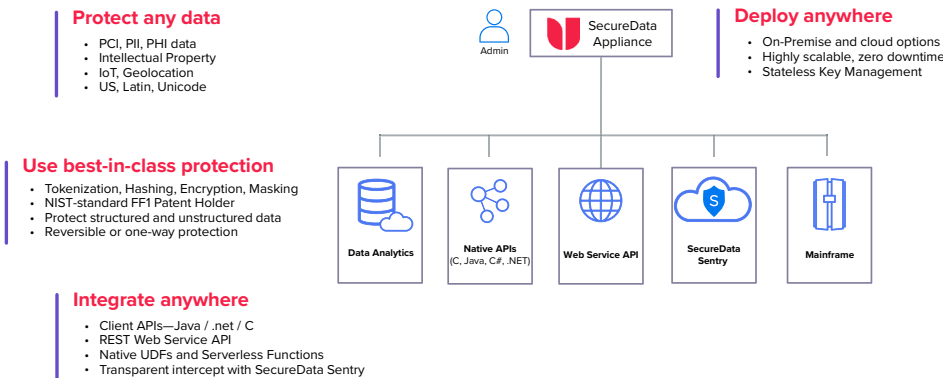


Figure 3. Voltage SecureData Architecture

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.