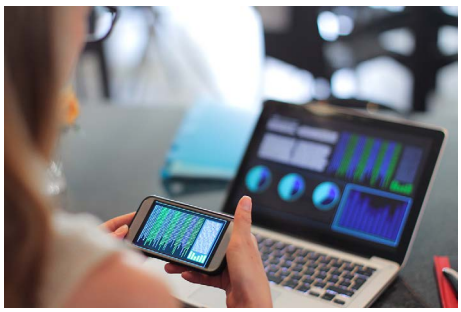
Secure Cloud Analytics

Accelerate cloud migration with Voltage for Cloud Analytics and unlock the potential of secure data analytics at scale with data privacy by design.

Cloud Analytics Enabling Capabilities Include:

- 100% cloud-native protection enables high-scale secure cloud analytics
- Deterministic, field-level protection travels with sensitive data, preserves data usability
- Centralized key management delivers continuous multi-cloud data security
- Provides flexibility to securely integrate broad range of native CDW and CSP datastores
- Integrated data discovery and classification to automate remediation and risk reduction



The Cloud Analytics Market size is set to grow from USD 23.2 billion in 2020 to USD 65.4 billion by 2025, according to a market research report published by MarketsandMarkets.[1] Companies are increasingly shifting their workloads and sensitive data into the cloud, transforming their IT environments to hybrid or multi-cloud. *Why this shift?* The cost-effectiveness, elasticity and large amounts of services provided by cloud solutions enable organizations to get more value from monetizing their rapidly expanding data volumes in these large-scale environments. However, with this trend accelerating, privacy and security remain the primary concerns. With customer data flowing from or to other cloud services or cloud platforms, cloud misconfigurations have become the leading cause of breaches. With a data breach's average cost reaching over $4 million per incident, this remains a board-level concern.

Voltage for Cloud Analytics helps customers reduce the risk of cloud adoption by securing sensitive data in cloud migration and safely enables user access and data sharing for analytics. The tokenization technologies in Voltage SecureData help customers comply with privacy requirements by discovering and protecting regulated data at rest, in motion and in use in cloud warehouses and applications. These solutions also minimize multi-cloud complexity by centralizing control with data-centric protection that secures sensitive data wherever it flows across multi-cloud environments.

Voltage Products that Reduce Multi-Cloud Complexity

Voltage SecureData for Cloud Data Warehouses

The integration of Voltage SecureData with cloud data warehouses (CDWs), such as Snowflake, Amazon Redshift, Google BigQuery, and Azure Synapse, enables Voltage customers to conduct high-scale secure analytics and data science in the cloud using format-preserved, tokenized data that mitigates the risk of compromising business-sensitive information while adhering to privacy regulations.

In addition, SecureData's advanced tokenization technologies that permit the pseudonymization and anonymization of any structured data type, in any quantity required, across all languages, promote data sharing and mobility without requiring the data to be unprotected and reprotected at

1. Cloud Analytics Market by Solution (Analytics Solutions, Hosted Data Warehouse Solutions, and Cloud BI Tools), Deployment Mode (Public Cloud, Private Cloud, and Hybrid Cloud), Organization Size, Industry Vertical, and Region—Global Forecast to 2025, MarketsandMarkets, September 2020

Figure 1. Voltage SecureData for Cloud Data Warehouses

each technology border crossing. In a multi-cloud enterprise landscape, SecureData removes the security gaps between different CDWs, cloud services, query tools, business intelligence platforms, SaaS applications, and cloud service providers.

Voltage SecureData Sentry for SaaS, COTS, and in-House Applications

Voltage SecureData Sentry specializes in data protection for cloud software services as well as for on-premises applications. It extends the reach of Voltage data protection technologies to SaaS applications, such as Salesforce, ServiceNow, ALM Octane, and Microsoft Dynamics 365, as well as to commercial off-the-shelf (COTS) applications. Moreover, through additional innovations, such as secure local indices supporting partial and wildcard search terms, and secure email address formatting for SMTP relaying, Sentry preserves application functionality that is impacted by competing solutions. Sentry uses dataflow interception techniques to protect sensitive data flowing through the network, ensuring organizations remain in control of the security of their data used in SaaS and COTS applications that cannot be directly integrated with SecureData.

Reduce the Risk of Cloud Adoption with Voltage

The tokenization technologies in Voltage SecureData provide flexible implementation and protection for a virtually unlimited number of structured data types in any language, and any region, with proven performance and scalability. Voltage Format-Preserving Encryption (FPE), Format-Preserving Hash (FPH), and Secure Stateless Tokenization (SST) enable enterprises to de-identify sensitive information in ways that neutralize the effects of a data breach, but permit continued use of the data in its protected state in applications and analytics platforms. Voltage tokenization technologies maintain the context and meaning of the data—such as its referential relationships, logic, and business intent—in its protected form, ensuring that businesses can minimize requirements to decrypt. The preservation of referential integrity also enables protected data to be reliably referenced and joined for cross-cloud analytics, providing key insights through identifiers, such as phone numbers or IDs, common across disparate data sets.

Voltage Technologies Support Privacy Compliance in the Cloud

DATA PSEUDONYMIZATION WITH VOLTAGE

Voltage FPE, a mode of the Advanced Encryption Standard (AES), is a fundamental innovation which enables SecureData for Cloud Analytics to provide high-strength, robust data encryption, while maintaining flexibility for use. An implementation of the FF1 method as presented in NIST SP 800-38G[2], Voltage FPE is a cryptographic standard that provides the pseudonymization necessary to enable compliance with data privacy regulations at data field and sub-field levels, while simultaneously enabling organizations to run business processes and analytics on protected data sets.

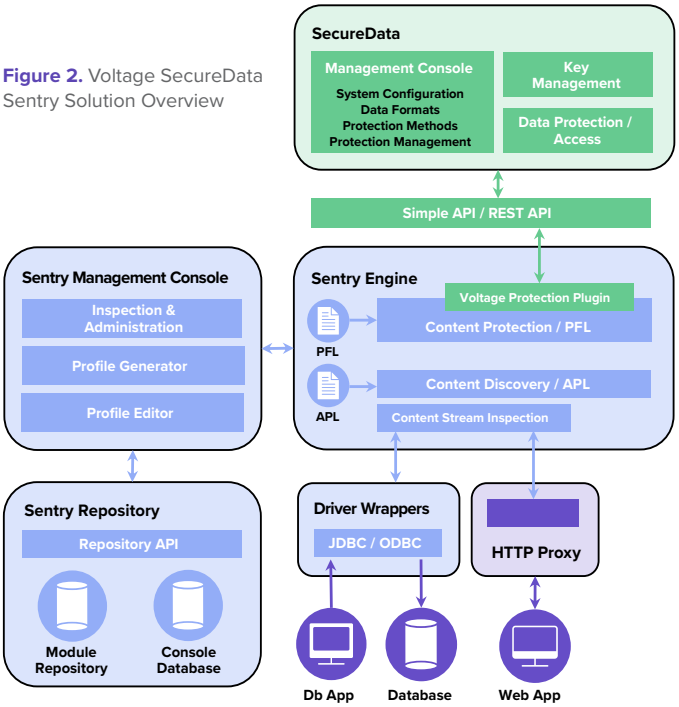


Figure 2. Voltage SecureData Sentry Solution Overview

Voltage Secure Stateless Tokenization (SST) is an advanced, patented, data security solution that helps assure protection for payment card data on premises or in the cloud. Voltage SST eliminates the token database and removes the need for storage of cardholder or other sensitive data,

2. National Institute of Standards and Technology (2016) Special Publication 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption

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 Uqhap 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	樂魚快的
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

Any structured data, any language...

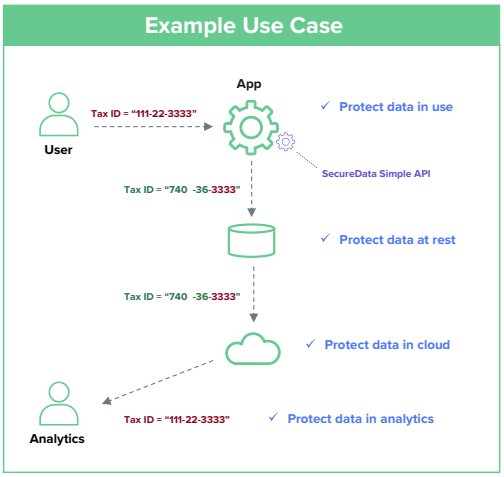


Figure 3. SecureData protects the world's most sensitive data

enabling a vast reduction in the scope of a PCI-DSS compliance audit, for example. By using a set of static, pre-generated tables to consistently produce a unique, random token for each data value, such as a Primary Account Number (PAN), the speed, scalability, security, and manageability of the tokenization process is optimized.

DATA ANONYMIZATION WITH VOLTAGE

In specific use cases, such as enabling secure and compliant test data management, the ability to recover data may present an unnecessary risk or be explicitly undesired. Voltage Format-Preserving Hash (FPH) offers full data anonymization but with the same benefits of other Voltage tokenization technologies regarding structure, logic, partial field application, and usability for some use cases, such as click-stream analytics. FPH employs a non-disruptive and more flexible one-way, irreversible transformation that enables high-performance data usability, unlike traditional anonymization techniques such as SHA-256.

VOLTAGE STATELESS KEY MANAGEMENT

Voltage Stateless Key Management is the cornerstone of Voltage simplicity and scalability. Keys are derived dynamically as required, with no key database to store, protect, backup, or to integrate with traditional key management solutions. Enterprises do not need to manage keys, certificates, or databases, eliminating the hardware, software, and IT and personnel processes and costs required to continuously protect key databases on-premises, in off-site back-ups, or even in the cloud. Voltage Stateless Key Management maintains an organization's complete control over their encryption keys while enabling low-cost, high-performance, highly available data protection that scales to protect the sensitive data of the world's largest financial services companies, telcos, payment processors, and other global enterprises and government agencies.

EVOLUTION OF HARDWARE SECURITY MODULES TO CLOUD ENVIRONMENTS

Where Voltage SecureData is used to migrate storage and workloads to cloud-based environments, an HSM-based root of trust in the cloud may be important. nShield as a Service from nCipher Security, a certified Voltage alliance partner, supports Voltage Stateless Key Management, and is a subscription-based, FIPS 140-2-certified nShield HSM solution for generating, accessing, and protecting cryptographic key material separately from sensitive data. This cloud-hosted model gives organizations the option to supplement or replace HSMs in their data centers.

Protecting Data and Enabling Analytics in the Clouds

Low-cost data storage combined with elastic computation and an ever-increasing range of data analytics services are succeeding in shifting the balance of big data deployments from on-premises to the cloud. But the external hosting of sensitive data carries additional security responsibilities and serious risks. Under the shared responsibility model, cloud providers will ensure that the hardware and software services they offer are secure, but customers are responsible for the security of their own assets.

Through ensuring that data is simultaneously protected and useable by cloud applications and services in its protected form, Voltage SecureData for Cloud not only eliminates the risk of data breaches introduced

“With reduced IT resources due to the pandemic, this customer needed to find a way to deal with sensitive data before moving it into the Snowflake Data Cloud. Using Voltage SecureData enabled them to use a single technology to address data protection across their hybrid IT environment and comply with evolving privacy requirements.”

Solution Architect

Contact us at **CyberRes.com**
Like what you read? Share it.

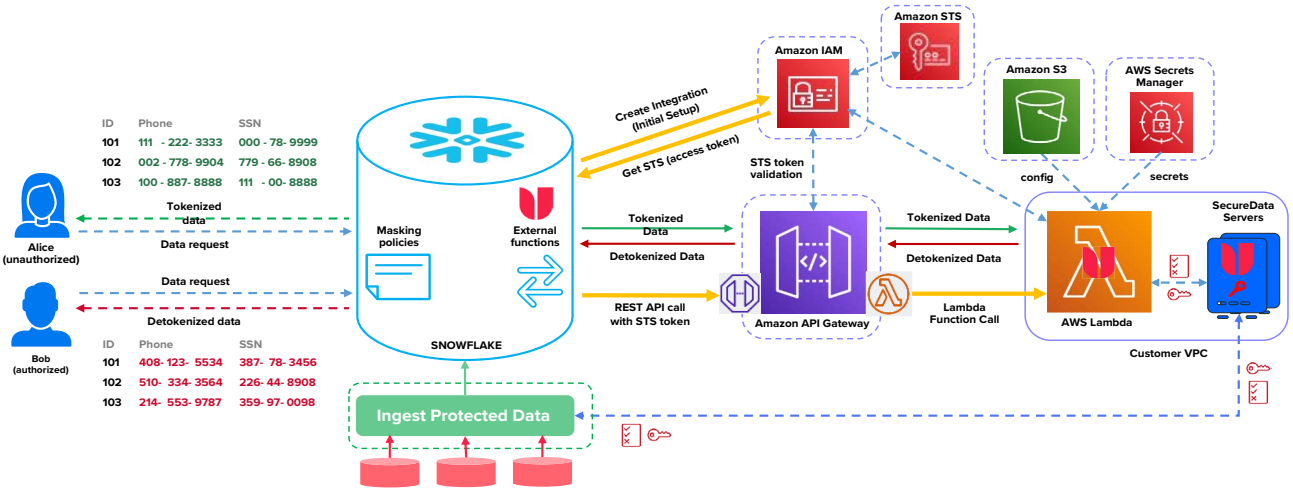


Figure 4. Voltage SecureData for Snowflake Solution Overview

through missing or misconfigured security controls but also enables the adoption of a continuous data protection model in multi-cloud environments through removing the need for in-cloud decryption. While data is being moved to the cloud, it needs to be persistently protected across its life cycle, at ingestion, at rest, and while in use.

Voltage SecureData for Cloud can be integrated with:

- Cloud ETL services, such as AWS Glue, Azure Data Factory, and Google Data Fusion, as well as other COTS ETL tools such as Informatica, Talend, DataStage, Ab Initio, and others.
- Streaming platforms, such as Kafka, NiFi, Storm, Streamsets, and Cloud streaming services such as AWS Kinesis, Azure EventHubs, Google Dataflow, and others.
- Data lake services, such as AWS Simple Storage Service (S3), Azure Blob storage, Google Cloud Storage, AWS RedShift, Azure Databricks, Azure SQL Data Warehouse/Synapse Analytics, Google BigQuery, AWS EMR, Azure HDInsight, Google Dataproc, Snowflake *(see Figure 3)*, and others.
- SQL and NoSQL database services, such as AWS RDS, Aurora, and DynamoDB, Azure SQL Database, Cosmos DB, Google Cloud SQL, and others.

Additional capabilities include:

- Voltage transformation on serverless compute services or Functions as a Service (FaaS), such as AWS Lambda, Azure Functions, and Google Cloud Functions, AWS Macie, AWS API Gateway, Google Data Catalog, Google Apigee, Azure Data Catalog, API Management, and others.

In summary, the mobility of data protected by Voltage SecureData is unconstrained: data remains protected while flowing from or to other cloud services or cloud platforms. This approach supports a multi-cloud strategy and data sharing requirements without requiring organizations to compromise on data security at the boundaries of these services. And with Voltage SecureData, customers always remain in complete control of their encryption keys and token tables, from the master keys down to the data encryption keys themselves, all in a stateless system that imparts no additional storage or management overhead. All these technologies accelerate cloud migration and allow customers to unlock the potential of their data at scale with privacy by design.

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

761-000068-001 | M | 11/21 | © 2021 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

CyberRes
A Micro Focus Line of Business