

Voltage SecureData Cloud

Faster time-to-value with data security assurance in the cloud—for Microsoft Azure and Amazon Web Services (AWS)

Product Highlights

The speed of business and competitive agility demand that more application workloads be spun up in the cloud to accelerate time-to-value. However, through efforts to achieve faster results, enterprises must ensure that their security posture, both on-premises and in the cloud, is transparent and consistent in approach—without creating new challenges to sensitive data as it’s moved outside of enterprise perimeters.

Current system and application-centric security controls embedded throughout existing IT infrastructure don’t extend to the cloud, creating risks when data is moved to a public, untrusted environment. Monolithic applications and associated security aren’t designed for the cloud, which requires a continuous integration and continuous development DevOps model.

Embed Protection into the Data

As organizations embrace the values of cloud computing, this opportunity comes with the trade-off of introducing potential new threats to data security. Data protection must be fundamentally embedded into the data itself in order to scale along with workload elasticity, while remaining agnostic to the platform where it may reside. IT leaders want to say “yes” to keeping sensitive data open to new business opportunities, not slow down cloud agility—but they need to do so safely.

Voltage SecureData Cloud: Trusted Security Assurance in Azure and AWS

Voltage SecureData Cloud for Microsoft Azure and Amazon Web Services (AWS) accelerates an organization’s ability to adopt hybrid IT infrastructure safely. The virtual appliance

solution enables organizations to seamlessly protect data, consistently between on-premises IT and the Azure or AWS cloud.

SecureData Cloud offers a platform-agnostic approach to data protection using a stateless key management architecture with data encryption that enables high-performance scalability for the elasticity required by modern cloud applications. SecureData Cloud is a fully cloud-native solution where applications, data and the security software appliance (SecureData Enterprise) interoperate, both on-premises or in the cloud, to enforce end-to-end data lifecycle protection.

Key Benefits

High Scalability and Agility without Compromising Data Protection

SecureData Cloud scales easily with applications hosted in AWS and Azure, allowing enterprises to quickly deploy the cloud while incorporating best-in-class data security. The software easily handles the demands of applications and data volumes, for example, adopting capacity on demand for Hadoop in cloud-transient workloads. This enables enterprises to realize the promise of reducing or eliminating on-premises hardware costs by deploying cloud-native applications to take advantage of cloud efficiencies.

SecureData Cloud can support multi-cloud environments in Microsoft Azure, AWS, hybrid cloud and on-premises environments such as z/OS, Linux, Windows, Stratus VOS and Non-Stop through the SecureData product family. SecureData Cloud integrates with AWS Key Management Service (KMS), and with Azure Key Vault, to add an additional layer of security for key material.

Voltage SecureData Cloud for Azure and AWS Enables Organizations to:

- Accelerate new cloud business models leveraging proven data-centric security for safe deployment of application workloads
- Embed data-centric security across on-premises and hybrid cloud IT with a single, consistent management view
- Adopt platform agnostic data protection for greater flexibility with highly-elastic applications that scale securely over time
- Support multi-cloud, hybrid cloud and on-premises environments through the Voltage SecureData product family
- Achieve fast time-to-integration with cloud-based SecureData Cloud setup for developers
- Protect data stored in AWS and Azure Storage with the same reliable approach as on-premises

Voltage SecureData Cloud: End-to-End Data Protection in Hybrid IT

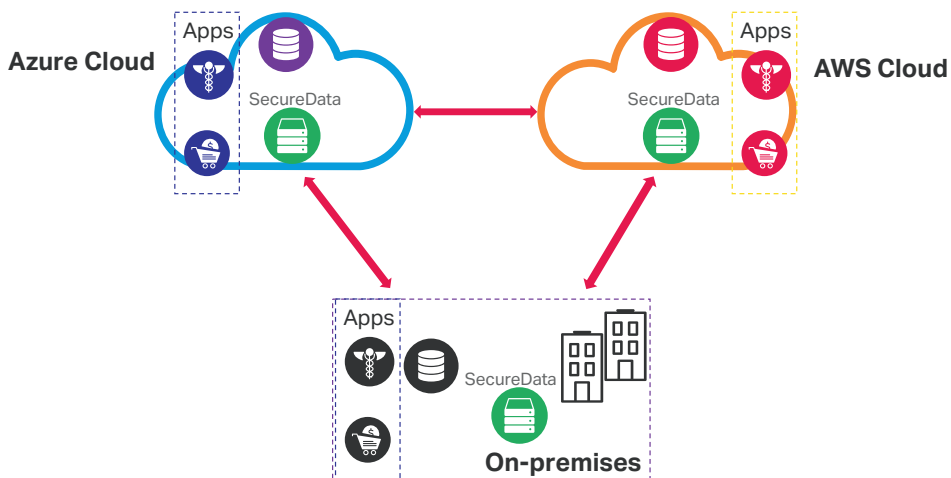


Figure 1. Voltage SecureData Cloud offers security assurance in the cloud and end-to-end protection for data on hybrid cloud and on-premises systems in combination with the SecureData product family.

Data Protection without Compromising Usability

SecureData Cloud for Azure and AWS secures sensitive data using Hyper Format-Preserving Encryption (FPE), an advanced and proven technology that enables protected data to be used for business processes and analytics. Voltage Hyper FPE protects data while maintaining data context and meaning, such as relationships, logic and business intent in the protected data. Hyper FPE enables organizations to run more business processes and analytics on protected data sets and only rarely expose sensitive data, depending on use case.

Hyper FPE is a fundamental Voltage innovation, enabling SecureData Cloud to provide high-strength, robust data encryption, while maintaining flexibility for use. Hyper FPE supports applications, analytic processes, and data repositories when using protected data with the vast majority of use cases—across distributed IT systems, platforms, and tools. Protection is applied at the field or partial-field level over sensitive data, leaving non-sensitive portions of fields available for applications. Hyper FPE preserves referential integrity across data sets so protected data can be reliably referenced and joined for cross-cloud analytics. For example, this is critical when common identifiers, such as phone numbers or IDs, are used across disparate data sets.

Voltage pioneered and implemented the AES-FF1 encryption method per the NIST SP-800-38G FPE standard that Voltage authored.

Key Features

Compliance in the Cloud

With the shared responsibility model of the cloud, maintaining compliance initiatives—PCI DSS, GDPR, HIPAA/HITECH and state/local/regional/industry mandates—can be achieved through a unified data security approach, providing a complete end-to-end data-centric solution. SecureData Cloud enables data privacy and compliance, while supporting business processes by de-identifying, encrypting, tokenizing, and pseudonymizing data, enabling organizations to run mission-critical applications in AWS and Azure clouds. By de-identifying data in the cloud, SecureData Cloud enables enterprises to meet data residency requirements and meet compliance audits.

Consistent Data-Centric Security Assurance to Quickly and Safely Deploy New Applications in the Cloud

The key to a safe enterprise migration to the cloud is to embed data security consistently and seamlessly to span across legacy and hybrid IT, allowing data to flow securely across environments. SecureData Cloud for Azure and AWS simplifies deployment of a trusted IT architecture where data, applications and workflows can run on-premises and in the cloud, dynamically. SecureData Cloud for Azure and AWS accelerates the enablement of new business models, leveraging safe deployment of flexible workloads, enabling high-speed, responsive approach to business initiatives, while protecting the data that matters most.

Contact us at:
www.microfocus.com