Data Security Solutions

Micro Focus® Data Security solutions enable advanced format-preserving encryption, secure stateless tokenization, and stateless key management to protect enterprise applications, data processing infrastructure, hybrid IT/cloud, payment ecosystems, mission-critical systems, storage, and Big Data/IoT platforms.

Key Solutions:
- Scaling Big Data Security
- Reducing High Cost of Compliance
- Securing Workloads to the Cloud
- Hardware-Based Trust Assurance
- Secure Enterprise Messaging

What We Do:
- Format-Preserving Encryption
- Secure Stateless Tokenization
- Stateless Key Management
- Hardware Security Modules and Appliances

Why We Help:
- Neutralize breach impact through data de-identification
- Enable usable protected data for applications and analytics
- Extend data security from legacy to hybrid IT without gaps

Micro Focus Data Security drives data-centric security innovation with encryption and tokenization solutions. We enable the world’s leading brands to neutralize data breach impact for data at rest, in motion and in use by de-identifying sensitive information. Data Security solves the industry’s biggest challenge by simplifying data protection across complex legacy and modern IT.

Solutions

Scaling Big Data Security
Hyper FPE protects data streaming into data lakes with high performance, enabling analytic insights while lowering exposure to data misuse or breach. Safer, de-identified data can now offer wider access to business leaders and operations teams to accelerate new value creation and IT optimization without increasing risk as data volumes scale.

Reducing High Cost of Compliance
Data is de-identified using a proven, standards-based approach that can meet GDPR and similar mandates for data pseudonymization and anonymization. Format-preserving encryption and hash avoids breaking applications and processes, extending to legacy and hybrid IT. Secure Stateless Tokenization enables audit scope reduction, proven for PCI DSS, in use by leading banks, retailers and payment processors.

Securing Workloads to the Cloud
SecureData cloud-native data protection for application workloads extends from hybrid IT to include legacy on-premises systems using a consistent single pane of glass approach.

SecureData enables a platform-agnostic approach to deploying IT that transcends boundaries with a stateless architecture and transparent gateways using SecureData Sentry.

Hardware-Based Trust Assurance
Atalla HSM and Enterprise Secure Key Manager (ESKM) offer hardened security appliances, validated to NIST FIPS 140-2 security assurance, for protecting cryptographic material used in high-trust applications, including payments applications, and storage and server media key management. Atalla HSM integrates with SecureData software appliances to enable hardware-based root of trust for protecting cryptographic secrets.

Secure Enterprise Messaging
End-to-end encrypted email for desktop, cloud, and mobile that scales to millions of users, while maintaining sensitive data (PII, ePHI, etc.) privacy. Secure communication enables organizations to confidently meet privacy compliance mandates, while lowering exposure to misuse and data breach impact resulting in data loss, fines and remediation.

Products

Voltage SecureData Enterprise
End-to-end protection using Hyper FPE and tokenization for complete data-centric security to neutralize data breach impact from point of data creation throughout the information lifecycle—in use, in motion, at rest.
- Delivers high-scale transaction performance to secure data ingestion, processing, storage and similar solutions
- Meets regulatory compliance for scope reduction, while lowering implementation and management costs
- Spans legacy to modern hybrid IT for an approach that extends to new applications seamlessly

**Voltage SecureData Payments**
Point-to-point encryption and tokenization for PCI compliance and payments security from POS capture to card processor.
- Protects credit card data end-to-end, at rest and in transit, within the digital payment ecosystem
- Reduces PCI scope without changing mission-critical business processes and workflows
- Provides complete point-to-point encryption (P2PE) and tokenization for retail payment transactions

**Voltage SecureData for Hadoop and IoT**
Enables protection of sensitive data in use for Hadoop and IoT (Kylo, Apache NiFi).
- Protects data at the edge for safe ingestion into data lakes and warehouses at high scale
- De-identifies data while maintaining usability for Big Data applications and analytic insights
- Limits exposure to specific data fields, applications and users to reduce risk and neutralize breaches

**Voltage SecureData Cloud**
Cloud-native approach to securing data in application workloads with consistency when migrating from legacy to hybrid IT.
- Deploys data protection in the cloud to accelerate time to value for securing application workloads
- Enables hybrid (cross) cloud analytics with platform-agnostic control over keys independent of data locations
- Extends across hybrid IT with transparent gateways for a single pane of glass management approach

**Voltage SecureData Sentry**
Transparent encryption using an advanced CASB approach to simplify security deployment and accelerate time to value.
- Delivers a transparent approach to minimize disruption and risk to legacy environments
- Implements application security faster vs API to simplify development across wide-ranging applications
- Extends next-generation CASB support for use cases across SaaS/cloud, enterprise, COTS, legacy and beyond

**Edge Protection with SecureData**
Voltage SecureData Mobile protects data captured on device endpoints and Voltage SecureData Web uses Voltage Page Integrated Encryption (PIE) to secure sensitive data from Web browsers.
- Enables omni-channel protection and unified eCommerce security across digital payments systems
- Helps merchants reduce PCI DSS scope from transactions across mobile and Web endpoints
- Accelerates development using simple, native libraries for iOS and Android applications

**Voltage SecureMail**
Global enterprise mail encryption for employees and mobile users extending to customers and partners.
- Provides a single approach to desktop, cloud, and mobile email and attachment protection
- Scales using stateless key management with standards-based Identity-Based Encryption (IBE)
- Allows flexible hybrid IT deployment on-premises or in the cloud via SaaS offering

**Atalla HSM**
Leading FIPS 140-2 Level 3-validated hardware security module to protect cryptographic material and enable card authentication.
- Meets highest government and financial industry standards for trust assurance
- Provides secure, high-performance and scalable financial transaction processing
- Sets the bar for superior remote management and key protection

**Enterprise Secure Key Manager (ESKM)**
Cryptographic key management to protect storage and server media infrastructure, supporting the OASIS KMIP standard.
- Supports KMIP-interoperable solutions using a FIPS 140-2 Level 2 hardened appliance
- Enables high-availability protection of media for disk array, tape library, and related IT
- Unifies enterprise key management by protecting keys across global applications

Learn More At https://software.microfocus.com/software/data-security-encryption