MICRO FOCUS

Data Sheet
Security

Voltage SmartCipher

Simplifying unstructured data security

Product Highlights

Global data volume is growing exponentially to 163 zettabytes by 2025, ten times more than in 2016*. It is estimated that 80% of this data is composed of unstructured data in all kinds of files—anything from a document to a video. But among these zettabytes of data, there are potentially trillions of files containing sensitive information that need to be protected. However, files can't stay locked away in encrypted storage repositories. In order to generate business value, internal and external users must continuously share files across multiple platforms for collaboration, which creates significant challenges for file protection.

Platform-specific security does not typically extend beyond the host collaboration platform, and most Information Rights Management (IRM) solutions are dependent on platform OS or application integrations. That means security policy can't travel with the file, leaving the file either unusable or vulnerable. Enterprises also need to discover and classify files containing sensitive data and apply protection policy automatically and continuously, to accelerate protection and stay ahead of constant business change.

All of these concerns increase the complexity of managing sensitive data files and the risk of a damaging data breach, along with the possible fines and remediation from increasingly strict data privacy regulations. The exponential growth in the uncontrolled dissemination of sensitive files represents the biggest challenge that information security professionals face. Enterprises need a new approach to simplify privacy controls that protect sensitive data.

** Data Age 2025: Don't Focus on Big Data; Focus on the Data That's Big, IDC, April 2017*

Quick View

- Simplifies unstructured data management by embedding files with access and use controls that persist across the data lifecycle.
- Increases visibility and control over sensitive file access, use, and disposition with centralized policy control.
- Reduces risk of a data breach by encrypting and wrapping security policy that travels with files to protect them wherever they go.
- Improves compliance audit and inquiry response with real-time discovery, classification, monitoring, and reporting on files for sensitive data usage and creation.
- Accelerates Hybrid IT adoption by enabling secure collaboration across platforms with no changes to applications or OS.
- Enables seamless implementation with non-disruptive modes of operation for fast time to value.
- Provides a comprehensive information lifecycle security solution for data privacy together with the Micro Focus security, risk, and governance solution portfolio.
- Satisfies "cloud first" approach with IaaS Azure hosted deployment model and at same time meets data residency requirements by deploying into regional Azure datacenters.
- Expands privacy and security with SecureMail integration by encrypting and inspecting email content and attachments with SmartCipher policies.
- Gain visibility of end user activity including sensitive content usage and policy violations.
- Enables integration with automation, workflow, and 3rd party products such as DLP as well as laying the foundation for Micro Focus portfolio products with the integration framework.

Voltage SmartCipher Simplifies Unstructured Data Security

SmartCipher simplifies unstructured data security, delivering control over the use and proliferation of sensitive files for secure collaboration and improved privacy compliance. It provides persistent file protection, and complete control and visibility, over file usage and disposition across platforms. Files are transparently encrypted and embedded with access and use controls that protect files wherever they go, enforced by centralized policy management for real-time monitoring, discovery, and classification.

SmartCipher enables enterprises to manage access and use policy centrally from a single pane of glass and enforce it remotely at a file level. SmartCipher allows enterprises to expose information safely to create business value by protecting the privacy of unstructured data.

Key Features

Secure Collaboration across Environments

SmartCipher's unique patented Transparent File Encryption technology embeds access and protection policy around individual files and the data within, persistently protecting files. Transparent File Encryption technology wraps the file with strong AES256 encryption to help prevent unauthorized access to contents or policy while allowing policy updates from the central console.

Transparent File Encryption enables protected files to remain agnostic to the operating system, applications, and user, securing them across any collaboration platform, including email and cloud-hosted environments such as Microsoft One Drive, Dropbox, Box, and others.

Increase Visibility and Control with Centralized Policy Management

SmartCipher increases visibility and control over sensitive files with centralized access and use policy managed centrally and enforced locally at a file level. It gives enterprises a simple-to-construct, but highly flexible, policy creation framework that covers who has access to files, and how can they interact with a file, from a single pane of glass. New policies can be dynamically implemented and synchronized with files on endpoints or collaboration platforms.

Improve and Accelerate Compliance Audits and Inquiries with Real-Time Monitoring, Discovery, and Classification

SmartCipher has built-in file usage monitoring and alerting, allowing enterprises to determine when, where, and how each file is accessed and altered, and by whom, to provide broad control and protection over unstructured data. Automated discovery inspects files during creation, in use, or at rest, to analyze content with the use of filters that can interpret content and metadata.

File classification is based on content rules, dictionaries or regular expressions. Existing dictionaries can be edited, and new ones can be created to accommodate the needs of specific industries and geographies. Classification can also be performed contextually based on file location, user profile, or other variables. Files can be automatically located and classified dynamically, as they are created, with the use of a crawler that continually monitors the network for files created that contain sensitive content.

Seamless, Non-Disruptive Implementation

SmartCipher may be implemented in stages, according to the needs of enterprises, allowing administrators to map file location and roll-out file protection without disruption.

SmartCipher and SecureMail Integration—Better Together

Email is a common collaboration platform that handles a significant amount of unstructured data. This data is in-transit and at rest at both the server side (Exchange) and endpoint client (Outlook). SmartCipher content inspection policies can now be applied to e-mail address, subject, body, and attachments.

The SmartCipher and SecureMail integration delivers full policy-based content inspection to e-mail and attachments using the same policy engine as the rest of the SmartCipher unstructured data policies.

This solution provides persistent and transparent encryption directly to the file attachments, protecting the attachments even after saved at the recipient side. Without SmartCipher these attachments would no longer be protected upon save from SecureMail.

Contact us at:
www.microfocus.com

Like what you read? Share it.

A Comprehensive Set of Solutions for Privacy Protection

SmartCipher adds unstructured data protection and management to an industry-leading Micro Focus portfolio of security, risk, and governance products and solutions. Businesses can comprehensively manage and secure information, detect and respond to data breaches, and enforce identity and access controls. Products and solutions in the portfolio include:

- **Voltage File Analysis Suite**—Unstructured data governance and advanced file analysis.
- **Data Discovery**—SaaS-based file analysis on all of your unstructured data.
- **Data Privacy Manager**—Structured data management and protection across the data lifecycle.
- **NetIQ**—Identity and access management policies enforced across local, mobile and cloud environments.
- **Fortify**—Application security on-premises and on-demand for the entire software development lifecycle.
- **ArcSight**—Real-time threat detection, analytics, and investigation from any source, anywhere.

Whether complying with privacy regulations, such as GDPR or CCPA, or extending data privacy during collaboration in the cloud for consistency, SmartCipher and the Micro Focus portfolio protect sensitive data with granular privacy controls for users, applications, and data to reduce privacy-breach risk through a multi-layered, multi-vectored approach.