SECUREMi®

Protect your sensitive data

SECUREMi®

DATA SHEET

Comprehensive solution

SecureMi is a comprehensive enterprise content-aware data leakage prevention solution that is designed to prevent data leakage in government and corporate. It can classify your sensitive data and discover, monitor and protect your classified data wherever it is stored or used, across networks, storage and endpoints. It can identify sensitive information in text format stored in computers, and as it is being transmitted, being copied, saved, or printed. Actions are then taken based on pre-defined policies to protect the information from loss and misuse.

The modules within SecureMi suite that provides this complete functionality are:

- SecureMi Centralized Management Console (CMC)
- SecureMi Storage
- SecureMi Endpoint

SecureMi Storage and SecureMi Endpoint are managed through SecureMi CMC, a web application with a consistent user interface to centralize the control of content aware inspection techniques for data classification process.

Sensitive data is classified using both precise data identifier (finger-prints of sensitive data) and partial precise data identifier (keywords, phrases, regular expressions, file properties and its location) in configuration of the data protection policies.

SecureMi Storage and SecureMi Endpoint provides the sensitive data protection required. SecureMi CMC provides the administrative access and management of the data protection policies across the network, storage and endpoints.

Software licensing covers the complete SecureMi Suite, which includes SecureMi Central Management Console (CMC), SecureMi Storage and SecureMi Endpoint which will classify, discover, monitor and prevent data leakage from your network, storage and endpoints.

DEVELOPED BY: EVAULT

IN COLLABORATION WITH: MOSTI Ministry of Science, Technology and Innovation; CyberSecurity MALAYSIA An agency under MOSTI

SecureMi Centralized Management Console (CMC)

- Provides a web based centralised management console for authorized administrators to manage data protection policies.
- Centralize data protection policy management of dynamic protection of classified data. Policies will be synchronized to SecureMi Endpoint and SecureMi Storage periodically via web service.
- Centralize the policy management of static protection.
- Centralize the policy management of administrator's Role based Access Control (RBAC) for supporting separation of duties.
- Centralize the incident workflow and remediation management to improve the inspection process and at the same time educating user of any policy violations.
- Centralize the management of report, audit trials and dashboard information.
- New version of software can be updated on the fly upon release by administrator by using our software deployment method.
- Provide Environment Aware Inventory – Endpoint Information (Hardware, Network, Operating System, Application installed).
- Provide Environment Aware Inventory – Server Information (Hardware, Network, Operating System, Application installed).
- Trigger data discovery process on demand by Administrator.
- Support multiple languages and regulatory compliance such as PCI DSS and Malaysian PDPA 2010.

Technical Specifications

SecureMi Storage or CMC Server System Minimum Requirements:

- Dual or quad core Intel Xeon processors
- 4GB or more RAM
- 256 GB or more Hard drive
- NIC 1000/100
- Or equivalent virtual machine's resources

SecureMi® Endpoint Minimum Requirements

- Windows XP, Windows 7, Windows 8, Windows Server 2008 operating systems (64/32 bit)
- 2GB RAM
- Minimum 300MB free Hard drive space

SECUREMi®

Protect your sensitive data

SECUREMi®

DATA SHEET

Highest risk today – Data leakage due to insider threats

Data breaches due to insiders expose an organization's confidential and sensitive data to unauthorized parties.
A data breach may occur as a result of an internal employee's mistakes or carelessness such as non-compliant behavior, stolen or misplaced computing devices, or malicious attacks such as sabotage, theft, fraud and sabotage.

Data Leakage due to insider threats are on the rise.

Among the many issues are, most do not know where their confidential data is. They are not able to monitor and protect it and there are so many ways for insiders to steal data.

It is difficult to enforce compliance to security policy and regulatory policy.
It is difficult to identify the cause of data breach when it happens.

Data Leakage Prevention has become a business imperative and a strategic business initiative.

Content Aware Data Leakage Prevention

SecureMi suite of data leakage prevention solution is engineered to prevent data leakages that can lead to compliance violations and intellectual property loss and provide the versatility to protect sensitive or classified information from misuse or leakages.

SecureMi ensures that sensitive and confidential data is shared, used, stored and transmitted appropriately and securely. SecureMi consists of policies, procedures, and technical controls that can be defined via a centralized management console.

It can classify, discover, monitor, and protect data by monitoring who is using it; how it is being used; where it is being transferred; and what real-time action is taken to prevent data leakage through dynamic and static protection with content aware inspection.

SecureMi Endpoint

- Discover, Monitor and Protect data used by end users.
- An agent based solution that sits on end user workstations and laptops.
- Monitor and control by notifying senders, blocking or quarantining any classified data depending on data protection policies.
- Monitor and control any classified data on wire. It supports multiple protocols such as HTTP, HTTPS, FTP and SMTP.
- Monitor and control any classified data copied via removable devices such as external hard disks, USBs, etc.
- Monitor and control any classified data shared on the workstations / laptops' memories.
- Apart from the dynamic protection capabilities above, SecureMi® Endpoint is also built-in with static protection capability to provide extra classified data protection.
- Provides implementation of rights management on printer management on classified data.
- Provides application of encryption on classified data.
- Provides secure storage (Endpoint Vault) to store sensitive and critical unstructured data in encrypted form at endpoint.

SecureMi Storage

- Discover, monitor and protect data at rest.
- Can be installed on the same server with the centralized management console or on another server anywhere on the network.
- Identity and discover classified data on repositories that hold data such as file shares, file servers, web servers and etc.
- Data discovery scanning process can fingerprint data to be used to identify unstructured data elsewhere

DEVELOPED BY: EVAULT

IN COLLABORATION WITH: MOSTI Ministry of Science, Technology and Innovation; CyberSecurity MALAYSIA An agency under MOSTI