S.M.S. FEATURES AND FUNCTIONS

Armarius Software's software solution, Scribe Management Suite (SMS) is the most comprehensive, feature rich security tool in the industry today, far surpassing the likes of Symantec, McAfee, RSA or Websense. The module SMS within the Event Monitoring & Management Application solution includes features from our previous software products and new functions we have added through our customer feedback. Besides having the most intelligent agent based solution within the DLP space, SMS provides your organization with benefits in several other functional areas which will impact your bottom line directly. These additional functions and reports include Help Desk Remediation, Application Analytics, User Productivity Reports and Software License Compliance/Usage Reports. All of these features are bundled into our tool today for our clients to take advantage of for one low cost.

LEGEND:

FEATURE - [MODULE]

(Competitors – module name)

EMAIL MONITORING / ENCRYPTION - [SECURE]

(Competitors: Cisco Ironport, McAfee – DLP Suite, Proofpoint, RSA – DLP Network, Symantec – DLP Suite, Trustwave, Verdasys Digital Guardian, Websense – Email Security)

|

Monitor all email and attachments. Encryption method is PKzip. Standard default 8 character dictionary password is 128-bit encryption and by requiring complexity forces it to 256-bit encryption.

- Allow all emails
- User optional encryption
- Mandatory encryption
- Block attachments
- Block content in the email body / subject
- Block or Allow only specific extension types
- Safe domains

EMAIL ARCHIVE - [SECURE]

(Competitors: GFI, IBM, MailArchiva, Quest, Proofpoint, Ubistor)

The agent will archive email in raw text

- Archive incoming read email
- Archive outgoing email

HARDWARE CONTROL - [SECURE]

(Competitors: GTB Technologies, McAfee – DLP Suite, McAfee – Device Control, RSA – DLP Endpoint, Safend – Protector, Symantec – DLP Suite, TriGeo, Trustwave – Edge, Verdasys – Digital Guardian, Websense – Data Security)

The agent has the ability to control any device(s) plugged into a pc.

- Force encryption to files being sent to removable drives
- Block the usage of;
    - CD/DVD
    - USB Drives
    - Infrared
    - Bluetooth
    - Floppy
- Safe lists to allow certain devices by;
    - Manufacturer
    - Volume Name
    - Serial Number

DOCUMENT MANAGEMENT - [SECURE]

(Competitors: None)

The difference between Armarius Software's document management software and traditional database driven software is normally users check out data from the repository in a traditional system. With the agent, the administrator can lock down file shares to not only read/write access but block them from;

- Copy/Move – from the protected directory to any other directory
- Print – print the files to any type of printer including PDF writers
- Attach – Attach files from the directory to an email
- Copy/Paste – Copy and Paste actual text from within a protected document to any other target
- Rename – Rename the documents in the directory
- Upload – Upload any files from within the directory to any website

DATA DISCOVERY (SPIDER) - [SECURE]

(Competitors: GTB Technologies, McAfee – DLP Suite, McAfee – DLP Discover, RSA – DLP Datacenter, RSA – DLP Endpoint, Trustwave – Discover, Verdasys – Digital Guardian, Websense – Data Security)

Scan directories on the local machine or network shares looking for content or extensions. The spider can be controlled by parameters to for encryption on found content violations.

WEBSITE FILTERING - [SECURE]

(Competitors: Cisco IronPort – Web Security Appliance, Spectorsoft – CNE, Spectorsoft – 360, Symantec – DLP Suite, Verdasys – Digital Guardian, Websense – Web Security)

The agent has the ability to monitor website usage and access.

- Track or Block files from being uploaded
- Block FTP
- Block file downloads
- Block or Allow websites based on a Block/Safe List
    - Block URL patterns
    - Block based by "keywords" or meta tags
    - Allow site access based on time
    - Allow uploads based on URL
- Web-Mail – Specific support for 7 common web based email systems

CLIPBOARD MONITORING - [SECURE]

(Competitors: Verdasys – Digital Guardian, Websense – Data Security)

With an agent at the desktop, anything that is copied into the clipboard can be filtered including images. When an employee takes a snapshot of the screen the agent can screen scrape the text and then apply the filtering rules.

- Block clipboard ability to specific applications
- Block screenshots based on content
- Block screenshots based on the application
- Track all clipboard activity

APPLICATION ACCESS - [SECURE]

(Competitors: Verdasys – Digital Guardian, Websense – Data Security)

The agent has the ability to block applications based on;

- Caption
- Screen text within a caption
- Manufacturer name – Software company that created the software i.e., Adobe
- Executable name

Also

- Force services to restart
- Block applications based on location
- Block registry changes

FINGERPRINTING - [SECURE]

(Competitors: McAfee – DLP Suite)

The agent has the ability to tag documents that are considered sensitive based on their location. The agent can do this automatically or the organization can tag them manually. Then based on the keyword, the agent can;

- Block or Force encryption on attachments
- Block or Force encryption on files being moved or copied
- Block Uploads
- Block Printing
- Block Copy/Paste
- Block Rename
- Allow via Safe Domains

FILE SHADOWING - [SECURE]

(Competitors: None)

The scenario is as such; imagine a user does a query on the database, copies the text to a notepad document, saves it to the desktop, then moves it to the USB drive. As an administrator of the software, you would have been notified that this just occurred however you wouldn't get to see the content in the file. File Shadowing allows the agent to "shadow" make a copy of the file to the network location for review. File Shadowing can be done on;

- Files leaving via removable drives
- Files being printed
- Files being attached to emails
- Emails themselves (including subject / body text) – stored in html, rtf or txt files.

Other parameters include;

- Self purging
- Maximum file sizes
- Specific file types

SCREEN CAPTURE - [SECURE]

(Competitors: Spectorsoft – 360)

The agent has the ability to take snapshots of the screen as a user would. The agent can take;

- Single Application Capture
- Desktop Capture
- DVR Playback

Also;

- Scan Content – look for content and take a picture based on content
- Block Content – block the screen if content is found

NETWORK/PRINTING - [SECURE]

(Competitors: McAfee – DLP Suite, RSA – DLP Endpoint, Spectorsoft – CNE, Spectorsoft – 360, Symantec – DLP Suite, Verdasys – Digital Guardian, Websense – Data Security)

- Track all printing including PDF writers, USB and Network based printing
- Block all printing
- Block only sensitive printing

CONTENT PROFILING - [SECURE]

(Competitors: GTB Technologies – DRAM, GTB Technologies – Inspector, McAfee – DLP Suite, RSA – DLP Datacenter, RSA – DLP Network, RSA – DLP Endpoint, Symantec – DLP Suite, Trustwave – Protect & Monitor, Trustwave – Discover, Trustwave – Edge, Websense – Data Security, Websense – Email Security)

The agent has the ability to scan for content within the raw text of the files. Content Patterns include;

- Credit Card Numbers – Government issued algorithm
- Social Security Numbers – Government issued algorithm
- Bank Routing Numbers
- Keywords
- Multiple Keywords
- Text files containing keywords
- Straight patterns i.e. 9999999990
- Table Files containing numbers
- Regular Expressions (RegEx)

AGENT SETTINGS - [ALL MODULES]

(Competitors: None)

Inside the agent there are other features including;

- Ability to customize all policy screens displayed to the end user
- Track Outside IP address with the IP Address Locator
- Disable Safe Mode
- Shutdown Windows automatically

USER ACTIONS - [INTELLIGENCE]

(Competitors: Netvizor, Spectorsoft – CNE, Spectorsoft – 360)

The agent has the ability to track all user actions including keystrokes from when the user logs in to when they log out. The agent can also compute the time the application is open vs. the time the application is actually used. Thus providing a time sheet from when they log in to when they log out including “Idle” time.

APPLICATION PERFORMANCE - [INTELLIGENCE]

(Competitors: NetQoS, NetScout, Quest)

The agent has the ability to track the time in milliseconds from when an application icon is double clicked on the desktop to when it is actually ready for input. The agent will also track the time from when the user clicks a button, menu item, hyperlink or more until the next screen is available. Within application performance the agent can track;

- Specific buttons, windows or screens
- Custom built java-based applications

HELPDESK REMEDIATION - [SUPPORT]
(Competitors: None)

The agent has the ability to track when errors occur on the desktop. So when the agent "senses" an error, the agent will collect DNA information about the PC and the last user actions that potentially caused the problem.
Some of the events the agent can "sense";

- GPF Errors
- Runtime Errors
- Unhandled Exceptions
- Unexpected Errors
- DEP Errors
- Script Errors
- Dialog Errors
- Application Fault Errors
- HTTP Errors
- Agent Errors
- Custom Application Screens
- Baseline PC DNA – Ability to gather the default information every X amount of days

SOFTWARE USAGE ASSESSMENT (SUA)

The agent has the ability to capture all installed applications on your desktops and laptops within your enterprise. This baseline report will give the customer an accurate and up to the minute snapshot of all the different types of applications and versions installed for all of your users. The next component of the process which we will provide, which makes us very unique, is that we now can tell you who is using all these applications and how often they are using these applications. You now can meet and pass any software compliance audit you face but now you can be proactive in understanding what applications you might want to replace because no one is using them and more importantly you now can accurately assess the number of licenses you need to purchase for the individuals that are actually using these applications. Two reports that will save your organization thousands to millions of dollars depending on the size of your organization.

DESKTOP SECURITY RISK ASSESSMENT (DSRA)

The scope of the Desktop Security Risk Assessment was to capture desktop activities in order to determine what and how data is being transmitted outside of your organization, and shared internally bypassing the control of the network security policies. Employees who are permitted access to sensitive data and unknowingly expose that information in emails or maliciously remove data by copying it to an external device represent a great and invisible security risk. The security challenge is that in many cases access to and utilization of this data is considered part of their job.

Desktop security software was installed on all desktops in a "passive" mode that captured local events and activities for a period of 10 business days. This analysis period is representative of normal data access and transmission activities that occur during daily business. This information was used to analyze how information was being used, where and how it was transmitted, and what users have access to the most security sensitive information and data transmission tools. Our desktop security risk assessment methodology has been applied to these events to identify data at risk. This methodology separates activities into distinct event types based on the mode of data transference and allows the identification and distinction of acceptable activities and assesses data at risk. Risks are then examined and recommended approaches for risk mitigation are developed.

Digitally signed by Bîrsan Vitalie
Date: 2022.09.30 10:04:20 MSK
Reason: MoldSign Signature
Location: Moldova