Data Leakage Prevention

Product Capabilities

HKM Consulting

DLP - Data Leakage Prevention

Product Capabilities

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data, also known as the CIA triad, while maintaining the focus on efficient policy implementation, all without hampering organization productivity.
This is largely achieved through a multi-step risk management process that identifies assets, threat sources, vulnerabilities, potential impacts, and possible controls, followed by assessment of the effectiveness of the risk management plan.

An important cornerstone of information security covered by our solution is confidentiality. Many compliance mandates require privileged access and demonstrable enforcement of confidentiality for all innovations and trade secrets. For this purpose, correspondingly resilient evidence must also be provided. Our solution can help meet these requirements.

In detail, this is achieved through monitoring, actions, reporting as well as other solution features.

Remote Monitoring

SNAP Tunnels:
Safely send data to remote networks using SNAP Tunnels.

Remote Support:
Securely connect to monitored workstations and servers with Remote Desktop even through firewalls and across the Internet with Data Leakage Prevention.

Monitors

Action Scheduler:
It will run your defined Actions when you specify.

All-Systems-GO:
Reports to the All-Systems-GO service which can notify you if the monitoring installation is affected in any way that would prevent its from alerting.

Drive Sight:
Protects servers and workstations by preventing CD/DVDs and/or external drives, including USB drives, from being attached. Any specified devices that are attached are immediately detached by the operating system so they cannot be accessed.

Dynamic Server List:
Dynamic Server Lists are groups of serves that meet your criteria. Once the list is known, you can define Dynamic Groups based on the list, and use that group everywhere else groups are used.

File Sight Monitor:
The monitor watches real time file access by users and programs. You can configure which files it watches, and how the system will notify when a particular operation (file read, write, delete, etc.) occurs and records the file access operations to a database for reporting (by user, by file, by operation, etc.).
Policies can also contain quota definitions and alert on user usage patterns (i.e. user reads X amount of data in Y time. This logic can be very powerful for ransomware protection and detecting file copying.

Note:
This monitor can detect actions on drives on the local computer. Watching files on remote computers requires an agent or a script for replication (agent-less integration).

Inventory Collector:
Collects inventory information (hardware information, pending Windows Update, anti-virus status, etc.) from a variety of sources including WMI, SNMP and an optional System Details application.

Action List

Action List:
Groups of actions for common notifications, group notifications, etc.

Add to Blocked List:
Adds all users reported on by a File Sight monitor to the Global Blocked Users List.

Call URL:
This action will call a URL you specify, optionally posting information about the current alert. This makes it easy to connect to a helpdesk/ticketing system.

Desktop Notifier:
Delivers alerts to Windows desktops via a pop-up message box or a slider in the lower right corner of the screen.

Dial-Up Connection:
Connects or disconnects a Windows Dial-up Connection. Typically this is for servers that are not on the Internet, but need to connect to send alerts.

eMail Alert:
Sends SMTP eMail messages to mail boxes, cell phones, mobile devices, etc. The eMail action has Alert Digests which are a powerful/friendly feature that combines multiple alerts that happen within a short time into a single eMail notification. This can be very helpful when something goes really wrong. You can easily specify when messages should be sent or suppressed.

Execute Script:
Similar to the Execute Script monitor, this Action lets you extend the list of available actions via your own script written in VBScript. Many variables from the source monitor are also available for creating rich, situation-specific responses.

Message Box:
A simple message box that displays monitor findings. These message boxes are smart: if there are many pending alerts you can easily dismiss them all at once.

Monitor-Directed eMail:
The monitor which detects a problem specifies the eMail address to use for each alert. This is very useful when sending reminders and alerts to end users such as with the User Quota Monitor and the Directory Quota Monitor.

Network Message (Net Send):
Sends a message box containing the critical monitor details to every place that you are logged in.

Pager Alert via SNPP:
Send monitor results to pagers via standard Simple Network Paging Protocol (SNPP). You can easily specify when messages should be sent or suppressed, and the content of the message.

PagerDuty Integration:
Send alerts directly to your PagerDuty account and track them using the full power of the PagerDuty platform.

Phone Dialer (DTMF/SMS):
Dials a modem/phone and optionally sends DTMF commands or other commands (to send SMS messages for example). This is typically used by a disconnected server to send an alert over a normal phone line (where the CallerID identifies the server).

Play Sound:
Audible alert when monitors detect a problem with the server.

Reboot Server:
Reboots the server if a monitor has detected a critical system failure.

Run Report:
When this action is triggered, it will run the specified Scheduled Report including sending any eMails or saving PDF or CSV files that report requires.

SMS Text Message:
Send SMS text messages to your mobile device via your service providers SMS Internet gateway (SMPP server). You can control which information gets sent, as well as when messages are allowed.

Server Maintenance:
Set or remove the Immediate Maintenance period for a server or servers.

SNMP Trap:
Sends an SNMP Trap with details from the monitor firing the action.

Start Application:
Starts a specified application when the monitor triggers actions.

Start Service:
Sends control messages to the Windows Service Control Manager to start, stop or restart a specified service.

Syslog:
Sends monitor alerts to a Syslog server on the network.

Write to Event Log:
Writes monitor details to the Windows Event Log.

Write to Log File:
Log the findings of any triggered monitor to a file. Separate files can be created for each day, week, month, etc.

Reporting

Ad Hoc Reports:
Generate reports on the fly to quickly see graphical trends.

Branding Reports:
Easily brand reports with your company logo at the top.

Group Settings:
Group summary reports can be specified and controlled in a per-group way. In addition, group reports can be automatically eMailed to anyone that needs to keep track of the servers.

HTTP accessible reports:
Reports are generated in HTML and accessible from within the Enterprise Integrity Management Console application, or from a web browser.

Password Protection:
Password protect web reports in Enterprise Integrity Management.

Satellite Status:
Quickly see the current status of an individual Satellite Monitoring Service.

Satellite Summaries:
Two reports that let you see the status of all of the Satellites at once.

Scheduled Reports:
You can create scheduled reports which will get created when you want them, and optionally eMail the report to a list of recipients. Scheduled report URLs are stable so you can add them to your Favorites list to quickly and easily see the latest results.

Server Status:
Easily see at a glance the state of your server along with system statistics.

System Activity Log:
Quickly see which monitors are running, how long they are taking, which actions are being fired and more.

Standard Report Tabs:
View the tabs and information that is common among most report types.

File Sight - All Changes:
Get a quick report to see everything Enterprise Integrity Management has recorded in a specified time frame.

File Sight - Custom Data Set:
Create a report that filters on many different File Sight criteria.

File Sight - File Changes:
Quickly see all changes that happened to specific file or set of files.

File Sight - Type of Change:
See all file operations of a specific type. For example, all files that were deleted in the past two days could be quickly shown.

File Sight - User Activity:
Find all users who have done more than a specified number of specific operations. For example, anyone that has deleted more than 50 files in the past week.

File Sight - User Block List:
Quick way to see which users are on the File Sight User Block List, and which are on the white list.

File Sight - User Changes:
Select a specific user and a time frame to see all recorded file activities they have performed.

File Sight - User R/W Amt:
Find all users who have read and/or written a specified amount of data in a given time frame.

Group - All Errors Report:
The All Errors report show all recent errors on all monitors on all servers/devices within a group. This is a good place to quickly get a detailed view of any problems happening on the network.

Group - All Servers Report:
This report shows all of your servers in a group in a single page. Each server is a small box that is color coded according to the status of the monitors on that server.

Group - Custom Group:
Create custom reports at a group level to show custom HTML, charts, and other status values for the contained servers.

Group - Group Summary:
See a one line status indicator per server to see at a glance how the servers in your data center are doing. Per-group status reports are also supported.

Group - Status Map:
See a graphical map that contains status indicators that show you at a glance how servers in different geographic regions are doing.

System - Config Audit:
This report shows you what your current configuration is with your Groups, Servers, Monitors, and Actions.

System - Connected Sessions:
See all sessions (Console, Satellite, mobile apps) currently connected to the Central Service.

System - Error Audit:
Powerful report to look at current and past alert conditions that have been detected by the system.

System - Monitor Scope:
Displays a summary of what is being monitored on a per-group basis. This would be appropriate to show stake holders to indicate the level of monitoring work being done.

System - Monitor Status:
A quick table-based overview of current monitor statuses. You can specify a specific monitor type, only monitors in error, etc.

System - Statistics:
View system statistics such as HTTPS connections and data transferred, numbers of monitors and connected Satellites, etc.

System - System Audit:
Find out about activities within the monitoring system, such as alert eMails sent, user logins, Satellite disconnects, etc.

System - User Permissions:
This report will display all users defined in the system, what they have access to, and their permissions.

Product Features

Automated Maintenance Schedule:
While a computer is in maintenance mode, the system won't run monitors. It will turn itself back on automatically after the maintenance window expires if you manually entered maintenance mode, or it can automatically enter and leave maintenance mode on a schedule.

Automatic Fail Over:
Setup a second instance of DLP to monitor the primary monitoring service, and take over if it fails.

Bulk Configuration:
Perform changes of settings in actions, monitors, reports and scheduling for several servers at one time, or copy configuration settings to other servers.

Configuration Security:
Password protect the DLP Management Console, and alert on changes that could affect monitoring.

Database Options:
Easily point DLP monitor at the embedded SQLite database or use an external Microsoft SQL Server.

Easy Deploy:
Paste a list of servers or IP address from the local network into a list and let the DLP monitor silently deploy the Satellite Monitoring Service to those machines for you.

Easy to Use and Configure:
Due to the agent and agent-less integration in a network segment and the easy roll-out of satellite systems in sub-network, the system is one of the simplest, clearest and most effective monitoring tools.

Embedded HTTP Server:
Control the HTTP port that DLP monitor uses, and optionally enable HTTPS (SSL).

Error Auditing:
Keep track of which errors have been reviewed and acknowledged. Also a great way for administrators to have an overview of any errors within their area of responsibility.

External API:
Send basic configuration requests to the product via an HTTPS URL.

Runs as a service:
DLP Management Monitor is composed of a console that you interact with, and a system service that is started when the computer boots up and is always running in the background.

Server Grouping:
Group servers together in visual groups to help keep track of them. Group-based status reports are also available.

Simple Branding:
Easily brand DLP system to have your name and graphics by simply dropping a couple of files into the installation directory. Rebranding will be provided with the DLP Toolbox.

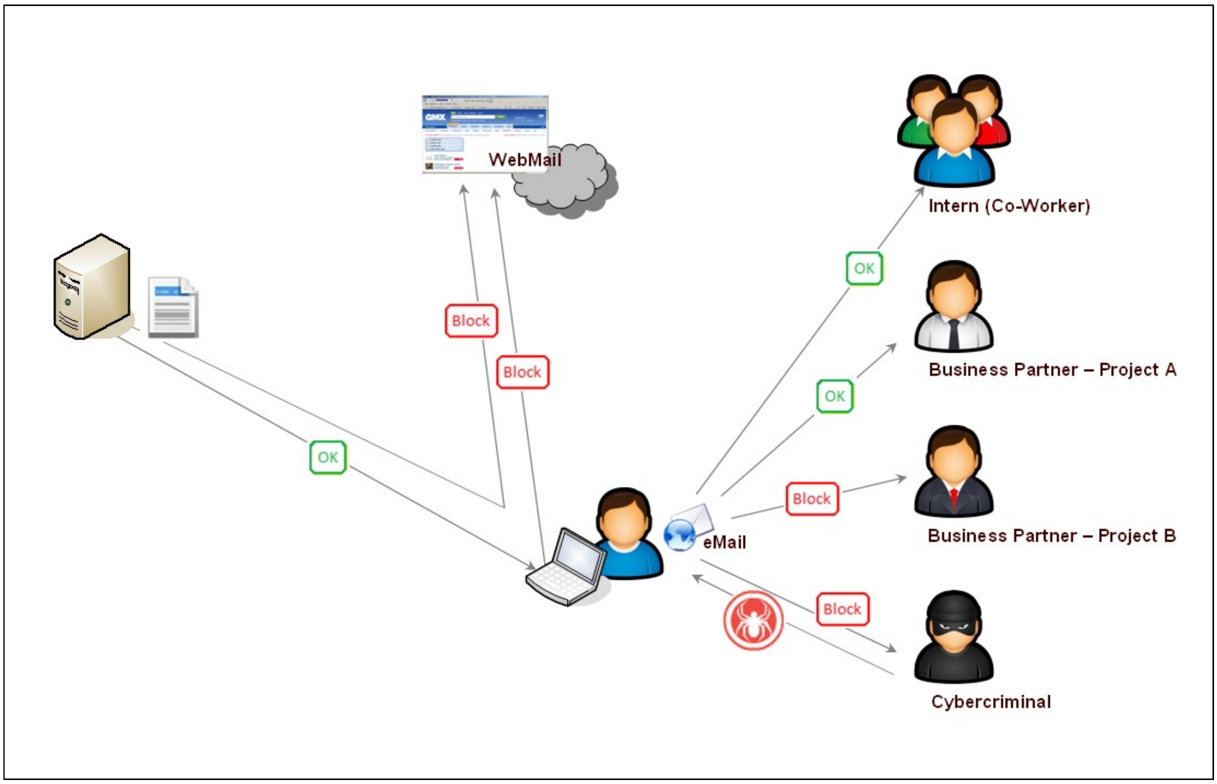
Simple Installation:
Takes less than 3 minutes to install and get a default installation customized for your system.

Fulfillment of Compliance Requirements:

An important cornerstone of information security covered by our solution is confidentiality. Many compliance mandates require privileged access and demonstrable enforcement of confidentiality for all innovations and trade secrets. Our solution can help meet these requirements, including those listed below:

- PCI (Payment Card Industry) DSS 10.5.5, 11.5, 12.9.5
- SOX (Sarbanes-Oxley) DS5.5
- GLBA (Gramm-Leach-Bliley Act) 16 CFR Part 314.4(b) and (3)
- HIPAA (Health Insurance Portability and Accountability Act) 164.312(b)
- FISMA (Federal Information Security Management Act) AC-19, CP-9, SI-1, SI-7
- ISO 27001/27002 12.3, 12.5.1, 12.5.3, 15.3
- ISO 27001:2013 - Annex A.5-A.18
- European Law on protection of Business Secrets (GeschGehG)
- BSI KRITIS
- §203 StGB
- BaFin (BAIT, KAIT & VAIT)

Protection and Auditing:



Picture 1: Protection and Auditing

Our DLP - Data Leakage Prevention system is highly scalable and enterprise-ready. The solution is capable to monitor lagre enterprises and enforce company policies on a global level. Easily define rules for all, countries, regions, or groups and set the level of enforcement. Cover all your confidentiality requirements from one central console.

Please contact your sales and consulting representative to work out you best integration type and pricing.

© 2023 HKM Consulting GmbH

© 2023 Janus Event und Entertainment GmbH

Alle Rechte vorbehalten. Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen Zustimmung des Verlags. Dies gilt auch auf die fotomechanische Vervielfältigung (Fotokopie, analoge oder digitale Ablichtung, Mikrokopie) und die Einspeisung und Verbreitung in elektronischen Systemen.

HKM Consulting GmbH
Klaus Martin Hecht
redaktion@hkm-consulting.de