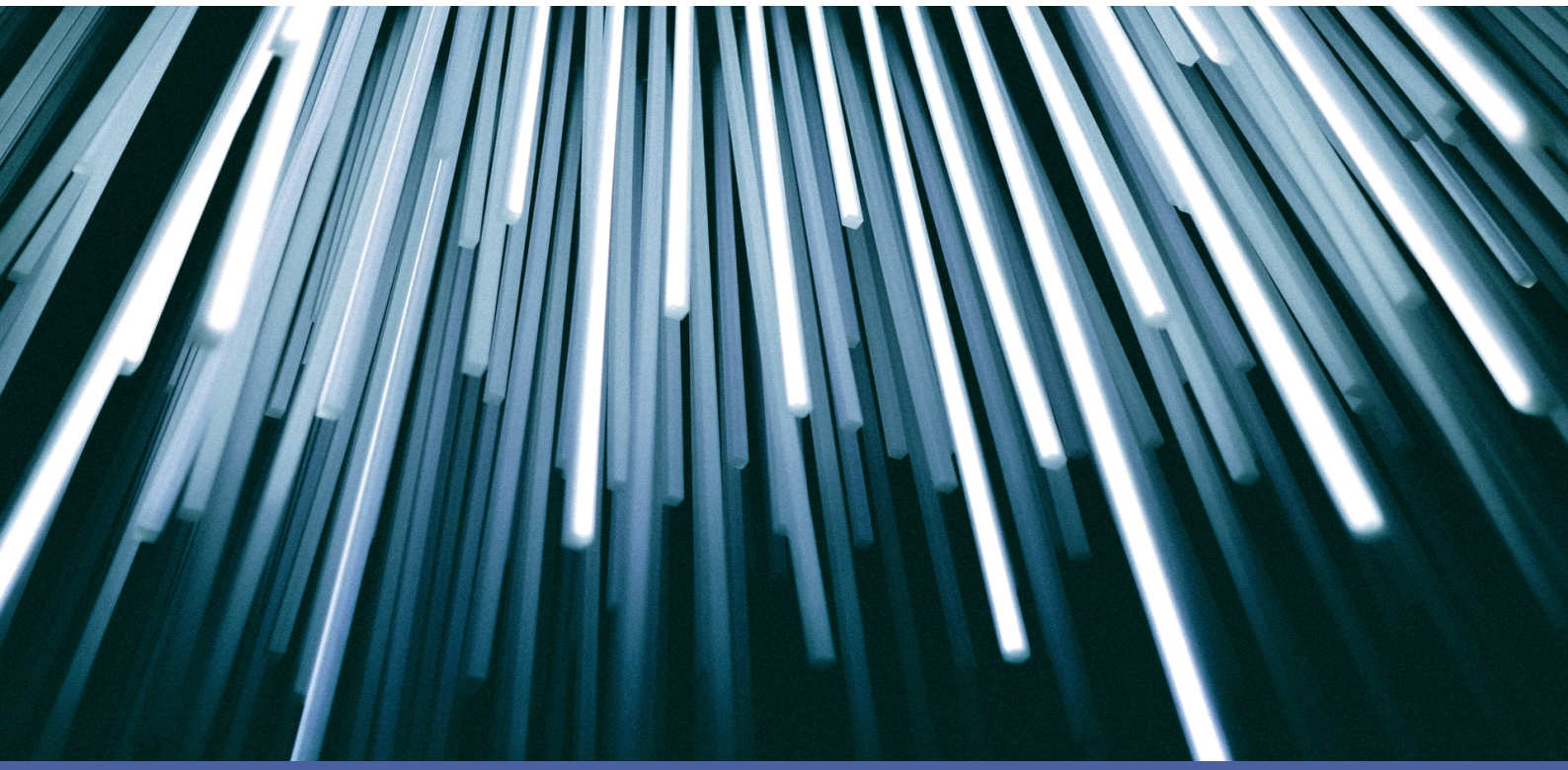
Cyber Security Framework (EIM, C2C, DLP)



HKM Consulting

Cyber Security – Framework (EIM, C2C, DLP)

Information Security

Information security is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation, although it may also involve reducing the adverse impacts of incidents.

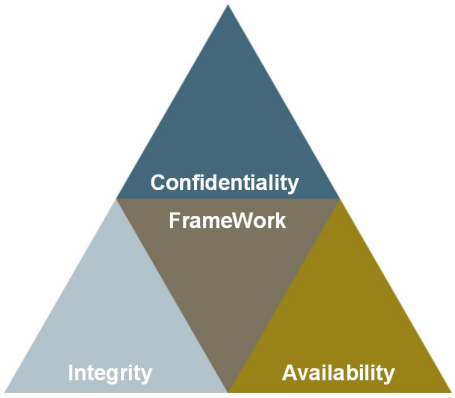
Information may take any form and is not only related to computer systems. Information can be electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data - also known as the CIA triad - while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a structured risk management process that involves:

- Identifying information and related assets, plus potential threats, vulnerabilities and impacts;
- Evaluating the risks;
- Deciding how to address or treat the risks i.e. to avoid, mitigate, share or accept them;
- Where risk mitigation is required, selecting or designing appropriate security controls and implementing them;
- Monitoring the activities, making adjustments as necessary to address any issues, changes and improvement opportunities.

To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability, security awareness and training, and so forth. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred and destroyed. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

C-I-A Triade

The C-I-A triad of confidentiality, integrity, and availability is at the core of information security. It describes the protection goals of information security in only three main areas.



Confidentiality – ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.
Data access is managed using security mechanisms such as user names, passwords, access control lists and encryption for authentication. A data classification needs also to be provided here to categorize the information according to the extent of the damage that can be caused if it gets into unintentional hands. This classification can be based on content and context.
On the basis of this, the distribution groups, distribution routes and distribution channels needs to be defined/establish with whom confidential information can be shared and/or distributed.
In some scenarios, it is necessary to verify whether the recipient should be able to use confidential information that has already been transmitted at a later point in time.
If these key points are taken into account, security measures can be implemented accordingly.

Integrity – ensures that information are in a format that is true and correct to its original purposes. This principle applies to both data-in-rest and data-in-motion.
So it must be ensured for the author of data as well as for anyone who can later access this data or receive it that this data is original.
It is mandatory that information can be edited by authorized persons. Possible modifications like create, delete, open, modify, rename, copy, move, and so on needs to be recognized. Unauthorized modifications as well as malfunctions must be detected.
Systems with redundancies and high availability or systems for backing up data can help to be on the right way again if data have been changed in an undesirable or undesired way, however they replace these systems for data integrity.

Availability – ensures that information and resources are in place and ready to use to those who need them. It is implemented using methods such as hardware maintenance, software patching and network optimization. Processes such as redundancy, failover, arrays and high-availability clusters are used to mitigate serious consequences when technical issues do occur. Dedicated hardware devices can be used to guard against downtime and unreachable data due to malicious actions such as distributed denial-of-service (DDoS) attacks.

This visualization helps to formulate the central requirements in fine granular form and to set up policies in the individual areas. These requirements can be driven by internal standards or mandatory external compliance requirements.

The related solution components to this protection goals of information security are:

- Confidentiality - Data Leakage Prevention (DLP)
- Integrity - Enterprise Integrity Management (EIM)
- Availability - DataCenter Design, ITIL Continuity Management, SIEM

The visualization also helps to consider and combine the individual protection goals in a holistic approach. The various compliance requirements like:

- ISO 27001/27002
- ISO 27001:2013 - Annex A.5-A.18
- BSI KRITIS
- §203 StGB
- BaFin (BAIT, KAIT, VAIT & GwG)
- European Law on protection of Business Secrets (GeschGehG)

but also international requirements like:

- PCI (Payment Card Industry)
- SOX (Sarbanes-Oxley)
- GLBA (Gramm-Leach-Bliley Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- FISMA (Federal Information Security Management Act)
- MLCA (Money Laundering Control Act) / KYC (Know Your Customer)

and many more can be met by including Data Leakage Prevention, Enterprise Integrity Management and Security Information and Event Management in a security and risk strategy. Their effectiveness can be verified in an auditable manner. A balanced framework that takes all of these requirements into account helps to serve the three areas comprehensively.

Framework

The framework is both the binding link between the three areas of data security as well as the legal regulations and requirements. It offers a clear view of the requirements as well as a holistic approach for the risk assessment based on them.

It is designed in such a way that it also offers a structured overview, both in the purely disciplinary view of cybersecurity and for the organizational implementation in projects.

Every part of the framework is sorted by corresponding building blocks for:

- Performance Directory
- Projects
- Toolbox
- Test & Verification

Integration Manual - Overview:

The Integration Manuals (Windows Server 2016, 2019, 2022) consists of:

- Basic OS installation
- Accounts at the EIM, C2C & DLP Server (Non-domain Integration)
- Device Manager (Devices and Driver)
- Network Interface
- Computer Name and Network Name
- Operating System - Updates and Patches
- EIM Server
  - Desktop and Environment for Policy Integration
  - Tools
  - Storage and System Clean-up
- C2C Server
  - Desktop and Environment for Policy Integration
  - Tools and Analysis
- DLP Server
  - Desktop and Environment for Policy Integration
  - Tools and Forensics

Integration Manual (EIM, C2C & DLP Server) - Overview:

The Integration Manuals (EIM, C2C & DLP Server) consists of:

- EIM, C2C & DLP: Application and Database Installation
- EIM, C2C & DLP: Server Customizing and License
- EIM: Folders and Policies (Detector)
- EIM: Scripts (Replicator) and Tools
- EIM: Task-Scheduler (Scheduler)

System Hardening Description - Overview:

The System Hardening Description consists of:

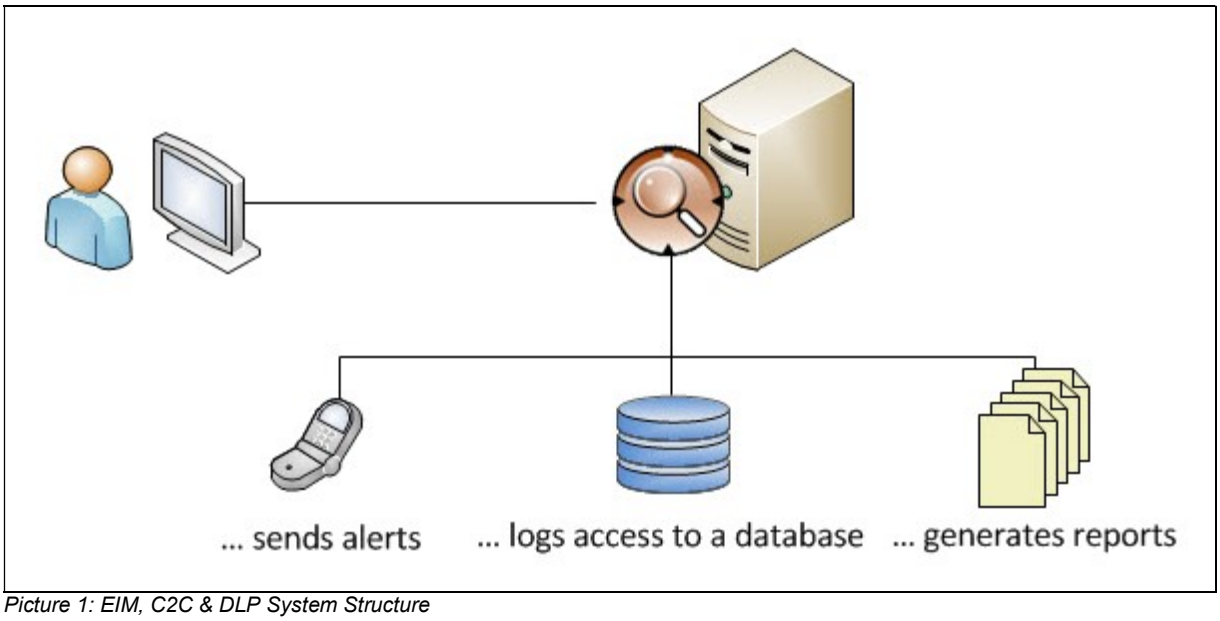
- System Hardening
- Hardening using Group Policies
- Microsoft Security Baseline (MSB)
- Center for Internet Security (CIS)
- Deviations from specifications
- Internet Explorer 11 and Office 365 ProPlus

System Structure of EIM, C2C & DLP server

Each EIM, C2C and DLP scenario includes the central management console at the top level. All administrative tasks can be performed via the dashboard. The intelligent design of the system allows it to work with a proprietary database. to work with. SQL Server is also supported and can be run both on the same computer - not recommended and not calculated in the sizing - or on an external computer. computer. The installation of the ODBC driver for SQL Server during initial during the initial setup is strongly recommended.

During the initial set-up, a quick number of interfaces and connectors are installed for alarming is installed. Additional alarm systems can be added later via the option to run a script option or the option to run an application. All these embedded tools require a minimum of resources on the EIM, C2C or DLP server.

The generated reports consume only a few 100KB of disk space. Automatically generated reports can be transferred to a final file store.



Picture 1: EIM, C2C & DLP System Structure

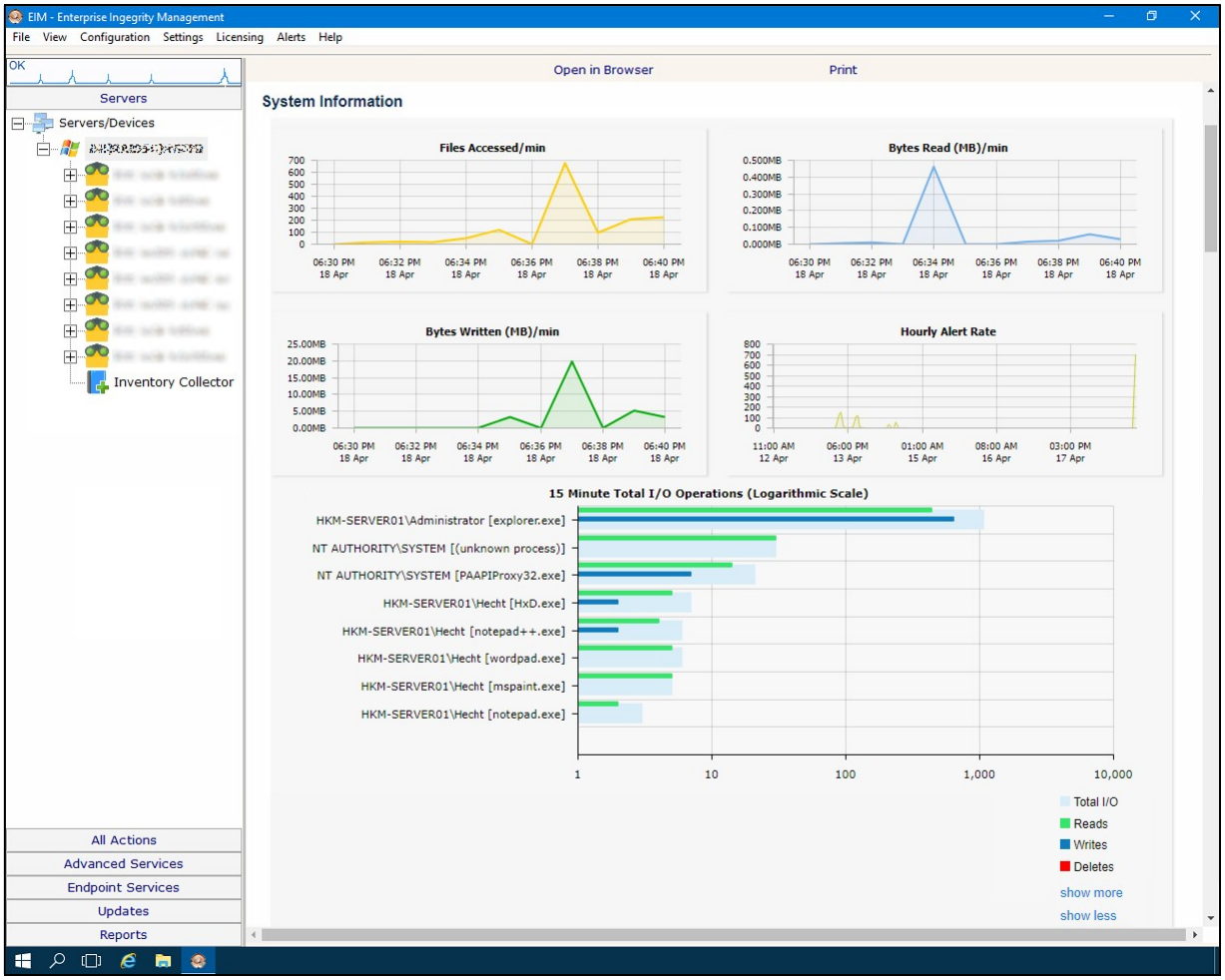
Enterprise Integrity Management, Compliance to Code as well as Data Leakage Prevention has been designed to require as few system resources as possible.

EIM Server Components:

The EIM Server consists of several various components. Some of this components are available via the EIM Server Console (Detectors), others are defined by seperate applications integrated at the EIM Server (Replicator and Scheduler). An overview of the core components, whose function and mode of action are also part of the EIM framework, is described in the EIM Product Capabilities.

Server Console

The central management console provides the policy configuration on the left hand site. All server monitors and device monitors with its policy definitions and associated actions are listed here. The right hand side shows the selected details. Starting the console the system information is shown on the right hand side.



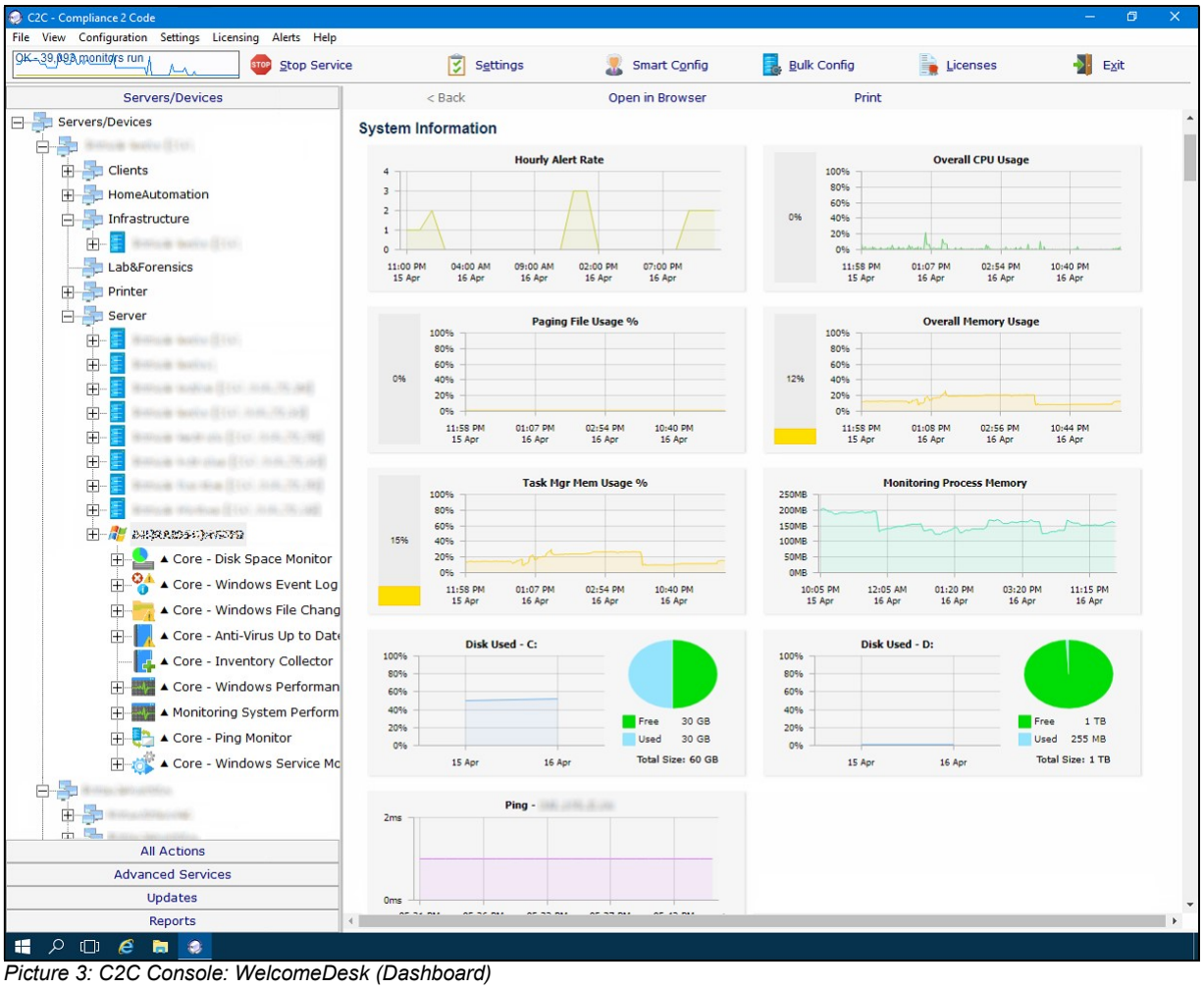
Picture 2: EIM Console: WelcomeDesk (Dashboard)

C2C - Compliance to Code

The DLP server consists of several different components. The components can be configured centrally via the DLP server console.
An overview of the core components, whose function and mode of action are also part of the C2C framework, is described in the C2C Product Capabilities.

Server Console

The central administration console offers configuration options on the left-hand side for devices, instances and management units. All server and device monitors are listed here with their control units and associated actions. The selected details are displayed on the right-hand side. When the console is started, the system information is displayed on the right-hand side.



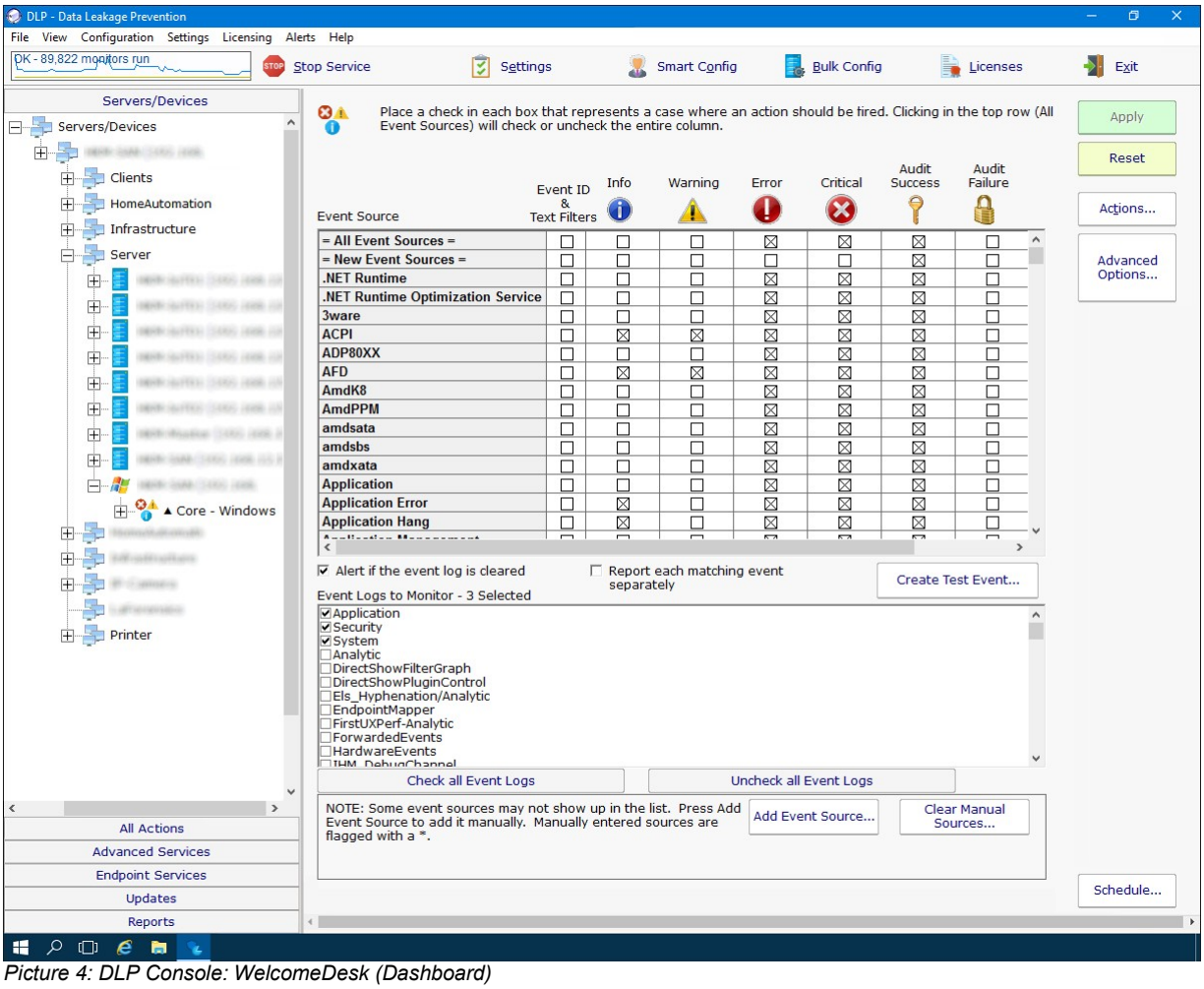
Picture 3: C2C Console: WelcomeDesk (Dashboard)

DLP - Enterprise Integrity Management

The DLP server consists of several different components. The components can be configured centrally via the DLP server console.
An overview of the core components, whose function and mode of action are also part of the DLP framework, is described in the DLP Product Capabilities.

Server Console

The central administration console offers configuration options on the left-hand side for devices, instances and management units. All server and device monitors are listed here with their control units and associated actions. The selected details are displayed on the right-hand side. When the console is started, the system information is displayed on the right-hand side.



Picture 4: DLP Console: WelcomeDesk (Dashboard)

Statement of Work - Overview:

The Statement of Work consists of:

- Introduction
  - Scope
  - Abbreviations and Acronyms
- Requirement
- Solution sketch and system design
  - Product Overview and Solution Outline
  - Solution Design
- EIM – Enterprise Integrity Management
  - Product Overview
  - Typical Installation (Console Main Install)
  - Integration Methods
  - EIM Service Network - Distributed Capabilities
  - EIM Service Network - Centralized Capabilities
- C2C – Compliance to Code
  - Product Overview
  - Typical Installation (Console Main Install)
- DLP – Data Leakage Prevention
  - Product Overview
  - Typical Installation (Console Main Install)
- EIM, C2C & DLP - Environment and Sizing
  - Operating System
  - Software
  - Memory
  - Disk Space
  - CPU Usage
  - Hardware
- EIM Server Console
  - Configuration Components Overview
  - System Information
- C2C Server Console
  - Configuration Components Overview
  - System Information
- DLP Server Console
  - Configuration Components Overview
  - System Information
- EIM Server
  - Use Case
  - Detector
  - Replicator
  - Scheduler
- C2C Server
  - Use Case
- DLP Server
  - Use Case
- Policies
- Actions
- Reporting
- Outlook
- Factory Acceptance

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