Data Protection

We offer complete design, implementation, and customisation support for access-rights management systems and data leakage prevention solutions. This provides valuable information used for detecting unauthorised access events and any possible data leakages

---

Cognosec Services

Features

Cognosec can assist you while implementing the correct architecture to protect your data.

Network DLP

Typically a software or hardware solution that is installed at network egress points near the perimeter. It analyzes network traffic to detect sensitive data that is being sent in violation of information security policies.

Endpoint DLP

Such systems run on end-user workstations or servers in the organization. Like network-based systems, endpoint-based can address internal as well as external communications, and can therefore be used to

control information flow between groups or types of users.

Data identification

DLP solutions include a number of techniques for identifying confidential or sensitive information. Sometimes confused with discovery, data identification is a process by which organizations use a DLP technology to determine what to look for (in motion, at rest, or in use).

Data leakage detection

Sometimes a data distributor gives sensitive data to a set of third parties. Some time later, some of the data is found in an unauthorized place (e.g., on the web or on a user's laptop). The distributor must then investigate if data leaked from one or more of the third parties, or if it was independently gathered by other means.[8]

Data at-rest

"Data at rest"" specifically refers to old archived information that is stored on either a client PC hard drive, on a network storage drive or remote file server, or even data stored on a backup system, such as a tape or CD media. This information is of great concern to businesses and government institutions simply because the longer data is left unused in storage, the more likely it might be retrieved by unauthorized individuals outside the Network.[9] In order to protect this phase of data, systems use methods such as access control and data encryption.[1]

Data in-use

"Data in use" refers to active data stored in databases that the user is currently interacting with. DLP systems that protect data in-use may monitor and flag certain unauthorized activities.

Data in-motion

"Data in motion" is data that is currently traversing through a network to an endpoint destination. These networks can be internal or external. DLP systems that protect data in-motion monitor sensitive data that is

being sent over a network through various communication channels such as email or IM

Description

The protection of sensitive data such as passwords, payment information, financial data, or intellectual property needs to a priority for organisations. With the establishment of security regulations such as the PCI DSS, HIPAA, and the EU Data Protection Directive, systems can be brought to a high standard of security, but the sheer number of threats targeting vital systems is dramatically increasing, so efforts towards protecting data should as well. Security breaches resulting in leaked data can become very costly to an organisation and to it’s clients should attackers get ahold of sensitive data. Cognosec can perform an assessment on the IT-infrastructure handling the data and can ensure that your sensitive data is properly managed . We offer complete design, implementation, and customisation support for access-rights management systems and data leakage prevention solutions. This provides valuable information used for detecting unauthorised access events and any possible data leakages

Specifications

The term data protection is used to describe both operational backup of data and disaster recovery/business continuity (BC/DR). A data protection strategy should include data lifecycle management (DLM), a process that automates the movement of critical data to online and offline storage and information lifecycle management (ILM), a comprehensive strategy for valuing, cataloging and protecting information assets from application/user errors, malware/virus attacks, machine failure or facility outages/disruptions.

Sweden
Cognosec Nordic AB
Birger Jarlsgatan 12
114 34 Stockholm
Sweden
Tel +46 (0)8 400 170 00
sales.se@cognosec.com

UK & Ireland
Cognosec Limited
3rd Floor
The News Building
3 London Bridge Street
London SE1 9SG
UK
Tel +44 (0)20 3870 1539
sales.uk@cognosec.com

Germany
Cognosec GmbH
An der Welle 4
60322 Frankfurt
Germany
Tel +49 (0)69 7593 8490
sales.de@cognosec.com

Austria
Cognosec GmbH
Castellezgasse 16/2
1020 Vienna
Austria
Tel +43 (0)1 212 2020
sales.at@cognosec.com

UAE
Cognosec DMCC
2202 Indigo Icon Tower
Cluster F
Jumeirah Lakes Towers, Dubai
UAE
Tel +971 (0)4 451 1552
sales.dxb@cognosec.com