DEFENDEER
Data Centric Security Solutions

Data-Centric Audit and Protection (DCAP)

These days, almost all business-related processes are controlled by a multitude of business applications that process, collect and store large quantities of data. Much of this stored data needs special protection due to legal, regulatory or internal company requirements. The protection requirements are determined by means of data classification, which involves grouping the data and assigning it defined risk values. Today's applications and their authorisation concepts are unable to keep up with current and future requirements for protecting the processed and stored data. Although modern applications already include an authorisation model (RBAC), they do not offer fine-grained control of «which user can see what data in which role», because the control of access rights is based primarily on the application's authorisations. The approach defined by the Gartner Group as DCAP primarily applies in cases where business processes enable broad access to data. In addition to real-time monitoring of all access to particularly sensitive data and an alert system for unusual behaviour, the data can also be dynamically masked on its way from the database to the user without changing the record itself. The actual data objects are only made available if the work process actually requires it or if the user needs it due to their function. The approach defined by the Gartner Group as DCAP primarily applies in cases where business processes enable broad access to data. In addition to real-time monitoring of all access to particularly sensitive data and an alert system for unusual behaviour, the data can also be dynamically masked on its way from the database to the user without changing the record itself. The actual data objects are only made available if the work process actually requires it or if the user needs it due to their function.

The solution: Data-Centric Audit and Protection with SecuPi

With SecuPi, data-centric approaches can be implemented simply and effectively so that data in applications and in the areas of data warehouse and big data are protected from unwanted access and leakage. Access to particularly sensitive data is logged and alerts are generated when unusual behaviour occurs. This ensures that data access remains transparent (records of processing). In addition, the data is dynamically masked when retrieved or moved and is encrypted when exported. One major advantage of this approach is that applications and business processes do not have to be modified (apart from installing an agent), yet the requirements regarding data access and possible abuse can be met in full.

DCAP disciplines – SecuPi functions

Function: Data Classification and Discovery
The identification of data objects with special protection requirements is central to the solution as a whole. The key is to understand which data is used or stored during which processes. SecuPi offers a variety of options for classification in this area. The resulting information is used for rule creation and masking.

Function – Data Security Policy Management
The technical measures to be implemented based on use cases are represented as rules in SecuP. The rules enforce the guidelines directly in the business processes and applications. Because the rules are managed centrally, priorities for protecting especially sensitive data can be implemented in a targeted manner.

Function – Monitoring User Privileges and Data Access Activity
Even in cases where existing applications provide a role model for permissions and access, SecuPi can be used to implement and ensure more detailed governance requirements that go beyond the existing capabilities of the applications. In other words, data streams of especially sensitive data can be controlled individually in everyday business for each user/user group based on these guidelines. This means that when data is accessed, alerts can be triggered due to unknown roles and unusual access. (see alerting function).

Function – Auditing & Reporting
SecuPi offers a range of functions to ensure transparency in terms of which user has access to which sensitive data when. In addition to the Records of Processing report, users can generate other reports and access analyses. Reports for internal and external audits or in response to requests for information are therefore available at all times.

Function – Behaviour Analysis, Alerting and Blocking
SecuPi enables the behaviour patterns (behaviour analytics) of application users to be recorded when they access sensitive data for longer periods of time. On the basis of use cases, these behavioural patterns are compared to the norm and logged as alerts in the event of deviations. The alerts can be checked by specialists and additional measures can be initiated depending on the situation. It is also possible to intervene directly in the work process and, for example, cut the current user connection or deny access to the data.

Function – Behaviour Analysis, Alerting and Blocking
SecuPi enables the behaviour patterns (behaviour analytics) of application users to be recorded when they access sensitive data for longer periods of time. On the basis of use cases, these behavioural patterns are compared to the norm and logged as alerts in the event of deviations. The alerts can be checked by specialists and additional measures can be initiated depending on the situation. It is also possible to intervene directly in the work process and, for example, cut the current user connection or deny access to the data.

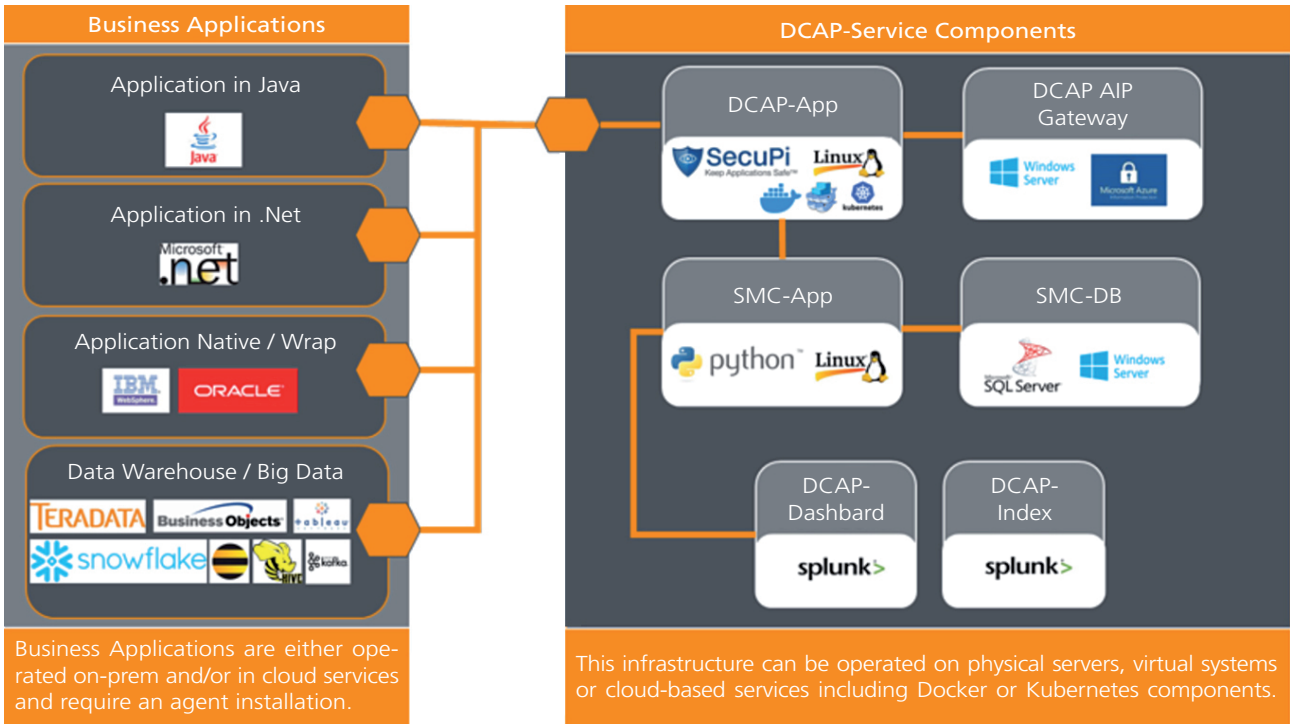
Function – Data Protection
There are a variety of options for encrypting the actual data objects, such as personal data. In this context, encryption means that the data is «hidden», «anonymised» or «pseudonymised» (encryption in motion) on its way from the database to the screen, so that the actual data is not visible to a user. However, the data remains unchanged in its original form in the source (e.g. database). As a result, unwanted access to data can be prevented in a targeted manner. This guarantees that optimal use is made of the «need-to-know» and «least privileges» principles and the right to be forgotten. If higher security requirements are to be implemented for individual data objects, these attributes (column, field) can be encrypted right at the source, e.g. the database (encryption at rest).If exports are initiated directly from the application (e.g. as a CSV file), the data is also masked with dynamic masking when exported. As an additional protective measure, the exported file can be encrypted directly via an encryption service (e.g. Azure Information Protection from Microsoft). These files can only be used within the company, because they cannot be opened elsewhere.

Security Event & Incident Management

All alerts are generated in the Security Monitor Center (SMC) and made available as an event or incident for analyses and evaluation and for triggering possible protective measures. The various tasks, such as assigning tickets to people (e.g. Security Operations Center), triggering notification emails using standardised templates, commenting on incidents and automatic processing are contained in the SMC. The SMC also serves as a reporting platform.

The architecture

DCAP can either be integrated in existing IT infrastructure at the customer's premises or used in combination with virtual servers or cloud-based solutions.



The technologies – our service milestones for DCAP

DCAP management application (console)

Management system for real-time monitoring and alerting and for protecting data through dynamic masking (pseudoanonymisation, anonymisation).

Security Monitor Center and Security Event & Incident Management

Management console for orchestrating processes and services via the central Security Monitor Center.

DEFENDEER Data Centric Security Solutions, a bluecoons group GmbH Division
Pilatusstrasse 3 | 6300 Zug/Switzerland | www.defendeer.com | +4141 552 02 95