ENTERPRISE SECURITY
ISSN 2691-4034
WWW.ENTERPRISESECURITYMAG.COM

PUTTING A FILE SYSTEM IN ORDER IS THE FIRST STEP OF A CYBER THREAT MITIGATION ADVENTURE

Publicly accessible day-to-day documents, and it should be all sorted which is a tough process. It's just because of how much information there's now in any average company. DCAP systems appear to be big helpers when it comes to facing all the corporate data management issues.

Properly deployed DCAP instruments will help organisations to:

Minimise the number of data breaches

Comply with corporate policies and general regulations

Detect computers which store documents containing critical information

Monitor user operations on documents

Conduct access rights audit

Restore lost information, the system creates shadow copies and saves all the versions of a document

The system can be tailored to the needs of any company. When categorising documents, a text, attribute, directory, computer, or particular combination can be specified so that only critical data, certain for a particular company, is controlled.

We've been living without DCAP tools, but now that we have them, we can't give them up

Use case: A confectionery factory (more than 300 PCs in the head office) purchased SearchInform software which helped establish that the company's accountant, after having been refused promotion, made a decision to covertly harm the employer. Since the situation about the refusal was known to the information security specialists, it was easy to figure out with the help of SearchInform FileAuditor that the disgruntled employee had corrected financial documents that had been stored on the file server. The documents could have been restored, again thanks to FileAuditor, but timely intervention saved the company time and money, which would have been spent on a fine when filing reports with the tax office.

First of all, DCAP is an approach with protection focusing on data. It makes you understand which data is stored within an organisation, where it is located and who can access it.

Alexey Parfentiev

These tasks could be solved even before. That's what clients say:

- Access can be managed via OS or NAS. Such functionality is implemented, though it's still quite primitive, in a data storage system. There are good RMS on the market.

- eDiscovery is another similar product, it helps detect a problem of improper storing.

- DLP can be also applied. The majority of systems now have a built-in eDiscovery function.

But all of these have shortcomings, as they:

- don't protect against unlawful access and don't control any current access rights

- don't monitor data lifecycle

- don't work proactively

- might overload the system and demand to much data storage system space

The major drawback of such a combined solution is that it is truly a zoo – plenty of creatures bundled together – try to work as a team thanks to exotic methods of an ultimately smart IT specialist/information security officer.

A DCAP is not a mere construction made of other systems

DCAP does incorporate functions of other systems – UEBA, SIEM, alternative AD, DLP, backup, which makes customers use them for atypical tasks as well. For me it came as a surprise that a client used our FileAuditor to save up data storage system space. He decided to back up not all the file storages, including trivial low priority files, but only really critical and valuable corporate documents.

DCAP can deal with ransomware. The system lets you minimise the overall area of the attacked perimeter, so that violators would get access only to that part of infrastructure which a user can access.

DCAP is the only software which supports access delimitation by content and not by context attributes, such as the format or location in a particular folder. DCAP will find out that a moved document is still subject to personal data or trade secret policies and the necessary measures will be taken as these policies will alert to a potential incident.

An open source DCAP is a waste of time and efforts

It's so difficult that the creation isn't worth it even for the biggest corporations. For example, Huawei has opted for integrating its OceanStor data storage system with SearchInform FileAuditor instead of developing the system on their own.

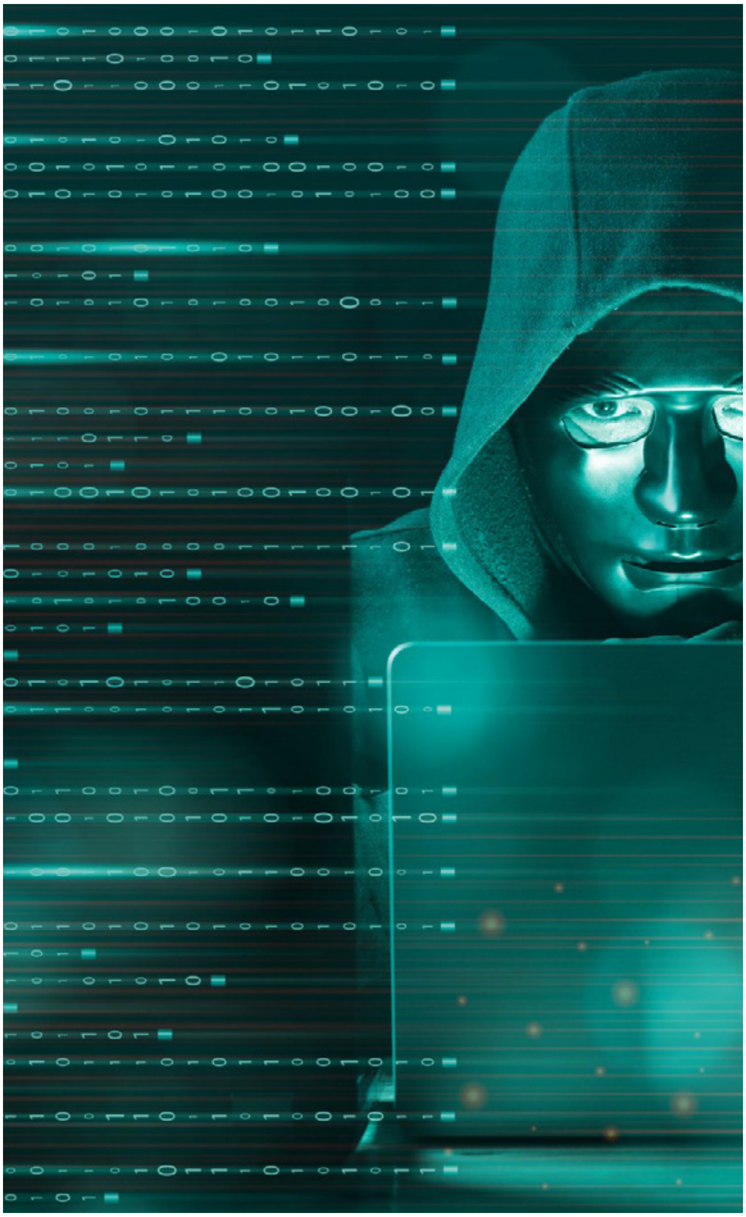
Let your company test a DCAP solution which is already on the market – your management will be surprised which documents are stored by your employees and how.

A customer gets so amazed is the amount of data a company appears to store. And many critical files are stored disorderly: personal and payroll or financial data, internal instructions, dozens of versions of some marketing plan and so on. Half of them are subject to GDPR, HIPAA, etc.

A DCAP is a proactive system – it should enable blocking as well as changing access rights in case of an incident

As soon as the purpose of DCAP is not to notify but to protect, proactivity is a must. Yes, there's always a possibility of a false alarm, but system configurations can be adjusted.

Customers need careful proactivity, as the main idea is not to harm business processes.



DCAP grows big

DCAP class of solutions keeps growing in popularity alongside DAG systems.

Logical way of DCAP evolution is its smart instilling in a wide family of security systems. SearchInform DCAP solution and the company's DLP system, for example, understand each other without any kind of "interpreter" or mediation: the first one tags documents, the second one reads those tags deciding on whether to filter a document or let it be sent. Those tags are recognised by other information security systems.

DCAP should be able to read metadata from other systems. For example, SearchInform FileAuditor reads from MS Office, where there are many important fields, such as author, owner, editor – thus, the system supports an option for an employee to tag his or her own document emphasising its importance.

DCAP might become a central element of a data protection system, because it's logical to begin with classification and tagging.

The data-centric ideology becomes recognised and omnipresent. DCAP functionality will be part of OS, the way it happened to antiviruses and firewalls.

To summarise, DCAP systems are becoming an inevitable engine in your overall mechanism, but not all of them provide truly needed features which are surely basic for the type. SearchInform FileAuditor guarantees smooth integration, smart blocking of suspicious activity with files, quick response to changes, integrated tagging in MS Office, inventory of operations on data and frequent data verification thanks to double-checking of only new files.

SearchInform FileAuditor solution's full version can be tried for free. ES

Enterprise Security Magazine is an enterprise technology magazine which reaches out to more than 41,000 qualified subscribers across the U.S, APAC and Europe and over 87,000 digital subscribers across the globe. It is the go-to resource for senior-level technology buyers and decision makers to learn and share their experiences with products/services, technologies and IT trends. We provide a knowledge platform to CISOs and senior IT executives to share their experiences and learn from each other along with short but in-depth articles about top providers in the IT sector.