zIIP offload up to 95%

SF-SafeDump®

Dump & log file anonymization to effectively prevent confidential data leakage and theft

Your goals

Eliminate all confidential data from your dump files

Ensure that all dump files remain technically fully usable

Rely on a comprehensive, efficient and transparent anonymization procedure

Prevent confidential data leakage via dump & log file anonymization

Did you know that **your company's IT staff sends dump files with highly confidential information to external third parties every** day and thus violates elementary security policies without even knowing it?

What, in fact, is a dump file? When more complex technical problems need to be solved, as in the case of an abnormally terminating ("abending") program, application or system, software vendors will ask for a so-called "dump", which captures every detail surrounding the error or problem. Such a dump file is a snapshot of the current status at the time of error, including all the required debug data, e.g. memory content, processor registers, any currently executed SQL statement, etc. While system programmers deal with system, memory, core or kernel dumps, application developers prefer to work with "user mode process dumps" or SQL dumps. Additional types result from other sources. Dump files easily become huge and may include a gigabyte or more of data. When browsing through a dump file you may easily feel overwhelmed by an almost infinite amount of purely technical information.

What is the security-related problem regarding dump files? For non-specialists these files look boring, or even worse, harmless, since most of the information seems to be binary or even cryptic, i.e. in a format unreadable to humans. No one will assume that these "ugly" dump files could include highly sensitive company secrets like confidential client information or security-related details of your systems.

How do secrets get into dump files? Dump files will include confidential and revealing information when the application and system memories are captured – for debugging purposes only, of course. Such a memory dump may include client names, account or credit card numbers, and many other kinds of critical data stored for processing the moment it was made.

How can you solve this high-risk security problem? Our SF-SafeDump solution finally prevents your dump files from including any confidential or security-critical data yet still remains completely technically usable for their actual purpose – to solve your software problems. Our expert knowledge based on more than 15 years of experience in this field guarantees the ultimate solution to this quite tricky and hidden problem.

Your IT staff will definitely support this kind of data leakage prevention ensured by our SF-SafeDump technology! Since fully transparent integration is ensured, SF-SafeDump always matches all current dump file handling and operational procedures established with your service partners. This means there is simply no impact on how your specialists currently transfer, compress, manage and analyze their dump files. These files simply become safe and compliant by no longer unveiling any secrets!

Finally you can fully enforce your data leakage prevention policies by including even the trickiest and most technical data leaks in IT: dump files. SF-SafeDump is **the only measure preventing any information leakage** resulting from frequently performed dump file exchanges between software users and their vendors. SF-SafeDump lets you enforce a modern and safe information provisioning policy to provide information on a need-to-know basis. Without dump file anonymization, your information leakage prevention policy will definitely not be up-to-date.

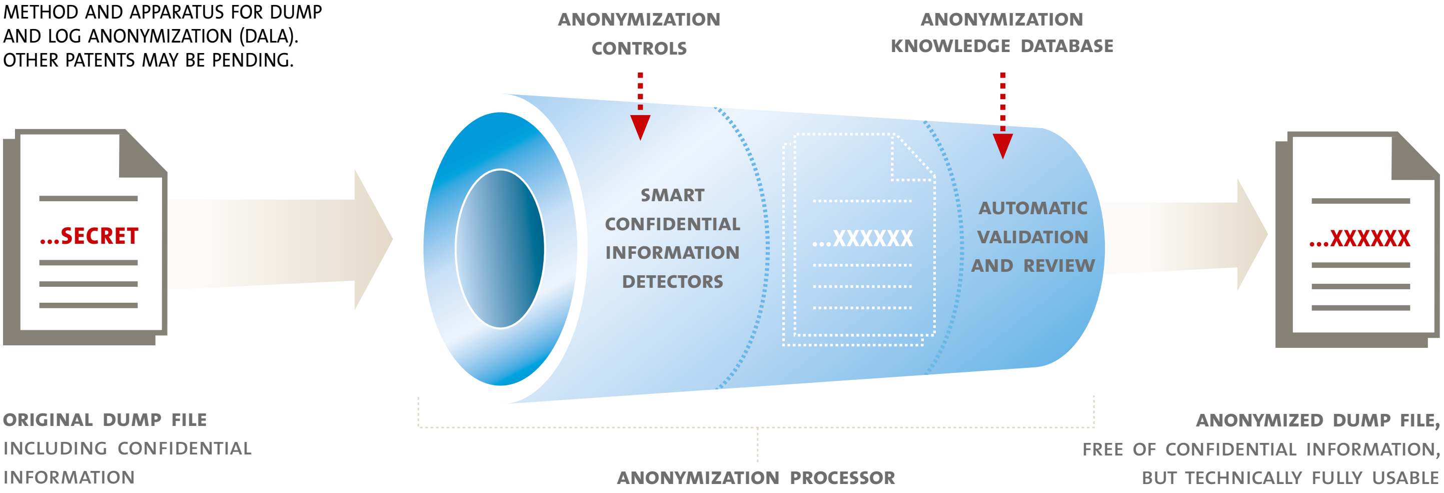
Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM

SF-SafeDump always prevents company secrets from leaking via dump files!

SF-SafeDump®

»YOU FINALLY STOP ANY DATA LEAKAGE RESULTING FROM DUMP FILES!«

US PATENT NO: 8,166,313
METHOD AND APPARATUS FOR DUMP
AND LOG ANONYMIZATION (DALA).
OTHER PATENTS MAY BE PENDING.


ANONYMIZATION CONTROLS
ANONYMIZATION KNOWLEDGE DATABASE
...SECRET
SMART CONFIDENTIAL INFORMATION DETECTORS
...XXXXXX
AUTOMATIC VALIDATION AND REVIEW
...XXXXXX
ORIGINAL DUMP FILE INCLUDING CONFIDENTIAL INFORMATION
ANONYMIZATION PROCESSOR
ANONYMIZED DUMP FILE, FREE OF CONFIDENTIAL INFORMATION, BUT TECHNICALLY FULLY USABLE

PERFORMANCE

FULFILL SECURITY AND COMPLIANCE OBLIGATIONS RESULTING FROM SOX, PCI, ISO, BSI, FERC, DOD, HIPAA, ETC.

SUPPORT FOR MAJOR PLATFORMS LIKE Z/OS, AND MORE

DETECTS ASCII, EBCDIC AND UNICODE

ESSENTIAL ALSO FOR CLOUD SERVICES VENDORS

STRONG REASONS WHY SF-SAVEDUMP® IS UNIQUE AND SO IMPORTANT

» **Why does the risk of data leakage and misuse increase with globalization and cloud computing?** It's a fact that the overall globalization of IT services makes updating a company's dump file exchange policy a vital necessity. Do you really know which parties and regions of the world or the cloud are effectively involved and will receive your dump files to solve technical problems? Be smart and obligate your cloud service providers and vendors, including their subcontractors, to also apply dump file anonymization. Otherwise, your secrets may "drop out of the cloud" whenever such vendors forward their dump files.

» **How can I explain this very special IT risk even more simply and effectively to management?** Quite easily! Just compare the hidden information phenomenon represented by dump files using an analogy from daily life. Giving dump files to software vendors is like sending a blood sample to a laboratory. Aside from performing the requested medical test to measure your cholesterol level, the lab could also check your current overall condition, including any allergies, genetic malfunctions and vulnerabilities, etc. you may have. Accordingly, the vendor's IT specialists, who analyze dump files to actually solve software problems, are also able to extract secrets from your dump file, or check your system configuration for any weaknesses in order to perform a highly efficient attack.

» **How can I explain the process of dump file anonymization more clearly and non-technically?** Consider a document shredder. However, unlike a shredder, SF-DumpAnonym leaves all the technical information in the dump file untouched and fully usable. Only confidential and security-critical information is removed in order to avoid any risk of abuse – it wouldn't support the debug process anyway.

» **We already send all our dump files encrypted! So, why do I need SF-SaveDump?** Encrypting dump files is an excellent idea. Congratulations! But encryption does not solve the actual problem. Any person who needs to process a dump file by using any debug or dump analysis tool will access the original, i.e. decrypted, dump file. Encryption primarily secures the transfer to the vendor. It does not prevent the dump file itself from including technically irrelevant, but highly confidential data. SF-SaveDump lets you continue to follow this strict encryption policy, only now you can send risk-free dump files thanks to complete anonymization.

» **What percentage of all dump files really includes secrets?** Isn't this an insignificant problem? Definitely not! Simply check the next system or kernel dump created on your production server. For sure, you would never forward it to any external third party without having passed anonymization. The risk involved becomes even worse, however, when products, applications or operating systems send dump files automatically, maybe even without your explicit permission.

» **We only cooperate with "world class" IT service companies. If we can't trust these partners, who can we trust?** Of course this is a strong statement, but only at first glance, since it primarily involves legal or formal liability concerns. One problem with dump files is that you can unwittingly provide confidential information to a third party without knowing what you have sent or enjoying an adequate level of trust. This implies that you will be ultimately liable for any abuse since you took the first step and delivered the information without request. But the ultimate argument in favor of SF-DumpAnonym comes from such IT company's current organization itself, which usually involves a high level of fluctuation and massive integration of subcontractors worldwide.

» **Let's save money and anonymize dump files with own scripts!** Comprehensive knowledge and a lot of research are necessary to achieve an error-free and technically fully usable dump file, while maximizing the level of anonymization at the same time. We know what we are talking about. Our company has been successfully dealing with dump files for over 15 years by providing powerful dump analysis tools and analyzing them during support. Therefore, anonymizing dump files is not as easy as removing secrets from a humanly readable document by performing a corresponding massive amount of global changes within an editor. Just searching for specific strings in order to remove or overwrite corresponding records, fully or partially, will quickly result in unusable dump files that fail their intended purpose. Such dump files will include a wide spectrum of highly complex and "tricky" faults causing the corresponding dump analysis tool to abort, and your staff will need to hand over the original dump file.

» **Finally, why doesn't Enterprise-IT-Security.com provide dump file anonymization as a service in the cloud?** We don't want access to your secrets. We can't be liable for what we don't know – it's that simple.

» **There is simply no doubt about it! The unique SF-SaveDump technology significantly improves your security and compliance levels. There is no easier way to avoid the actual unnecessary risk of confidential data leakage provided by non-anonymized dump files!**