TRUSTED SOLUTION FOR THE PROTECTION OF SENSITIVE INFORMATION

DATA SECURITY

NETWORK SECURITY  |  ENDPOINT SECURITY  |  DATA SECURITY
DATA CONFIDENTIALITY: ARE YOU READY?

NEGLIGENCE AND INDUSTRIAL ESPIONAGE ARE ONLY PART OF THE PROBLEM
An organization's most precious resources, information assets, are relentlessly exposed to numerous instances where its sensitive data is lost or stolen – malicious behavior from inside the company, the theft of computers, data leaks due to the exploitation of a vulnerability, unauthorized access to a computer or even the careless configuration of a security policy, etc.

NEW USER HABITS
With the growth of outsourced infrastructures, applications in the cloud and/or the mobility of collaborators working on multiple peripheral devices [including personal devices (BYOD)], organizations have no other option but to come to terms with new user habits. This transformation to the digital landscape increases exposure to the risks involved in sharing information.

IMPACT
All this presents a real cost to the organization:

- Loss of clients and/or projects
- Loss of the trust of coworkers
- Tarnished public image of the organization
- Publication of sensitive data such as R&D and product innovations
- Remediation in terms of human and financial resources

DATA THEFT IN A FEW FIGURES
Source: Ponemon

33% of incidents of data theft are linked to a malicious internal employee

2.55 M€ Average cost of data loss in France
Data protection
How confidential is your data?

Your unencrypted data is stored on a server. Do you know the level of protection or the names of your provider’s subcontractors? Do you know what country your data may be in?

ON-CALL TECHNICAL SUPPORT
Your client’s sensitive information (technical architecture, information on equipment deployed) is viewed on a mobile terminal. Is confidentiality guaranteed for your client?

RESELLERS
Your resellers are multi-brand entities with diverse partnerships and relationships. Would you like your sales practices to be made known to your competitors?

CREATING INNOVATION THAT SPELLS YOUR SUCCESS
Launching products requires sharing plans that, once communicated to a third party, are no longer considered a trade secret for your organization. What if an indiscretion took place and your idea was leaked?

DISMISSAL PROCEDURE IN PROGRESS
Are you able to guarantee the ethical behavior of a coworker holding on to unencrypted information on his computer or storage device? Would you take this risk?

SERVICES IN THE CLOUD
Your unencrypted data is stored on a server. Do you know the level of protection or the names of your provider’s subcontractors? Do you know what country your data may be in?

ON-CALL TECHNICAL SUPPORT
Your client’s sensitive information (technical architecture, information on equipment deployed) is viewed on a mobile terminal. Is confidentiality guaranteed for your client?
Preserve the confidentiality and integrity of your information while taking full advantage of the potential in cloud-based collaboration.

How do you guarantee the confidentiality of your business data when mobility has become part and parcel of everyday life? Is there a way to be protected from external interception or internal indiscretion?

Seamless and built into your usual communication tools, the Stormshield Data Security solution allows your specialized teams to create safe collaboration environments, regardless of the medium (e-mail, USB keys, etc), terminal (computer, smartphone) and application (collaborative, intranet, shared networks, etc.) used.

Its proven robustness, backed by its EAL3+/NATO certifications, means that Stormshield Data Security will ensure that you preserve the confidentiality of your projects from any internal or external indiscretion.

With Stormshield Data Security, your sensitive information is protected from end to end – when it is created, modified or transferred.

Advantages of the solution

- Fully turnkey solution (centralized administration, PKI, encryption agent)
- Comprehensive data security service based on a trusted infrastructure that we provide
- Certified solution
- Scalable solution: adapted to large-scale deployments (large groups) as well as projects or services

PROTECTION IN AN UNCONTROLLED INFRASTRUCTURE

- On-premises / Private cloud / Public cloud
- Vulnerabilities of datacenters
- Improper use leading to data leaks [e.g. recycling authentication credentials]
- Maliciousness of employees with privileges on the system, the network or in a database
- Interception of data over the network

PROTECTION FROM INTERNAL THREATS

- Malicious administrators
- Accidental data leaks
- Theft of peripherals
- Unauthorized access to workstations
STAY IN CONTROL OF YOUR DATA

Collaborating in total security has never been this easy

1. WORK
Create sensitive content in full security
Store confidential information on removable media
Exchange important data inside and outside the organization

2. DEFINE
Allow users to manage the confidentiality of their data
Allow users to define their trust bubble themselves
Manage data confidentiality and integrity

3. SHARE
Safely communicate through e-mails
Save files or volumes confidentially on removable media
Collaborate simply in workspaces over the network
Exchange sensitive information with external parties

4. GUARANTEE
Opt for strong authentication
Deploy a separate authentication method from the one offered by Windows
Reap the benefits of a trusted infrastructure
Erase data by rewriting over it
Separate security administration and IT administration roles

5. COLLABORATE
Integrate the solution easily into standard tools
Take advantage of the simple user experience
Benefit from features from various platforms
Arkoon and Netasq, fully owned subsidiaries of Airbus Defence and Space, run the Stormshield brand and offer innovative end-to-end security solutions to protect networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).