



STORMSHIELD

Data security

Protecting sensitive and critical corporate data



Cyber-serenity in accessing and sharing your sensitive data within your company or via Cloud collaboration tools



With today's proliferation of cyberattacks, the leakage of information – including personal data and confidential material such as patents, financial data and business processes – is an issue of growing concern.

Encryption solutions offer a very effective way of addressing this issue by ensuring the integrity and confidentiality of the most sensitive assets. They are also specified, among other things, as a technical solution for complying with the requirements of the GDPR.

In an increasingly open world in which collaborative interactions are growing exponentially, end-to-end security is essential for providing effective protection. Encrypted files come with their own protection, remaining protected regardless of where the data is located. Data protection management is completely independent of its storage: the system administrator manages solutions and storage, whereas sensitive data can only be accessed by authorised users.

Lastly, the encryption solution must be transparent, and – if it is to be widely adopted within the company – must not interfere with users' work practices.



Pierre-Yves Hentzen
CEO, Stormshield

Ensuring the integrity and confidentiality of the most sensitive assets

Enjoy optimal protection



Encryption everywhere

Encryption is applied end to end, and is exclusively controlled by the company. The file comes with its own security and, as a platform-agnostic solution, can be shared with total peace of mind on various Cloud platforms or within the company. The result

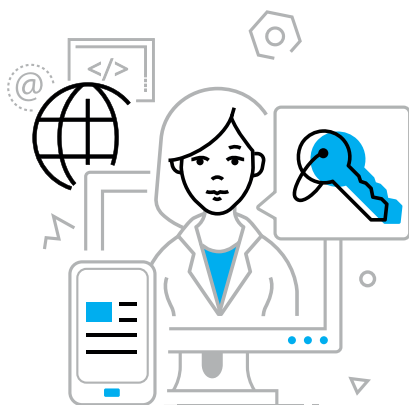
is that the encrypted file remains accessible regardless of where it is stored.

DATA
PROTECTION
DATA ENCRYPTION
IN GOOGLE
WORKSPACE



User-oriented protection

Never has an encryption solution been so simple and transparent for users, who can maintain their existing working practices. Users have direct control over the security of their data, specifying who has access to information and creating secure collaboration spaces.



The keys belong to the company

Encryption keys provide access to protected content, and form the critical point of any data protection solution. By retaining possession of the keys, you ensure that **sensitive data remains totally confidential**; nobody – not even a company administrator – can view the data.



Collaborative

Encryption in Gmail

Maintain control over the confidentiality of the sensitive data you exchange

GDPR

Encryption in Drive

Secure, effective collaboration

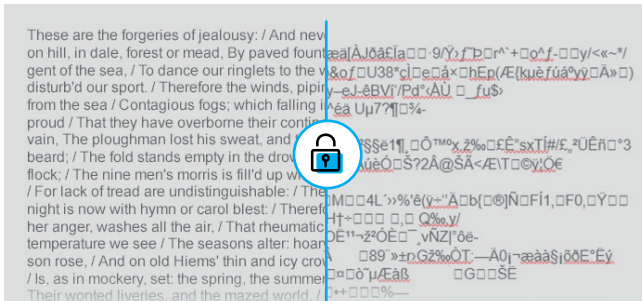


Combating the theft of sensitive information

Simple

Google Meet and Calendar encryption

Keep your meeting information secret and protect the data you share there



Key features

Trust

File and container encryption

Keep your most sensitive data secure



Confidentiality

Outlook email encryption

Get streamlined security for your email exchanges

In your collaborative tools or locally



Security

Encryption in OneDrive-SharePoint

Store data securely

Protect your data in your company

With Stormshield Data Security
Enterprise's transparent integration,
you enjoy automatic security for data
shared between internal and external
employees.



STORMSHIELD Data Security

A comprehensive protection suite

Stormshield Data Security Enterprise ensures the confidentiality of all data, from local file to email protection and including internal corporate collaborative spaces. This solution is easily integrated, regardless of whether or not the company uses Active Directory or a PKI.

Guaranteed confidentiality

Users play a central role in their own data security. They can specify who has permission to access their information, and can create secure collaboration spaces.

Easy management of zones of trust

This encryption solution is easily integrated into collaborative or communication tools, and is scalable and especially well-suited to global deployment, either by business unit or by project (BU or cross-functional services), and can also be used to safeguard exchanges with subcontractors.



Stormshield Data Security is the ideal solution for guaranteeing the confidentiality of data shared online, delivered via trusted encryption.

Without altering the user-friendliness and efficiency offered by OneDrive, Office365's SharePoint Online and SharePoint on-premise services, SDS enables IT departments to provide users with

collaborative services while controlling information security, facilitating a serene, secure transition to the cloud and digital transformation in your company.

The Stormshield Data Security solution is transparent and integrated into your usual Google workspace, enabling your business teams to create secure collaboration environments, regardless of the media, devices and applications involved.

Integrated into Google Workspace

Logging into your Google space activates data encryption. The Stormshield Data Security solution offers you the guarantee of secure communication with all users in your environment. This full integration ensures that all your employees enjoy the same user experience. One click is all it takes to activate data protection.

Secure your Google space

Set up user-oriented policies

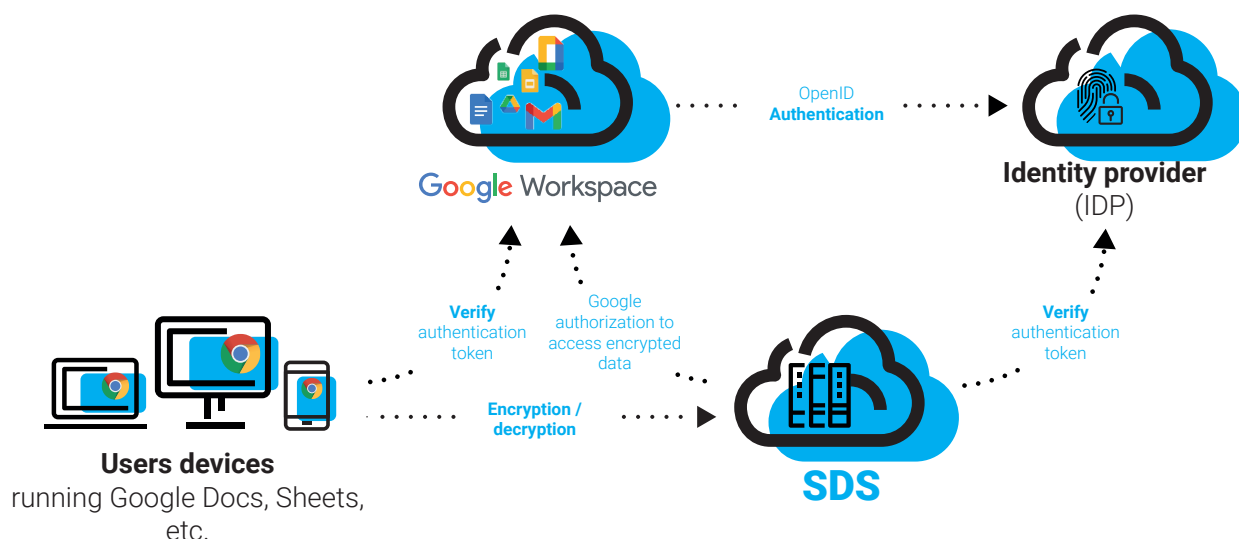
In addition to centralised security policies, the solution gives users the freedom to take decisions based on the sensitivity of the data they are handling. For example, the “encrypt all Cloud-stored data” policy ensures that data is accessible only to the author. The author can then decide for themselves who this sensitive data may be shared with.

Ensure separation of duties

Cloud data is stored on servers beyond the scope of the company. There must, therefore, be a guarantee that the administrators of these platforms cannot consult sensitive data. In addition to file access controls, the data is also protected by a key for authorised users.

SDS As a Service

The Stormshield Data Security for Google Workspace offer is a turnkey service offering sovereign data protection. The encryption, decryption and user key management processes are handled entirely by Stormshield.





Sovereign solution

As a major French cybersecurity player, we have been offering solutions that have been meeting European legal requirements for the last 15 years.



User empowerment

Users play a central role in their own data security. They can specify who has permission to access their information, and can create secure collaboration spaces.



Transparent encryption

Encryption is performed in real time in the synchroniser, thanks to the detection of synchronisation tools. The encryption is incorporated into the user's tools.



Secured collaboration

You are protected against the remote exploitation of vulnerabilities, the threat of a malicious internal user, and attacks specific to certain sensitive environments.



Agnostic protection

Information does not depend on Cloud services or providers, so it can move safely from one department to another, according to your requirements.



Technical support

Our technical support works closely with our R&D teams, so you benefit from the publisher's expertise.

.....

www.stormshield.com

.....

Find out more about Stormshield

Cybersecurity of networks and IT infrastructures

The core functions of Stormshield Network Security solutions provide comprehensive security and high-performance network protection. **Choose efficient, scalable security.**

Cybersecurity of industrial systems

Stormshield offers a holistic approach to securing the entire operational chain, **ensuring the availability, integrity and functionality of business processes** through a unique combination of IT and OT protection solutions.

Cybersecurity for workstations

Stormshield Endpoint Security is a standalone protection system that **dynamically tailors its security operations in response to its environment**. And at the same time, it analyses access to applications and company resources in response to the location of the workstation.