SMiD Business

Lock your data & keep your keys

Simple and Secure Solution for Enterprises and SMBs

- Network Attached Storage and Cloud Security Gateway
- Integrated On-Site and Off-Site Data Protection
- Robust Encryption, immediate, automatic and round the clock

EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND
A WAY TO MAKE EUROPE

SMiD Business is a device that merges Network Attached Storage (NAS) functionalities with many different cloud storage services in a way that your data confidentiality and integrity is assured. SMiD has been designed to be an extremely user friendly solution that complies with the strictest international data protection and privacy laws, because everyone –not just big companies- should have the ability to use cloud storage with total privacy and security.

Whether storing data at rest in your physical data center, a private or public cloud, or in a third-party storage application, proper encryption and key management are critical factors in ensuring sensitive data is protected and your organization maintains compliance.

While encryption is used in many contexts, it is only effective if properly deployed and following security best practices.

When evaluating any encryption solution you should ask these questions:

Why a device and not software?

SMiD is a **hardware device for security reasons**. It's the only reliable option to generate strong cryptographic keys. This also has another additional advantage: there is no client software installation required, nothing to install or configure. Extra of simplicity.

SMiD is a one in a kind product. It is the only one that allows the customers to have exclusively under their control: a dedicated device, the auto-generated cryptographic keys and the unique startup key.

Where can SMiD safely store the data?

SMiD delivers **total freedom to choose where the customers keep their data**, so they can regularly optimize their cloud usage and costs. SMiD lets them enjoy all the advantages of cloud storage, while simplifying information security tasks and keeping their reputation, credibility and integrity intact. **Private& Automatic Cloud Backup**. If they prefer not to use cloud storage, they can choose any local or private server as a provider. SMiD **is compatible with local and cloud storage** in a way that the data confidentiality and integrity is always assured.

SMiD Cloud
C/ Cristóbal Bordiú 35
oficina501
28003-Madrid

Contact:

smidcloud.com
info@smidcloud.com
Linkedin: linkedin.com/company/smid-cloud
Twitter: @smidcloud

Who control the keys?

With cloud storage provider encryption (CSP), the keys are always shared, or controlled completely by the CSP. Some systems provide customers with limited sharing control or work with cloud-based HSMs, but in practice, the cloud application always has access to keys and the protected data.

One of the main weaknesses of encryption software is that they run among thousands of other applications in the user's systems and so they are expose to malware.

Using a dedicated device, SMiD ensures it will remain uncompromised. SMiD follows security industry best practices **providing customers with exclusive key ownership.** Encryption keys are generated and managed inside the device, never go outside and only the user can turn the device on with his **physical startup key.** There is absolutely no way for others -except the owner- to have access to your cryptographic keys.

Who Protects the Data?

You are always responsible for your data, regardless of where it goes, and with SMiD you directly control encryption and never relinquish control to outsiders. **Robust Encryption is immediate, automatic and round the clock.** Encryption and decryption processes are always done inside the secure perimeter of the SMiD device and **only you can turn the device on with your startup key.** Nobody will have access to your cryptographic keys but you. In other solutions external encryption/decryption clients are required and they know the keys. This implies that they can access your data now and in the future.

Ransomware resistant

One of the main weaknesses of encryption software is that they run among thousands of other applications in the user's systems and they are easily infected by malware. Using a dedicated device, SMiD ensures it will remain uncompromised, it is Ransomware resistant.

SMiD connects to the LAN and encrypts all data at the source - before it leaves the office, clinic or international branch

Are There Protection Gaps?

SMiD eliminates all coverage gaps. From when the data leaves your office to when it returns it is never accessible until you decide to unlock it.

Will This Meet Regulatory Compliance?

Most regulations do not specify which technologies to use, but there is a strong consensus among compliance officers, auditors and regulators that encryption, if properly applied, is an important component of compliance. Other provider encryption does not meet most regulatory mandates because the data owner does not maintain exclusive control. **Encryption is only useful if you and only you control the cryptographic key and that is exactly what happens with SMiD Encryption**.

No client software installation required

SMiD is a plug and play data protection device. No client software installation is required. It's as simple as working with a network-attached storage (NAS) server, but with vastly more advantages. **Compatible with any infrastructure or operating system.**

Security independent of password or passphrases

Usually, software solutions don't have a strong key generation. They rely on a much weaker private password that needs to be remembered by a human being.

SMiD safeguards the data with long, internally-generated, random cryptographic keys and is bootable only with a unique startup key – that's in the customer's hands only.

It eliminates the local risks?

With SMiD only the files you are working on will be unencrypted. No unencrypted files will be permanently stored. If something happens to your office (fire, earthquake…) or someone steals your computer, or even your SMiD, you will not lose any data and your information will be safe. **No local risk of unwanted access, theft, loss or disaster**.

	CSP Encryption	Encryption Software	Encryption Gateways	SMiD
Hardware / software	Software	Software	Device	Device. Strong cryptographic keys
Where is the data safely stored?	Single-Cloud protection	Local and/or Cloud password derived encrypted storage	Single private cloud or on premise store provided by the owner	Total freedom to choose where you keep your protected data
Who control the keys?	The CSP controls keys and can access the protected data	Customer controls the keys but they are exposed to malware and other risks	The Encryption gateway use to receive the master key in this configuration	Controlled exclusively by the customer. Keys are never shared
Who Protects the Data?	The CSP encrypts the data and holds the keys	Customer protects the data but in a not fully controlled environment	The EG protects the data through an external cryptographic key	Customer controls their data and never relinquish control to outsiders
Protection Gaps	Clear text copies remain uncontrolled in the cloud memory	Clear text copies remain uncontrolled in the computer	No protection gaps as the gateway only process data but not store them	No protection gaps. Data always remains encrypted and are never accessible to others
Regulatory Compliance	Does not meet requirements for most data protection and data privacy laws	Does not meet most regulatory mandates if the computer compliance is not assured	Probably yes, because the gateway only have to comply the encryption/decryption requirements	Yes, only the customer control the cryptographic key material and all processes related with it
Client-side encrypted data storage	No client side encryption. Only a general browser is used to connect the cloud storage service	Client encryption/ decryption software whose integrity is not controlled	No client-side software is used. Data transport in clear text form up to the gateway interface	Dedicated device, SMiD ensures data cryptographic protection and file availability through it only
Security independent of password or passphrases	No. Usually all protections rely on a user's secret password	No. Usually all protections rely on a user's secret password	EG security depends only on the master key installed in configuration in it. No user interaction is required	SMiD protects the data using long and internally-generated random cryptographic keys, independent of the users
It eliminates the local risks?	Yes, if the cloud and the ISP provider are operative, and no local clear data are maintained	Yes, if no clear data are maintained in any local systems	No Apply, the EG don't stored any copy of the data that it process	No unencrypted files will be permanently stored. No local risk of unwanted access, theft, loss or disaster

	Cloud Providers	Encryption Software	Encryption Gateways	SMiD
Compatible with local and cloud storage	No	Yes	Yes	Yes
No local risk of unwanted access, theft, loss or disaster	No	No	No	Yes
Ransomware protection	No	No	N/A	Yes
Private&automatic cloud backup	No	Yes	No	Yes
Exclusive customer encryption keys ownership	No	Yes	Yes	Yes
Client-side encrypted data storage	No	Yes	No	Yes
Robust Cloud Encryption, immedia-te, automatic and round the clock	No, in most cases	No, in most cases	No in most cases	Yes
Long, internally-generated, random cryptographic keys	N/A	No	No in most cases	Yes
No client software installation re-quired	Yes	No	N/A	Yes
Security independent of password or passphrases	Yes	No	Yes in most cases	Yes
Local storage capacity	No	No	N/A	Yes
Unique startup key for the owner	No	No	No	Yes
Any infrastructure or operating sys-tem	Yes	Yes in most cases	Yes	Yes
Provider Independence	No	No	Yes	Yes

SMiD Cloud revolutionizes storage and data protection for SMBs and enterprise branch offices with SMiD Busi-ness, a hybrid solution that combines secure cloud storage services with on-premises storage appliances for a seamless user experience. SMiD Business provides a cloud services platform that enables service providers and IT resellers to quickly deliver cloud storage, hybrid local/offsite data protection to their customers.

For more information, visit smidcloud.com.

SMiD Cloud Security