# What is Data Security and Why is it Important?


The Storage Networking Industry Association (SNIA) defines data protection as an “assurance that data is not corrupted, is accessible for authorized purposes only, and is in compliance with applicable requirements.” This means “data integrity” where said data is only “usable for its intended purpose” – the data must be accessible but only to desired parties. Furthermore, performance must remain acceptable while meeting compliance, this

last part referring to organizational, federal, or legal requirements. The move towards SSDs and the cloud has made these issues more critical, not only because data is more at risk but because there's more sensitive data being stored.

Several factors are driving the adoption of encrypted storage in recent years, according to security experts. This includes the fact that data has its own higher value versus the hardware itself, that a lot of sensitive data is coming out of retirement and must be handled properly, and there are many new rules and regulations in both the corporate and governmental world for data protection. The obvious example is of a misplaced business laptop, but now smartphones and other mobile devices are prevalent in a wireless world with virtual identities. Illegitimate physical access remains a primary but not the sole concern in an increasingly cloud-based economy.

Within recent years the amount of hacked or ransomed businesses and government agencies has skyrocketed, from leaked credit card databases to police department records. As time goes on the storage – hard drives also, but increasingly SSDs – needs to be retired or replaced due to age and growing capacity requirements. The ability to safely store and erase this data is therefore critical to protect sensitive information. As such, corporate policies and government regulations for data protection have been augmented to protect everything from intellectual property to customer and client data.

Cloud and data center operations especially require security and robust encryption. For example, encryption-in-transit using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to prevent different sorts of attacks such as someone trying to intercept the message in transit, the so-called "man in the middle" attack. The data residing on cloud servers is also encrypted-at-rest to prevent physical theft. Naturally, the best policy is end-to-end encryption which includes encryption-in-use as you have when data is only decrypted at the client end. On the server side, this requires several technologies and techniques as described below to meet FIPS and other compliances – this could include hardware encryption with TPMs and the native ability to use cryptographic keys to securely delete data on SSDs.

## Data Erasure

The Blancco Technology Group lists six key situations where data erasure is necessary: at equipment end-of-life (EOL), during data migration, at data end-of-life, with employee departure, at customer demand, and after

disaster recovery. End-of-life means when the hardware is resold or discarded or when a project is definitively ended. As capacity and performance needs increase data is often migrated from server to server or between virtual machines and the source must be prepared for new information. It's not enough that data in transition is protected, both source and destination require security.

There have been many horror stories about disgruntled former employees with regards to the theft or ransoming of crucial data. Even with proper safeguards, it is necessary to make sure that any and all hardware is securely erased on termination. As for the clients, many new regulations – such as the EU's "right to be forgotten" laws – require that users have recourse to make sure their personal data and privacy are protected. Quite often it is found that data has been retained for months or years after the event during later security audits following breaches. This includes backup copies for disaster recovery which must be properly maintained and eventually erased, to maintain continuity as well as for security.

With hard drives, it was common to do intensive overwriting before retiring a drive, although more serious methods of degaussing (magnetic) or physical destruction were not uncommon. A simple delete or format has been and remains insufficient. SSDs instead have some features built-in, including secure erase, sanitize, and cryptographic erase. While the typical ATA Secure Erase deletes the mapping table, a Sanitize command goes further and erases all data as well – specifically in an uninterruptable manner as it is continued on any power-on with the chances of reconstructing any data being effectively zero. A Crypto Erase instead erases the encryption key for a self-encrypting drive (SED).

## Drive Encryption

Drive encryption has two primary schemes, that of file/folder encryption and full-drive encryption (FDE), which rely on the Trusted Computing Group's (TCG) protocols and Federal Information Protection Standard's (FIPS) government requirements. Encryption in the basic sense is a mathematical method utilizing algorithms and features like a true random number generator (TRND) to prevent the

deciphering of sensitive data by outside parties. Encryption strength is based not only on the standard used but the size of the cryptographic key. For example, most commonly the Advanced Encryption Standard (AES) is used with 256-bit keys, a combination known as AES-256. Also common is the Secure Hash Algorithm (SHA-256).

TCG's Opal Storage Specification, or just Opal for short, is the most commonly supported Security Subsystem Class (SSC) protocol, with Opalite and Pyrite as derivative subsets. This specification utilizes AES-256 hardware encryption and also pre-boot authentication (PBA) for client machines – this is performed in BIOS/UEFI with password protection to protect against rootkits and similar attacks. While this has advantages over software encryption – with regard to performance, security, upgrades, plus key deployment and management – it is reliant on the manufacturer to the point that some companies, such as Microsoft with regards to BitLocker, have suggested using software encryption instead.

File/folder-based encryption has the advantage of hierarchical permission control through the network and security policies and also can protect only data that is specifically sensitive. Further, data can be protected in transit, a surprisingly relevant issue – recent inter-company email leaks had weakly-protected zip files become exposed as that method was used to bypass security policy, for example. Full-drive encryption, on the other hand, can rely on a Trusted Platform Module (TPM) to tie it to a specific platform, and potentially data at risk, such as that in the swap file, is protected. This also allows for a secure authentication scheme. SED as a feature of many SSDs is a subset of full-drive encryption.

## Further Information

The basic U.S. government computer security protocol is the Federal Information Processing Standard 140-2 (FIPS 140-2) with 140-3 being the recent successor. This includes four levels of security. The first requires basic security of the encryption engine and firmware. The second requires evidence of tampering. The third must additionally have resistance to tampering. The fourth and last must-have attack detection with also the ability to cryptographic destroy information in the event of a potential breach. These criteria are specifically applied to the validation of cryptographic modules.

With regard to information technology (IT), there is the National Information Assurance Partnership (NIAP) which includes Security Functional Requirements (SFR) and Security Assurance Requirements (SAR). These standards specifically relate to the U.S. government while other governments or governmental bodies may have differing protocols. More generally, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have the 27040 technical guidance. The controls therein cover backup and recovery systems, continuous data protection (CDP), and replication technologies, emphasizing that “all the data protection solutions should be viewed as data resilience mechanisms” according to the SNIA.

To learn more about encryption and security in SSDs,  please contact us here.

## Our SSD Solution

Our ED1 PCIe™ Series is a powerful, high performance SSD made for edge storage applications. It comes in M.2 and U.2 form factors.

Our ER2 SATA SSD Series delivers affordability and performance with superior random read/write speeds of up to 90,000/45,000 IOPS. It comes in M.2 and 2.5" form factors.

Specifications and features are subject to change without prior notice. Images are samples only, not actual products. Please check with a Solid State Storage Technology Corp. representative for details.

**Request Full Specs Sheets**

# ABOUT US

A subsidiary of KIOXIA Corporation, **Solid State Storage Technology Corporation** is a global leader in the design, development, and manufacturing of digital storage solutions.  We offer a comprehensive lineup of high-performance customizable SSDs for the Enterprise, Industrial, and Business Client markets. With various form factors and interfaces, our SSD solutions help businesses simplify their storage infrastructures accelerating variable workloads, improving efficiency, and reducing total cost of ownership.



**Learn more at** www.ssstc.com