V. 06/20

SecurStor Security Suite

Fortified Security for Mission-Critical Applications

SecurStor is ATP's answer to the growing data security concerns in the industry. It helps protect mission-critical applications against unauthorized access to data or systems. Its feature range includes, but goes far beyond, conventionally available data-at-rest protection mechanisms and can be customized to the individual requirements of an application or a system.

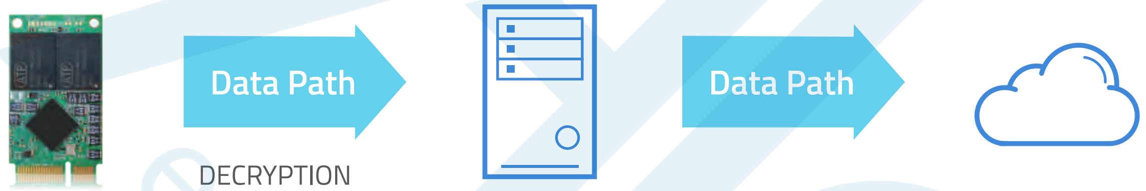
SecurStor

v1.0

Unique Challenges

The Internet of Things (IoT) and its implementation in the industrial segment (IIoT) are modern-day realities where everything is increasingly becoming interconnected. This unstoppable phenomenon is creating not only limitless opportunities but also greater security threats and vulnerabilities. In mission-critical industrial applications, standard security solutions already integrated in storage devices may not be enough as these generally provide protection only for data at rest.

The table below shows the possible risks and types of protection mechanism typically employed for specific data states:



	Data at Rest	System & Network Levels
Definition	Data stored on media, not in use	Data in process and/or shared in cloud/network
Possible Risks	Theft of HW, "unsafe disposal"	Malware, spyware, ransomware, unauthorized access
Protection	OPAL, eDrive	ATP custom features

The ATP SecurStor Solution

Data-at-Rest Protection

Most SecurStor enabled storage products are shipped with data at rest security features by default, providing protection for data that is stored on the media. These features include AES-256 encryption, TCG OPAL, eDrive or Self-Encrypting Drive (SED) and they help assure that in case of a loss or theft of the storage media the data stored on it is still protected from unauthorized access.

Custom-Built Security Solutions

In the connected world, data frequently travels between multiple locations. However, as soon as it leaves a storage media, e.g. to run in a system or be sent through a network, data-at-rest protection mechanisms fall short as they are only able to protect data that remains inside. ATP SecurStor includes a variety of options that go beyond data-at-rest protection. These features can be customized to specific application requirements and help protect against unauthorized access, illegal copying or ensure data, O/S or FW integrity.

ATP Securstor-Enabled Products

SD & microSD Cards*

Key Features

- SecurEncrypt: AES-256 encryption for the User Data area
- SecurWipe: Fast, safe and permanent removal of data
- SecurCopy: Pairs the storage device with a specific type of customer device to prevent illegal copying
- SecurWrite: Puts the device into “Write-Once” mode
- SecurAccess: Read protect and write protect

LEARN MORE

SATA & PCIe NVMe™ SSDs*

Key Features

- Data-at-rest security features, including SecurEncrypt, TCG OPAL, Microsoft eDrive
- SecurWipe: Ensures fast, safe and permanent removal of all data
- SecurOS and SecurBoot: Enables SSDs to assure they have not been compromised before they boot up and log on to a network and may include self-healing mechanisms in case invalid data is detected
- ATP is partnering with leaders in Storage security to provide advanced storage and system security protection

LEARN MORE

Managed NAND*

Key Features

- Data-at-rest security features, including SecurEncrypt, TCG OPAL
- SecurWipe: Ensures fast, safe and permanent removal of all data

LEARN MORE

*Actual availability of specific features may vary by product and capacity. Please contact ATP for details.

SecurStor Features

Feature and Description	SecurStor-enabled SD & microSD Cards	SecurStor-enabled SSDs	SecurStor-enabled Managed NAND Solutions
UniqueID Hardware-based product identification, using physically unclonable function (PUF) technology where needed.	*	*	*
SecurBoot Ensures the integrity and validity of the storage device's firmware image.	**	**	**
SecurUpdate Ensures the integrity and validity of any update to the firmware.	**	**	**
SecurAccess Password-protected access to all or part(s) of the User Data area.	**	**	**
SecurOS Ensures the integrity and validity of the operating system or application image stored in the User Data Area.	**	**	**
SecurCopy Pairs the storage device with a specific type of customer device to prevent illegal copying.	**	**	**
SecurWrite Puts the device into "Write-Once" mode.	**	**	**
SecurEncrypt AES-256 encryption for the User Data area.	*	*	*
TCG OPAL and other features defined for data storage devices by the Trusted Computing Group.	***	*	*
SecurWipe Fast, safe and permanent removal of data by deleting the encryption key.	**	**	**

* Default ** Optional *** Not Available for this form factor