Secure your storage with data-at-rest encryption when regulatory mandates or the need to protect intellectual property from security breaches dictate. HP 3PAR StoreServ Data-at-Rest Encryption protects data from both internal and external security breaches. If your application or environment requires protection from unauthorized access of the data on a drive, then consider the HP 3PAR StoreServ Data-at-Rest Encryption solution. With this solution, HP 3PAR StoreServ is configured with self-encrypting drives (SEDs).

HP 3PAR StoreServ 7000, 7450, and 10000 models are available with drives SEDs, where data is encrypted as it is written to the drive. You have the comfort of knowing that all data contained on these drives is protected against unauthorized access, including hardware theft, failure of a drive or drive retirement.

Figure 1. HP 3PAR StoreServ Data-at-Rest Encryption with Local Key Manager
Features and benefits

Secure sensitive personal information according to regulatory mandates

- Encrypt electronic medical records for HIPPA compliance to provide patient confidentiality from unauthorized or inadvertent disclosure
- Comply with payment card industry regulations that define requirements for protection of cardholder data
- Protect intellectual property or other sensitive business data by encrypting data

Encrypt data easily with no user intervention

- All data on the HP 3PAR StoreServ Storage System is encrypted as it is written to the drives, and unencrypted as it is read from the drives. In the event of a drive failure, the data is protected from unauthorized access because the drives are set to lock on powerfail and would need the authorization key to unlock.
- The encryption process happens inside the drive architecture without any user intervention.
- Local Key Manager (LKM) included with the HP 3PAR StoreServ encryption license is used to manage all drive encryption keys within the array and provides a simple management interface.

Mitigate internal and external risk

- HP 3PAR StoreServ provides proper key management that is critical to maintain separation of duties and protection against improperly cared for disks or malicious intent from remote office employees.
- Encryption protects against disk drive theft and unscrubbed disk drives that repurposed.

Maximum data security

Protecting personal information, like patient records, banking details, is no longer a choice in many data centers; it a mandate or even a legal requirement. Even when it’s not required, good business practice warrants protection of your company’s intellectual property from unauthorized access. Data-at-rest encryption with HP 3PAR StoreServ Storage System mitigates data exposure as the result of losing physical control of disk drives, which can happen when drives are decommissioned at the end of their life, when they are returned for warranty replacement or repair or when they are stolen.

HP 3PAR StoreServ Data-at-Rest Encryption supports full disk encryption (FDE) based on the Advanced Encryption Standard (AES) 256 industry standard. AES is a specification for the encryption level of electronic data established by the U.S. National Standards of Institute and Technology (NIST) in 2001. AES is a symmetric key algorithm that uses the same key for encrypting/decrypting the data on the hard disk drive or solid-state drive. All data is encrypted prior to being written to the array. As data is read from the array, it is decrypted. All encryption and decryption is handled at the drive level and needs no other external mechanism.

The benefits of FDE encryption include:

- Government standard-based encryption—industry-wide standard
- Uses AES-256 encryption standard
- Dedicated engine for full speed encryption contained on every drive
- Encryption key is unique to each band and protected on the media
- Encryption key itself is encrypted when stored on the media

HP 3PAR StoreServ Data-at-Rest Encryption is supported with HP 3PAR StoreServ 10000, HP 3PAR StoreServ 7450, and HP 3PAR StoreServ 7000 models.
Minimize data loss with self-encrypted drives

HP 3PAR StoreServ Data-at-Rest Encryption utilizes SED, which are hard drives or solid-state drives with a circuit built into the drive’s controller that encrypts and decrypts all data to and from the media automatically.

This method of encryption ensures data contained on the drive is protected due to loss of equipment through either unauthorized access or a drive failure. In the event of a drive failure, or if an encrypted drive is removed from the array, the data resident on the disk drive is protected from any unauthorized use due to the data key, which is generated on the drive. The drive is protected from unauthorized use, because it is set to lock on powerfail and requires an authorization key to unlock.

When the storage system is retired or taken out of service, the SEDs can be securely erased prior to the disks being repurposed, ensuring that no data remains on the SEDs. Instant and secure erasure of the data is enabled through simple administrative processes.

- Keys are generated on the drive.
- Encryption key never leave the drive.
- Encryption cannot be turned off.
- Key management is done at the array level and implemented by an LKM.

Access authentication with local key management

The LKM module, which is part of the HP 3PAR OS and integrated with the HP 3PAR Management Console, handles key management functions including enabling encryption, key backup, rekey, and key recovery. The LKM is the process on HP 3PAR StoreServ that unlocks all drives in the array for reads and writes with single authentication keys. Authentication keys are enabled using the HP 3PAR Cluster ID and then stored in the local key store on the array.

The authentication keys are owned by a superuser with support for rotation of authentication keys. Only a user in a key manager role can be responsible for physical security of backup of the authentication keys.

When a SED drive is no longer powered on, the drive goes into a locked state and requires an authentication key to unlock the drive when power is restored. In the event of a drive failure or theft, a proper key sequence needs to be entered to gain access to the data stored within the drive. Without the key, access to the data on the SED is not possible.

HP Factory Express

HP Factory Express provides customization and deployment services along with your storage and server purchases. You can customize hardware to your exact specifications in the factory—helping speed deployment. Visit hp.com/go/factoryexpress.

Customer technical training

Gain the skills you need with ExpertOne training and certification from HP. With HP Converged Storage training, you will accelerate your technology transition, improve operational performance, and get the best return on your HP investment. Our training is available when and where you need it, through flexible delivery options and a global training capability. hp.com/learn/storage

HP Technology Services

Choose from a rich portfolio of services to make the most of HP Storage, so you can move with confidence to take full advantage of the broadest, most advanced portfolio in the industry.

Discover, plan, and design—understand your options and build it right from day one:

- HP Backup Recovery Efficiency Analysis
- HP Backup Recovery Impact Analysis
• HP Backup Recovery Modernization
• HP Storage Cloud Design Service

**Deploy and integrate**—increase uptime and decrease risk as you free up your resources:
• HP 3PAR StoreServ Storage Installation and Startup Service
• HP 3PAR Software Installation and Startup Service
• HP EVA to HP 3PAR StoreServ Acceleration Service
• HP Data Replication Solution Service
• HP Enhanced Implementation Service for SANs
• HP 3PAR Adaptive Optimization Policy Implementation Service
• HP Storage Virtual Volume Design and Implementation Service
• HP Thin Volume Conversion Service
• HP 3PAR StoreServ Health Check
• HP Performance Analysis Service
• HP 3PAR Rebalance Service
• HP 3PAR Storage Assessment Service
• HP Proactive Select

**Operate and support**—meet service level agreements (SLAs) with the right support level. Choose from three levels of operate and support care:
• Optimized Care—delivers the highest levels of performance and stability through deployment and proactive management practices
  
  HP Critical Service
  Additional options: 10 HP Proactive Select credits per year, per array
• Standard Care—maintains high level of uptime, along with expert help to cut the cost and complexity of implementation and support
  
  HP Proactive Care 24x7—plus, 20 credits per year, per array
  Additional options: HP Proactive Care Personalized Support (once per each new Proactive Care support environment), HP Personalized Support Additional Day, and an additional 10 HP Proactive Select credits per year, per array
• Basic Care—minimum recommended support
  
  Proactive Care 24x7—plus, 10 credits per year, per array
  Additional options: 10 Proactive Select Credits per year, per array

If none of our support recommendations meet your needs, we can tailor a service solution for your unique support requirements. Only HP brings together deep expertise, proactive and business-critical support and a strong partner network—plus, a full set of infrastructure services designed to power a converged infrastructure.

For more information, visit [hp.com/services/storage](http://hp.com/services/storage).

**Learn more at**
[hp.com/go/3parstoreserv](http://hp.com/go/3parstoreserv)