

Encrypted disk design based on NVMe Namespace

Presenter: He Meng

Firmware Test Director

meng.he@starblaze.com

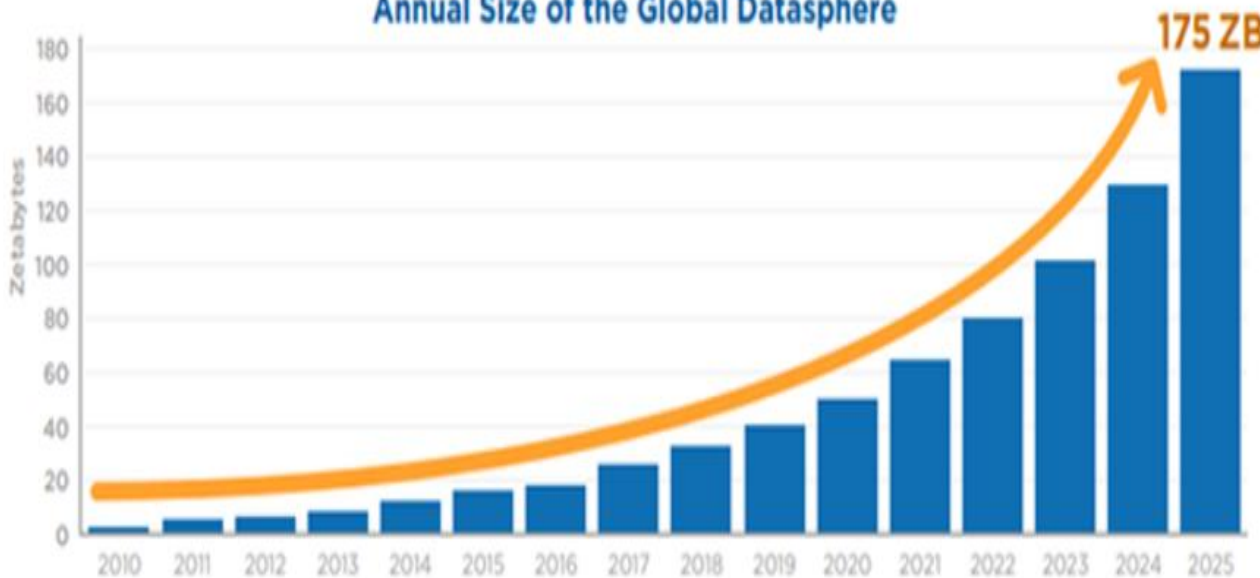


According to the IDC report, the annual size of global data will increase from 40ZB to 175ZB. Nearly 90% of the data require varying levels of security protection.

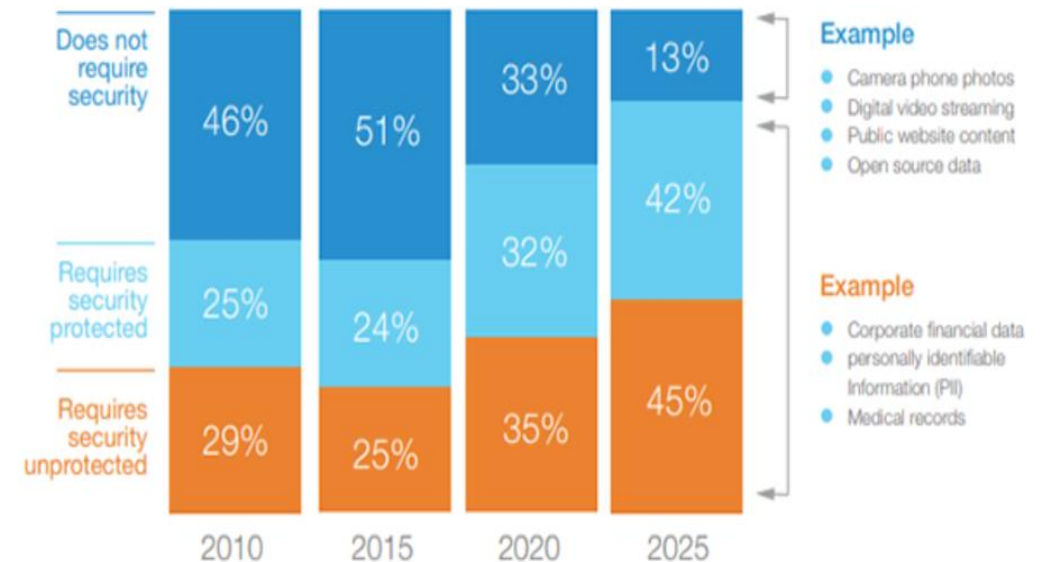
Research shows less than half of the data is actually protected.

The demand for security technologies continues to increase in the industry.

Annual Size of the Global Datasphere



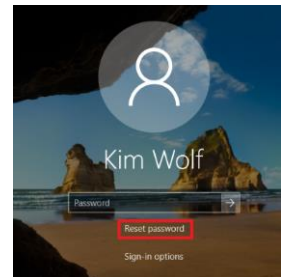
Source: Data Age 2025, sponsored by Seagate with data from IDC Global DataSphere





Host-Based security technologies

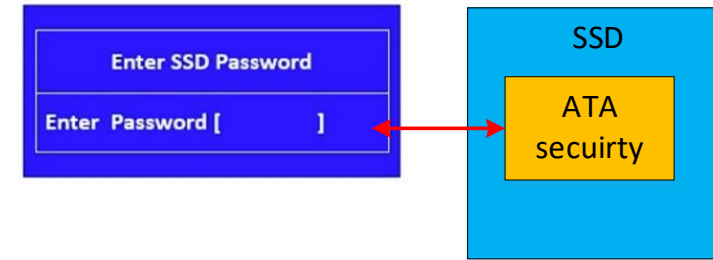
1. **Software Encryption:** Microsoft Bitlocker(OS) and Chinasec(Application)
2. **Security authentication:** Windows login password
3. **Hardware encryption:** TPM(Trusted Platform Module) Protect user data by integrating a security module to implement RSA/AES/SHA encryption algorithms and password management.



Device-Based security technologies - ATA security & Shadow area

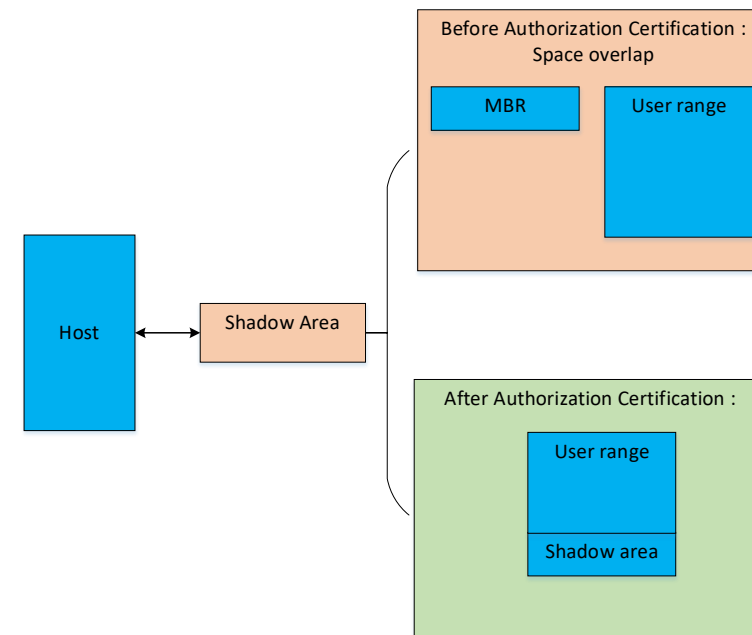
ATA security:

- ATA -> SCSI -> NVMe
- Boot Device
- Access Control to whole disk



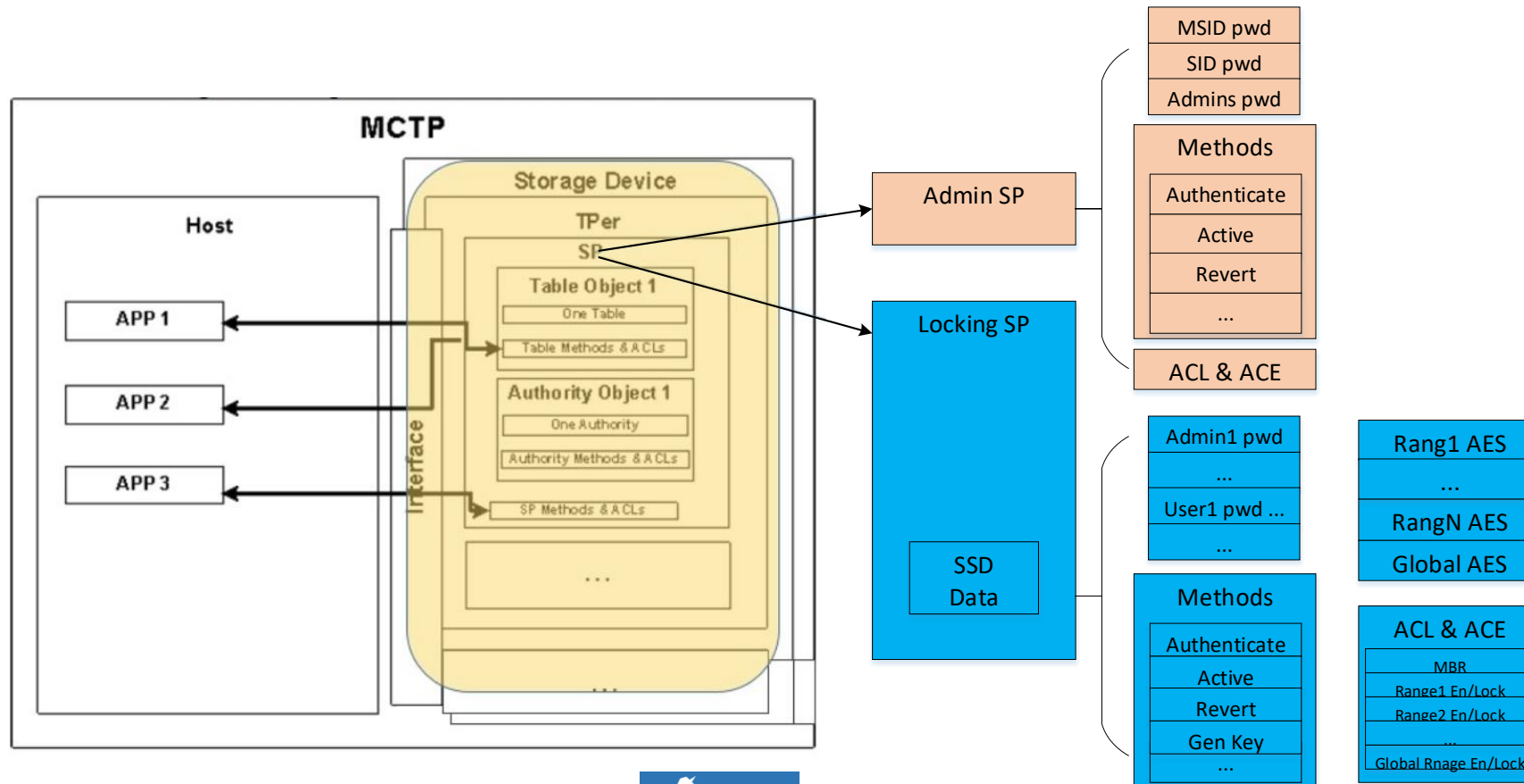
Shadow area

An additional partition, invisible to the host until authenticated



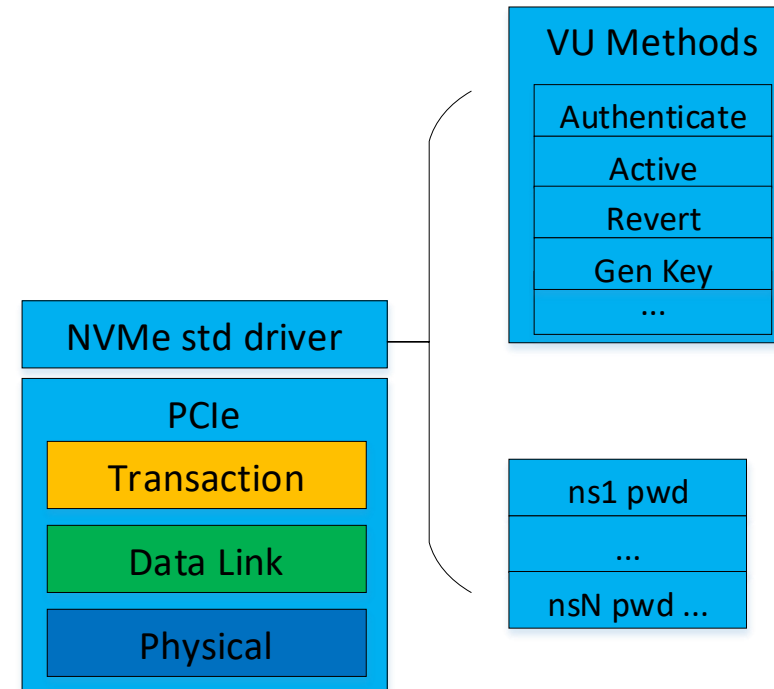
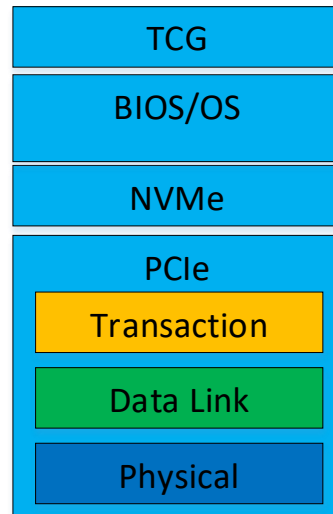
Device-Based security technologies - TCG

- Sector specific permissions
- Self-encrypting



Namespace encryption benefit

- Devices-based
- Namespace isolated security configurations
- Multi-platform(only need native NVMe driver)
- Easy to Use API (GUI、Vendor Specific cmd)



Demo on windows:

Support:

- 1.Namespace management(create, attach etc.)
2. Query security information of specific namespace.
3. Password management



Demo on Linux:

忆芯SSD口令工具

刷新

PassWordSet

用户口令

●●●●●●●●●●

●●●●●●●●●●

确认 取消

删除口令

```

root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# nvme list
Node          SN              Model                      Namespace Usage          Format          FW Rev
-----
/dev/nvme0n1   C1PSMYP007001   S1200ITT2-T2M21T-NZ        1          274.88 GB / 274.88 GB   512 B + 0 B   dd026
/dev/nvme0n2   C1PSMYP007001   S1200ITT2-T2M21T-NZ        2          274.88 GB / 274.88 GB   512 B + 0 B   dd026
[root@localhost ~]# nvme read /dev/nvme0n1 -c 8 -z 4096 -d data -s 128
Rounding data size to fit block count (4608 bytes)
read: Success
[root@localhost ~]# nvme read /dev/nvme0n2 -c 8 -z 4096 -d data -s 128
Rounding data size to fit block count (4608 bytes)
read: Success
[root@localhost ~]#
[root@localhost ~]#

```


Conclusion

- Client need to know how the data is protected or encrypted explicitly
- Namespaces-based configuration maybe a good practice for client