Flash Memory Summit

Encrypted disk design based on NVMe Namespace

Presenter: He Meng

Firmware Test Director

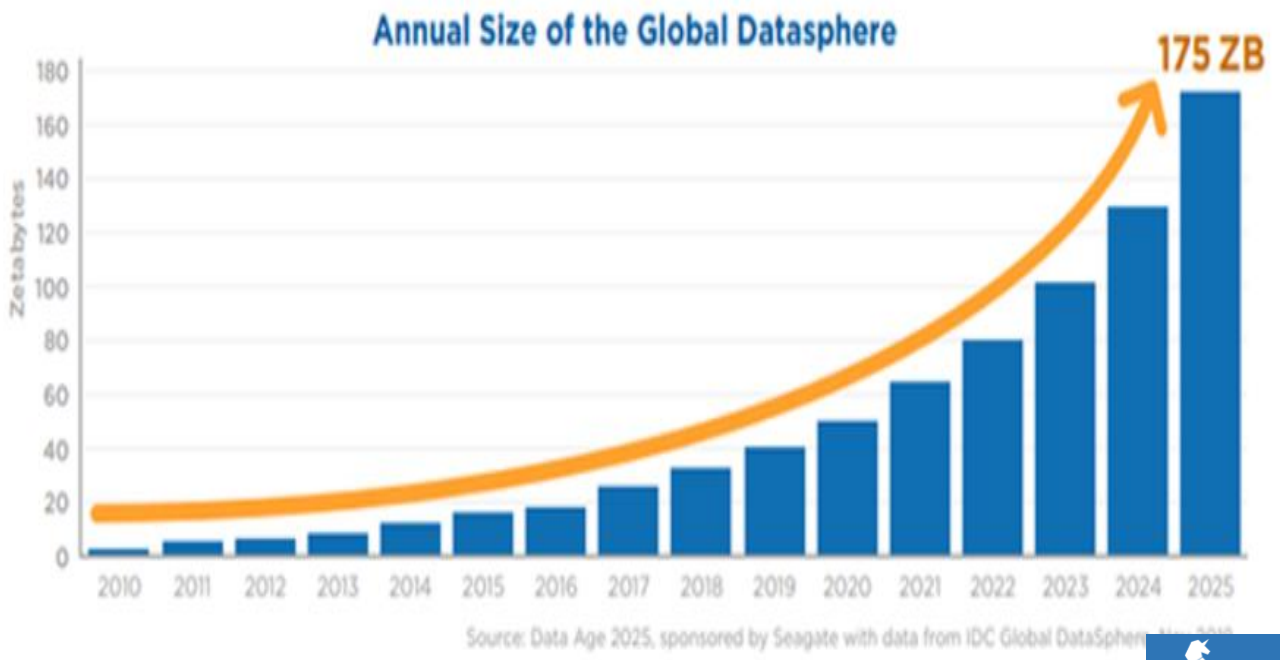
meng.he@starblaze.com

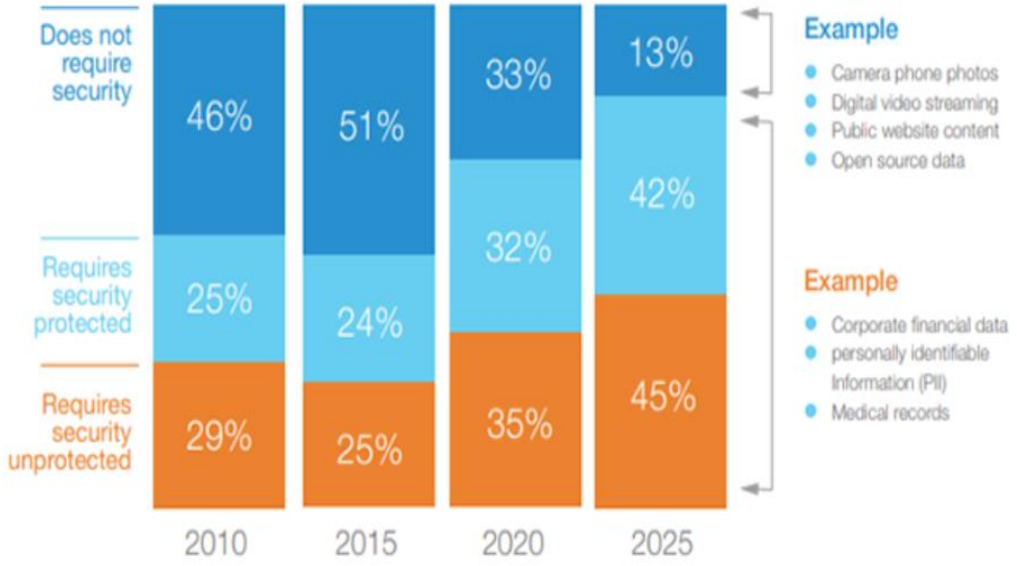
STARBLAZE

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.



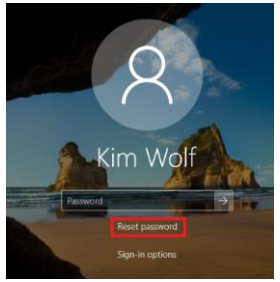


STARBLAZE

Host-Based security technologies

1. **Software Encryption:** Microsoft Bitlocker(OS) and Chinasec(Application)

2. **Security authentication**: Windows login password

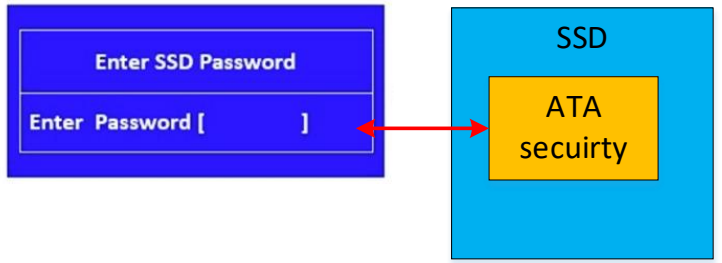


3. **Hardware encryption:** TPM(Trusted Platform Module) Protect user data by integrating a security module to implement RSA/AES/SHA encryption algorithms and password management.

Device-Based security technologies - ATA security & Shadow area

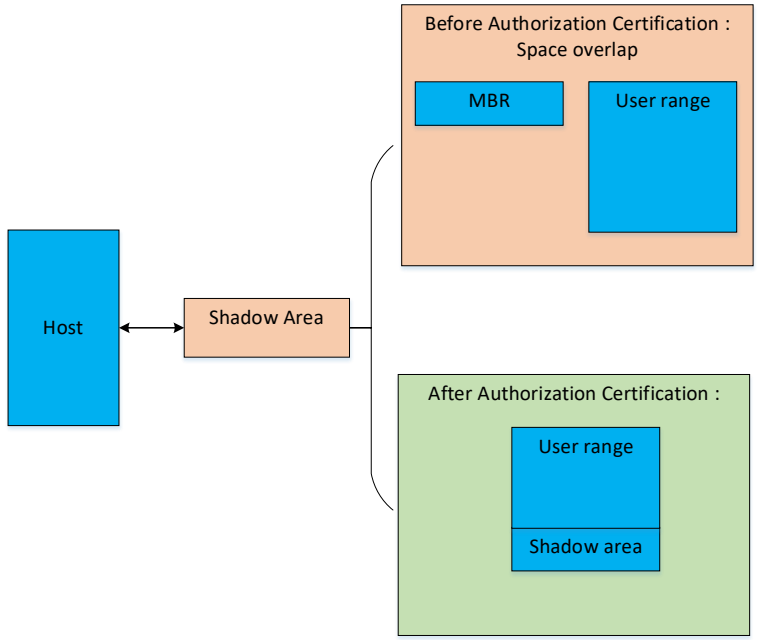
ATA security:

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



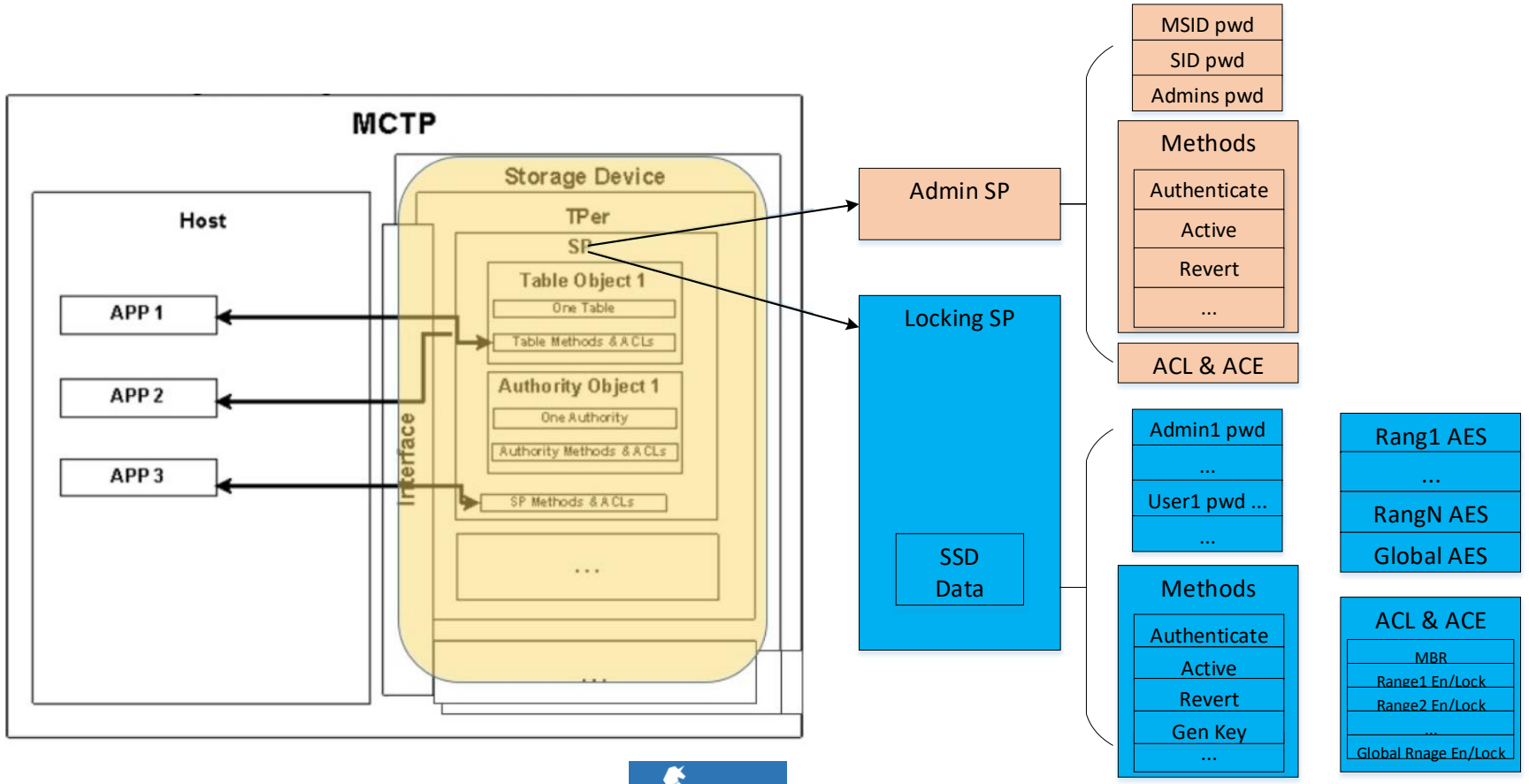
Shadow area

An additional partition, invisible to the host until authenticated



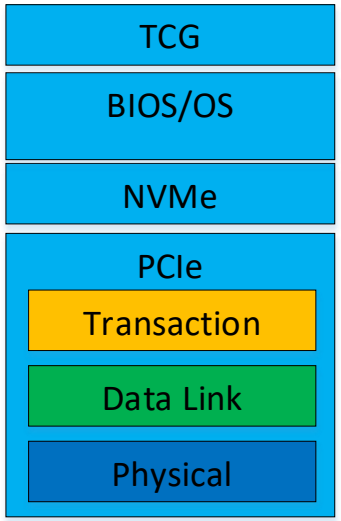
Device-Based security technologies - TCG

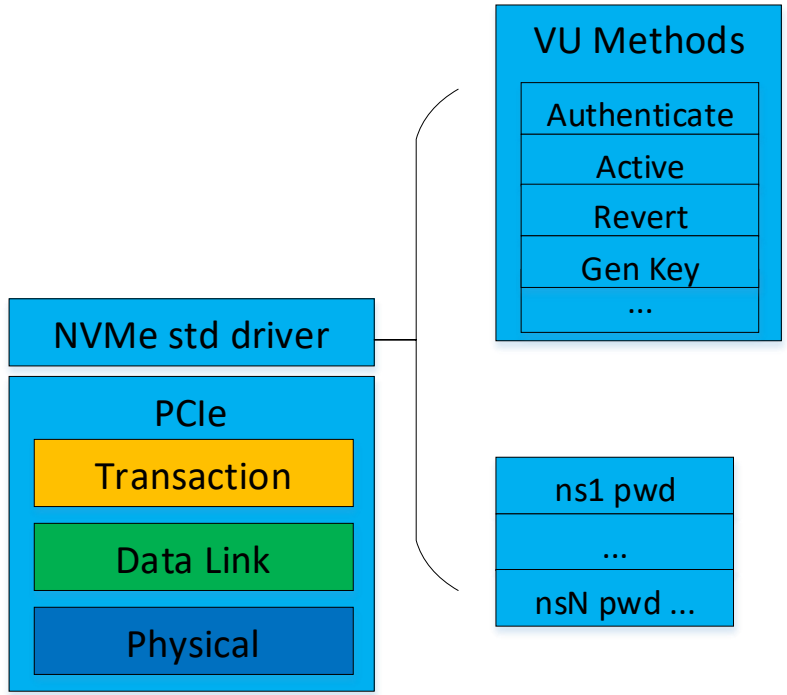
- Sector specific permissions
- Self-encrypting



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:

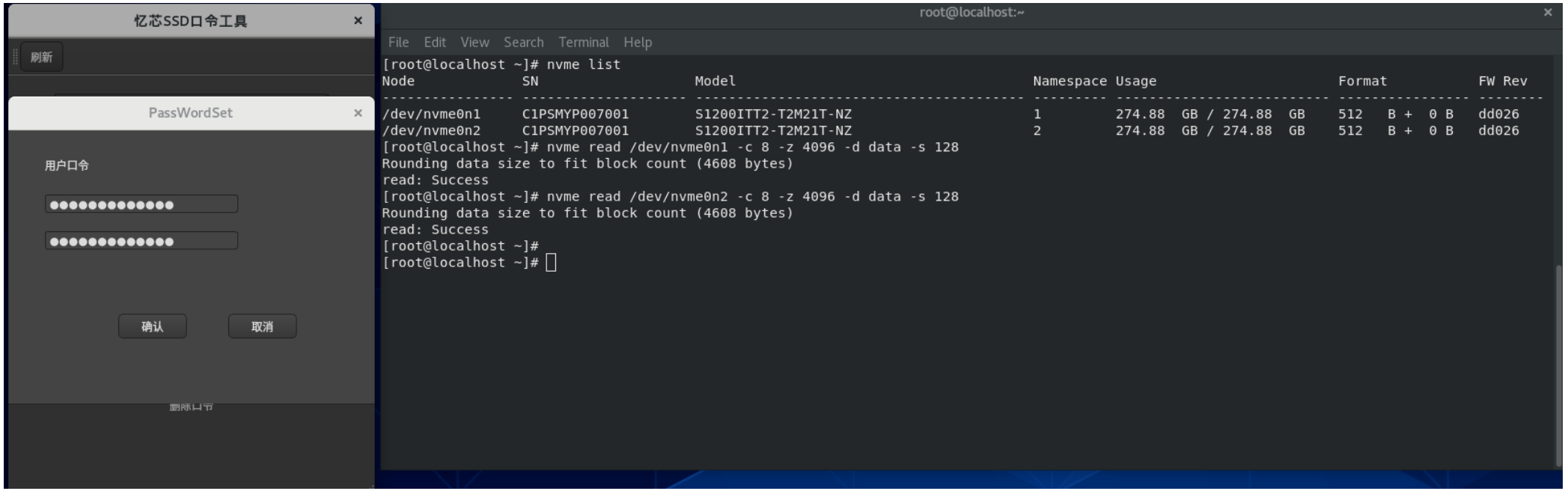
Support：

1.Namespace management(create, attach etc.)

2. Query security information of specific namespace.

3. Password management

Demo on Linux:



Conclusion

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