Establishing a comprehensive security strategy for your server infrastructure has never been more important. Meanwhile, as recent customer surveys indicate, security of hardware ranks as the top server purchasing criteria, and minimizing security risk is considered a “table stake.” Fortunately, a cyber-resilient strategy is within reach.

What’s a Cyber-resilient strategy?
Protecting customer data and intellectual property requires a layered approach, one that effectively Protects, reliably Detects, and rapidly Recovers, a cyber-resilient foundation built into PowerEdge servers.

5 Keys to Centralized, Scalable Key Management
Secure Enterprise Key Manager works on encrypted drives across data centers, remote locations, and in the cloud, and provides extra protection beyond Local Key Manager.

Highly-available KMS Cluster
Multiple servers forming a KMS cluster assures there is no single point of failure and that the externally stored keys are always available.

Built-In PowerEdge Security
PowerEdge servers contain a silicon root of trust, a secure boot cycle, signed firmware, BIOS recovery, and other security controls.

Keys assigned by external KMS
On set-up in the server, self-encrypting drives are assigned a key by the external key management server (KMS) that unlocks the drive so data can flow where needed.

Key-retrieval via iDRAC
When a power event occurs, drives are locked and keys are securely retrieved from the KMS via iDRAC, the embedded server baseboard controller.

Scale in a Linear Fashion
Encryption is done through each drive’s hardware, allowing the solution to scale linearly while helping meet unique regulatory requirements.

Industry-leading KMS
SEKM has been validated against industry-leading KMS servers.

Complies with the KMIP protocol

Sources:
1 Value of Secure Server Infrastructure Web Survey, IDC (February 2018)
2 Needs Based Segmentation Research by Dell / CMB (December 2019)