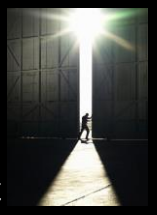
PowerEdge Product Group

Direct from Development



Data Security by using the System Erase feature of iDRAC9 on PowerEdge servers

Tech Note by:

- Paul Rubin
- Tad Walsh
- Doug Iler
- Aniruddha Herekar

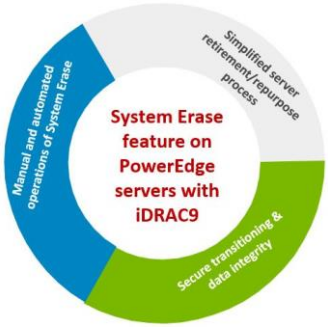
SUMMARY

When repurposing or retiring servers, erasing data from server storage devices is crucial for data security.

System Erase—a feature of PowerEdge servers with iDRAC9—simplifies the process of erasing data from server storage devices and server non-volatile stores.

The System Erase feature is effective on the following:

- HDD
- SED
- ISE
- NVMe drives
- NVDIMMS
- BOSS



Data security is a key consideration throughout the lifecycle of a server, including when the server is repurposed or retired. Many servers are repurposed as they are transitioned from workload to workload. Or, as they change ownership from one organization to another. All servers are retired when they reach the end of their useful life. When such transitions happen, IT best-practices recommend removing all data from the server to ensure that confidential information is not inadvertently shared. Beyond best practices, in many cases, government regulations about privacy rights also necessitate complete data deletion when IT resources are transitioned.

Data erasure is a key capability encompassed in the Dell EMC Security Development Lifecycle (SDL) model. The SDL and Secure Server Management tools ensure that PowerEdge servers are secure at every stage in the server lifecycle—from server conception, design and manufacturing, to operation and decommissioning. At this final stage (decommissioning/retirement), or when a server is repurposed because of a change of workload or ownership, this feature of PowerEdge servers with iDRAC9 can simplify data erase.

System Erase, a feature of PowerEdge servers with iDRAC9, simplifies the process of erasing server storage devices and server non-volatile stores such as caches and logs. To fulfill the varying requirements of system administrator for interactive and programmable operations, System Erase can be performed by the following methods:

- Redfish
- Lifecycle Controller GUI (F10)
- RACADM Command Line Interface (CLI)

Using one of these methods, an administrator can selectively reset a PowerEdge server to its original state (factory settings), removing data from internal server non-volatile stores and from storage devices within the server. System Erase can discover server-attached storage including Hard Disk Drives (HDDs), Self-Encrypting Drives (SEDs), Instant Secure Erase (ISE), Non-Volatile Memory Express (NVMe) drives and Non-Volatile Dual In-line Memory Modules (NVDIMMs). Data stored on ISE, SED, NVMe, and NVDIMM devices can be made inaccessible using cryptographic erase, while devices such as non-ISE SATA HDDs can be erased using data overwrite. The drives present in BOSS controller can also be erased.

Conclusion

Dell EMC PowerEdge servers with iDRAC9 have the capabilities, features, and management options to help ensure the security and integrity of data. When repurposing or retiring servers, IT administrators can use the System Erase function to easily secure server data.

For step-by-step procedural guidelines about how to perform the System Erase operation, see the technical white paper *Securing 14th generation Dell EMC PowerEdge servers with System Erase* on www.dell.com/support/idrac