Trusted Cyber Technologies

DELL Technologies | THALES Building a future we can all trust

Protecting Data Thales CipherTrust Manager and Dell PowerEdge Server

The Challenge

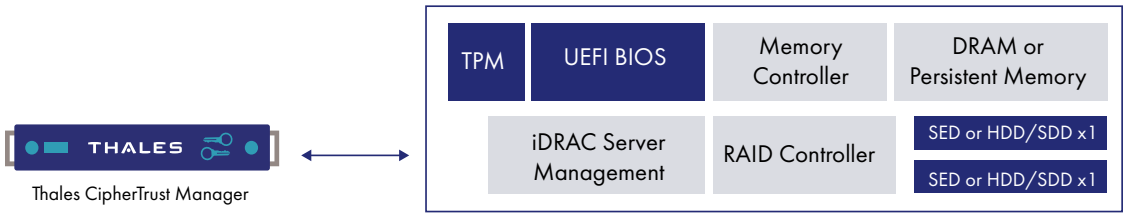
The challenges inherent in securing IT data environments today are multiple:

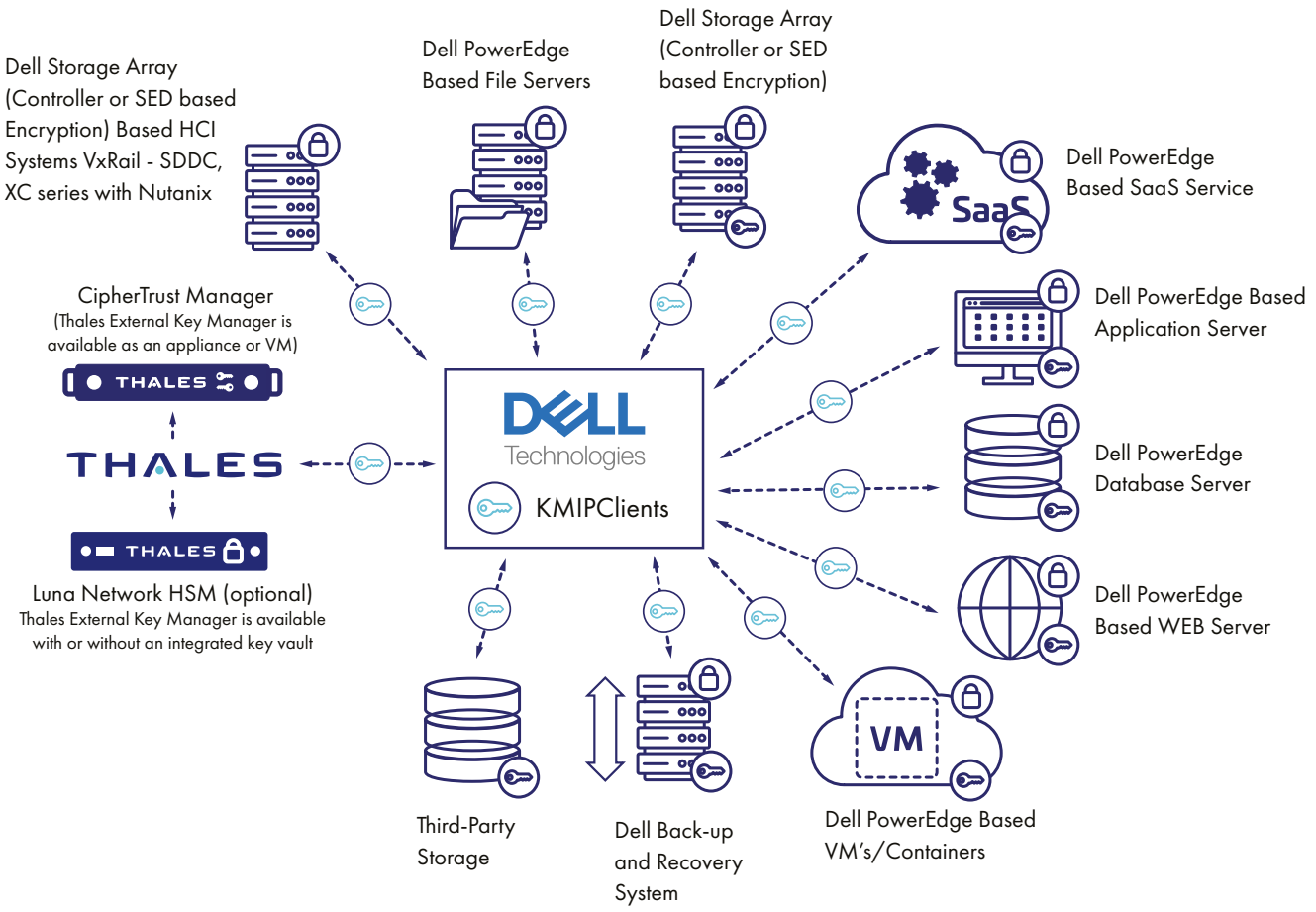
- Increase in regularity and sophistication of data breaches
- Data privacy/compliance mandates (e.g. FIPS, HIPAA, GDPR, PCI-DSS, etc.)
- Rapid digital transformation
- Explosive data growth
- Remote and distant workforce
- Cost control

To meet these challenges, a data-centric solution that reliably secures sensitive data as it moves from endpoints through networks to applications and the cloud is required. Data protection through proven encryption and centralized, scalable management of encryption keys is the last bastion of protection. Fortunately, Thales Trusted Cyber Technologies (TCT) and Dell integrate solutions that work at a lower total cost of ownership (TCO) to provide comprehensive data security and enable compliance in today's environment.

A Security Ready Solution

Dell PowerEdge servers integrate with Thales TCT CipherTrust Manager to mitigate the threat of unauthorized access to encrypted data residing on SED or SDD/HDD drives (see image below). This capability, called Secure Enterprise Key Manager SEKM, is enabled in PowerEdge servers through integrated code in the baseboard management controller (BMC), and complies with the KMIP security standard. Working with Thales TCT, Dell PowerEdge servers now offers an integrated, cyber-resilient, design that helps protect customer data-at-rest, within the data center. CipherTrust Manager provides security by storing and managing keys away from the data and the encrypted device, providing strong data security even if the server is compromised or stolen. The solution can be configured to hold the private keys offshore, preventing domestic authorities from seizing these keys and accessing critical private data.





Offered as part of Dell OpenManage Secure Enterprise Key Manager, Thales CipherTrust Manager simplifies and centralizes encryption key policies and management, and helps meet global compliance, security, and privacy standards.

Dell OpenManage Secure Enterprise Key Manager components include optional connector node licenses that can be purchase at the point of sale (POS), allowing the customer to connect to Thales TCT CipherTrust Manager straight out of the box

Security at a Lower Total Cost of Ownership (TCO)

With Thales TCT and Dell Technologies, the cost of key management is distributed amongst multiple appliances, eliminating the need for costly dedicated point products with disparate features and user interfaces a thing of the past. Whether the data is stored in applications, databases, files, virtual machines (VMs), containers, or storage appliances, CipherTrust Manager simplifies and lowers the cost of key management and encryption through centralized administration and automated operations across multiple encryption deployments and products. Thales Enterprise Key Manager (EKM) reduces the additional staff and time it takes to integrate and manage multiple systems, minimizing complexity, costs and the chance for user errors to contribute to the breach of valuable data.

CipherTrust Manager complements the PowerEdge cyber-resilient, secure design:

- Centrally manage keys with role-based access policies
- Support Administration of our Encryption Connector portfolio
- Enhanced auditing and reporting with multiple log formats and customizable alerts
- REST APIs to automate administrative function and allow programmatic encryption
- Multi-tenant capable with strong separation of duties
- Highly scalable – manage thousands of servers
- High Availability Clustering for mission-critical workloads
- High-speed Interfaces with NIC Bonding Optional 2x1GB/2x10GB network interface cards (NIC) as well as NIC bonding to increase available bandwidth.
- Password and PED Authentication: Choice of password or PIN Entry Device (PED) authentication
- Available as either a virtual or hardware appliance. Hardware appliance with FIPS 140 validated, Level 3 available.

Thales Enterprise Key Management Platforms

Features	Physical Appliances	Virtual Appliances
Max keys	1,000,000	25,000
Max concurrent clients per cluster	1,000	1,000
FIPS 140-2 Support	L3 with a built-in HSM	L1 or L3 with an external HSM
Supports the Thales Data Protection Portfolio	Yes	Yes

About Dell Technologies

Dell Technologies (NYSE:DELL) helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era. Dell PowerEdge Servers have a Cyber Resilient Architecture, creating a secure foundation for enterprise infrastructure.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com