

# Dell Technologies

## Encryption and Key Management

Stephen Tuomey  
Datacenter Account Executive – Federal Distribution  
[stephen\\_tuomey@federal.dell.com](mailto:stephen_tuomey@federal.dell.com)

**DELL**Technologies



# Dell Technologies

- Dell Technologies' Advantage
- Zero Trust
  - Dell's Security Vision
- Thales
  - Data Challenges
  - Encryption & Keys
  - Key Management
  - Management
- Questions & Answers



# Dell Technologies

## Accelerating IT from Ideas to Innovation

Strategic Partnerships  
highlighting technology leaders  
and innovators



**DELL**EMC

**Hugging Face**

**Secureworks**

**RSA**

**boomi**

**THALES**



Artificial  
Intelligence



Modern Data  
Center



Multicloud



Edge



Security

# Dell Technologies

## A new era for AI

AI is transforming how we work and innovate. Organizations need the right data, strategy, technology and tools to take proof of concept to proof of productivity. They need the path to be simple, have control over their models, and maintain their data sovereignty.

Dell Technologies makes this a reality by bringing AI to the data.



Artificial  
Intelligence



Modern Data  
Center



Multicloud



Edge



Security

# Dell Technologies

## Modernize your Data Centers

Design a Modern Data Center that's smart, flexible & resilient to meet the needs of today, tomorrow & whatever comes next.

### Flexible

- Power any workload across the edge, data center & public cloud.

### Smart

- Accelerate innovation with intelligent & efficient systems

### Resilient

- Deliver comprehensive data protection everywhere



Artificial  
Intelligence



Modern Data  
Center



Multicloud



Edge

Security

# Dell Technologies

## Unleash Multicloud by design

Dell Technologies brings disparate cloud experiences together with choice, consistency and control.

### Ground to Cloud

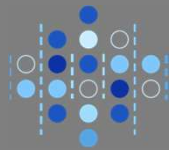
- Best-of-breed Dell software innovations.

### Cloud to Ground

- Modern cloud software and experiences.

### Simple

- Cloud experience in the Multicloud with technology you trust.



Artificial Intelligence



Modern Data Center



Multicloud



Edge



Security

# Dell Technologies

## Tap into the Edge

Proximity to data at the edge drives innovation.

### Leverage AI

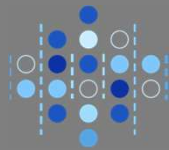
- AI and analytics near data sources.

### Simplify the Edge

- Modernizing your Edge AI architecture, workloads and operations.

### Protect the Edge

- Embedded cybersecurity with Dell's Intrinsic Security.



Artificial  
Intelligence



Modern Data  
Center



Multicloud



Edge



Security

# Dell Technologies

## Advance Cybersecurity & Zero Trust

Don't let security risks stifle innovation.

### Reduce the attack surface

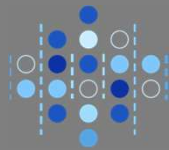
- Minimize the vulnerabilities and entry points that can be exploited.

### Detect and respond to cyber threats

- Actively identify and address potential security incidents and malicious activities.

### Recover from a cyber attack

- Restore the organization to a previous, known secure and operational state.



Artificial  
Intelligence



Modern Data  
Center



Multicloud



Edge



Security

# Zero Trust – Dell Technologies

Dell Technologies can help your journey to achieve Zero Trust

## • Zero Trust - A security model built on the following:



- Anything inside or outside the organization is not trusted by default
- Everything trying to establish a connection must gain / build trust
- Authentication and authorization must happen before trust can be built
  - and can be repeated to re-affirm trust

## • Zero Trust - An architectural framework that is:



- User-centric: Everything starts and centers around the user accessing the service or resource
- Device Trust: Devices are secured, resilient and compliant
- Service-oriented: Makes it easier to create and consume reliable services
- Based on intrinsic security: Every action is scrutinized in the context of its risk



### Device Trust

- Secure Supply Chain
- Secured Component Verification
- Silicon Based HW Root of Trust
- Case Intrusion Alerts



### User Trust

- SafelD
- Role Based Administration Model
- Multi Factor Authentication



### Transport & Session Trust

- Dedicated iDRAC network module
- SSH/TLS Communication Options



### Application Trust

- Signed BIOS/FW updates
- Secure Software Development
- Secure UEFI Boot Capabilities



### Data Trust

- Data-at-Rest Encryption
- Automatic BIOS Recovery
- Automatic OS Recovery



Trusted Clients



Servers



Storage

Data Protection



Network

vmware

Virtual Clients



Dell Technologies

# Dell's holistic cybersecurity vision...

Any Device



Any Application



Any Cloud



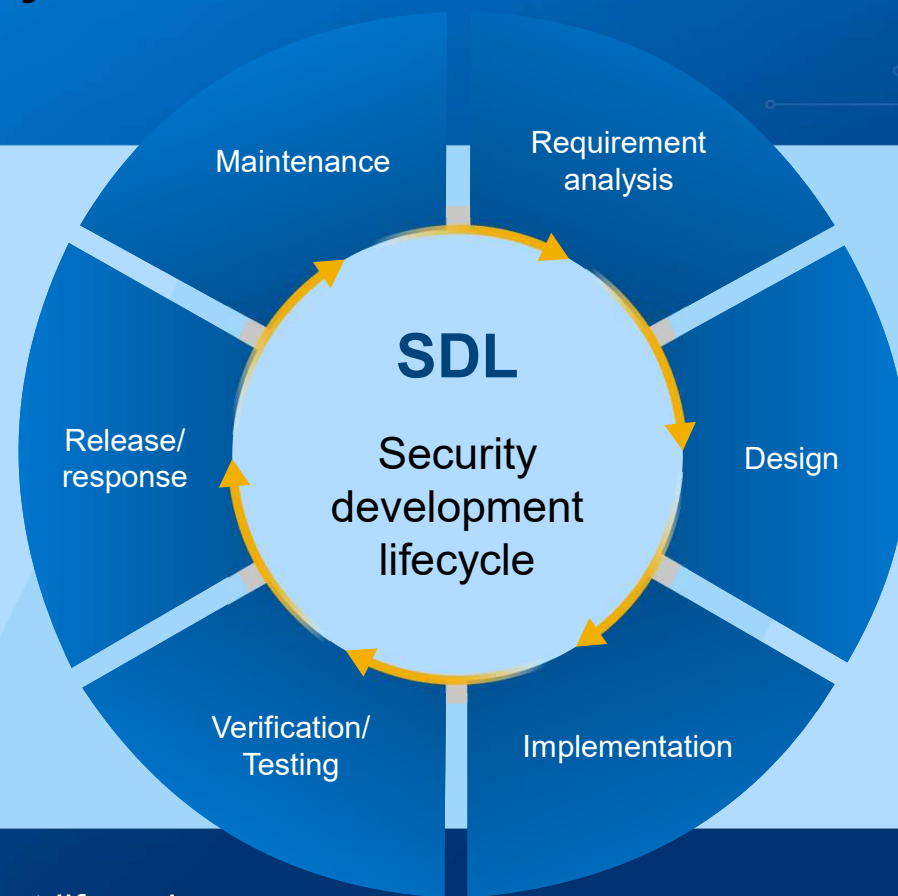
Trusted Infrastructure



# Dell secure development lifecycle

Dell constructed its business model with a partnership of trust among its people, customers and suppliers.

- 1 Sourcing security
- 2 Cybersecurity
- 3 Physical security
- 4 Security management systems



Secure development lifecycle

# Dell Trusted Infrastructure

Modern, resilient, and intelligent technology foundation



## Protect data and systems

Combat threats to critical applications and data with intrinsic security features across our enterprise-wide portfolio of IT solutions and multi-cloud services



## Enhance cyber resiliency

Lessen the impact of cyberattacks and resume operations rapidly with intelligent software-defined solutions and expert services to streamline recovery activities.



## Overcome security complexity

Confidently scale in the face of increasing complexity with automation and orchestration and amplify your resources with cybersecurity services.

Data storage

Servers

Hyperconverged

Networking

Data protection

# Thales - Building a future we can all trust

The Thales logo is displayed in a stylized, blocky font. The letters are dark blue with a lighter blue outline. The letter 'A' is unique, featuring a small teal circle in the center of its upper loop.

## Overview

Thales is a global technology leader with more than 77,000 employees on five continents. The Group is investing in digital and “deep tech” innovations – Big Data, artificial intelligence, connectivity, cybersecurity and quantum technology – to build a future we can all trust.

In the markets of defense and security, aerospace and space, digital identity and security, and transport, Thales provides solutions, services and products to help its customers – companies, organizations and governments – to carry out their critical missions.

## Leader in cybersecurity and data protection

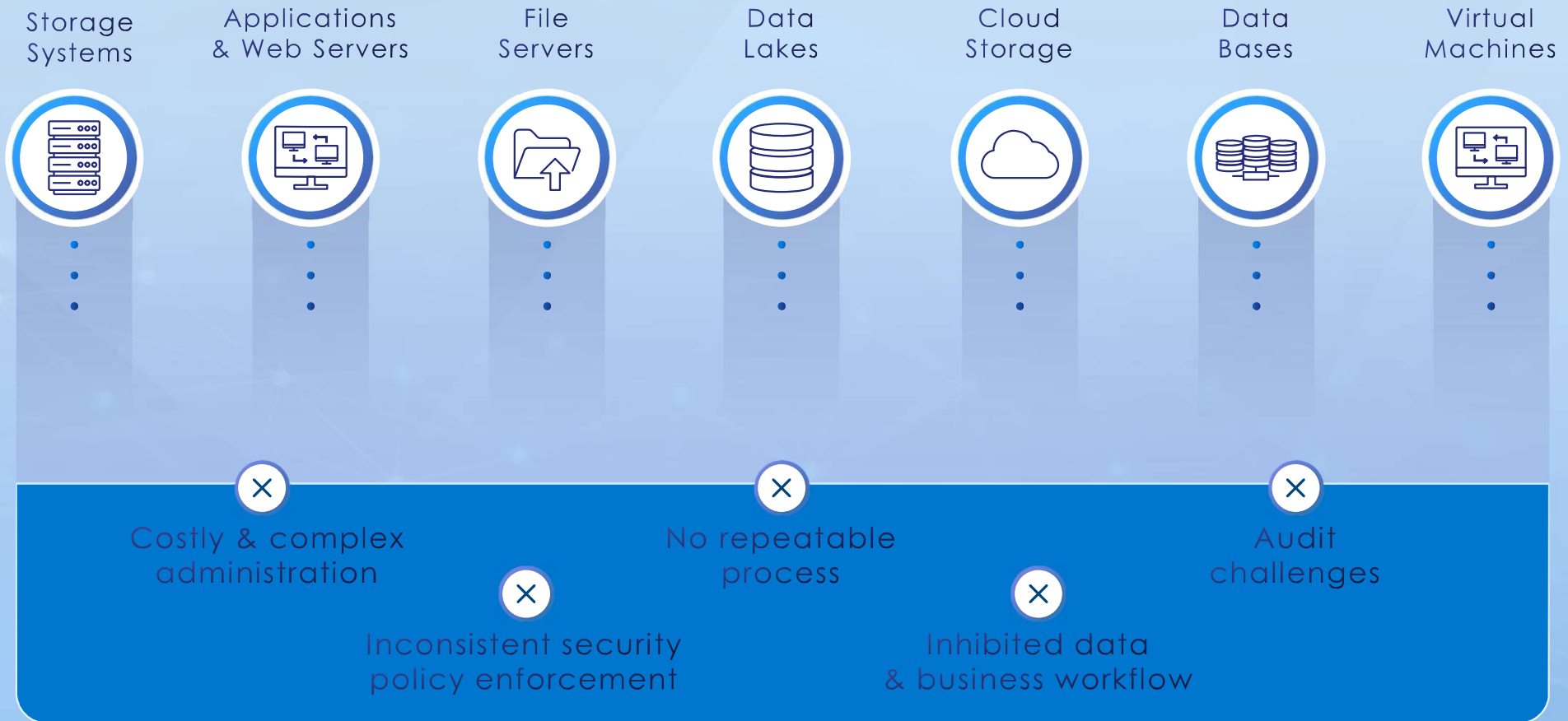
The most demanding companies, government, institutions and critical operators need to ensure the resilience of their activities to any cyber threat or attack. In this context, they need to reduce the cyber risks coming from the IT/OT (Information Technology/Operational Technology) or cloud infrastructure while maintaining the privacy of their data and their critical activities.

## Thales TCT

A separate company dedicated to the US Federal Govt, Integrators, and Partners.

Designing core Crypto solutions for U.S. Federal agencies with code maintained & compiled by Thales TCT. Providing Crypto and Key Management solutions that have a U.S. supply chain lifecycle. Maintain all government approvals and certifications of products required by U.S. Federal agencies. All Employees are including Technical and Sales support is on shore with only U.S. citizens

# Siloed data creates challenges



# Plain Data vs Encrypted Data

Data: Steve  
Binary: 01010011 01110100 01100101 01110110 01100101

Encrypted: wQ1TCGceaOihjUYsvAxX+2qqLWdlzUF3vRivOESik94RJxjcdcZk+CBvrepJU7Ky  
Encrypted Bin: 01110111 01010001 00110001 01010100 01000011 01000111 01100011 01100101 01100001 01001111 01101001  
01101000 01101010 01010101 01011001 01110011 01110110 01000001 01111000 01011000 00101011 00110010  
01110001 01110001 01001100 01010111 01100100 01101100 01111010 01010101 01000110 00110011 01110111  
01010010 01101001 01110110 01001111 01000101 01010011 01101001 01101011 00111001 00110100 01010010  
01001010 01111000 01101010 01100011 01100100 01100011 01011010 01101011 00101011 01000011 01000010  
01110110 01110010 01100101 01110000 01001010 01010101 00110111 01001011 01111001



From the input of the data to a standard ASCII binary stream is easy to understand and interpret (and intercept)  
Data at Rest – Hard Drive / SSD / Memory  
Data in Flight – TCP/IP over Ethernet

From the encrypted data there is no pattern

Binary: 01110111 01010001 ... 01001011 01111001  
Intercepted: wQ1TCGceaOihjUYsvAxX+2qqLWdlzUF3vRivOESik94RJxjcdcZk+CBvrepJU7Ky

Data: ????

← No Key, No Data (just random)

# Examples of Native Encryption



Storage Encryption



Storage Encryption



Backup/Restore Encryption



Tape Library Encryption



Database Native TDE



Cloud Provider Encryption



# Internal vs. External Key Management

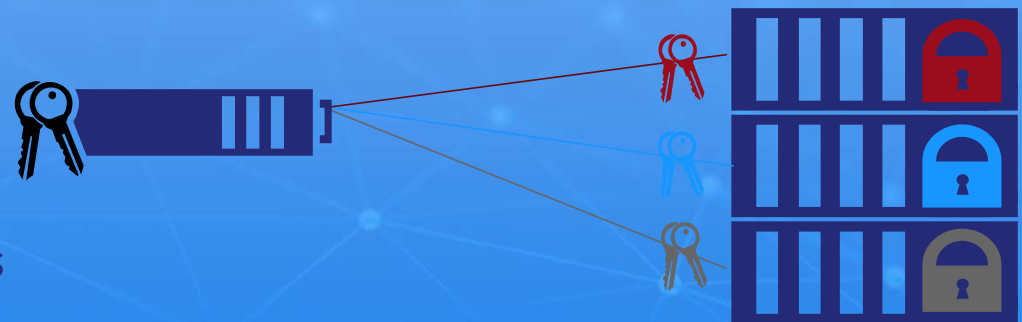
## On Board Key Management

- Keys stored with encrypted data
- Limited functionality
- Minimum security



## External Key Management

- Keys stored in enterprise key manager
- Unlock data upon request
- Manage multiple integrations
- Backup keys
- Audit for compliance
- Supports KMIP



# Typical Use Cases for Key Management



Protect Against  
Data Loss



Meet Compliance /  
Audit Standards



Consolidate Key  
Management



Secure  
Data

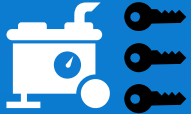


Protect IP In  
Enterprise and  
Multi-Tenant  
Environments



Keep Performance  
and  
Protect Data

# Cryptographic Key Lifecycle Management



## Key Generation

Key strength matches the sensitivity of the data. The greater the key length, stronger the encryption



## Key Access

Ensure the same person creating and managing the key has no access to the protected data



## Key Storage

Use FIPS 140-2 compliant appliances for key storage



## Key Rotation

Periodically rotate encryption keys and document key lifecycle



## Backup & Recovery

Given the magnitude of sensitivity, all keys must be backed up on a periodic basis.



## Strong Authentication

Two-factor authentication for increased security, and reduced insider threats



## Audit Trail for Compliance

Automated, logging and integration with SIEMs to maintain requisite risk and compliance



## Greatest Flexibility

Consistent security and compliance across physical, virtual, and cloud environments



## Unified Management

Central management and secure storage of encryption keys and policies



## Third-Party Integration

Support key management and storage for a variety of KMIP-enabled products

# Thales unified approach to data security



DISCOVER

Discover data wherever it resides and classify it

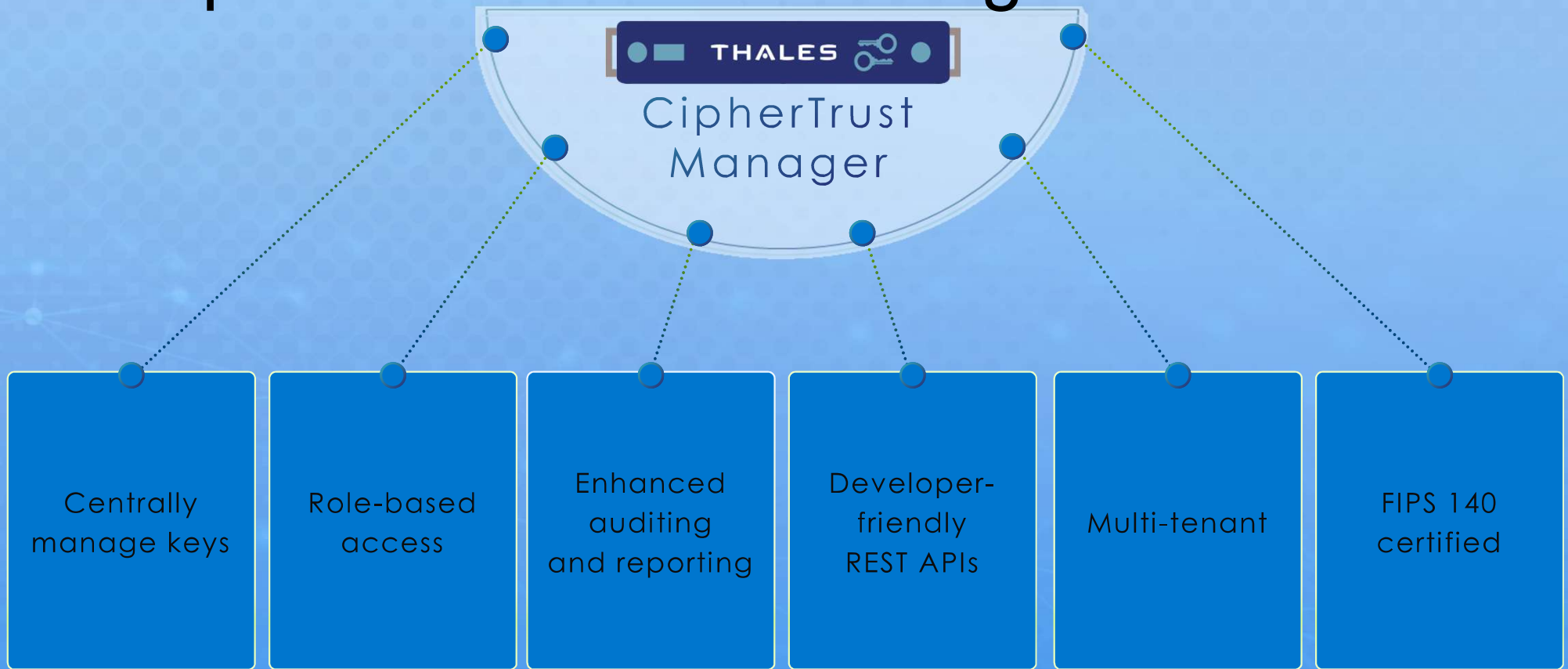
PROTECT

Protect sensitive data with encryption or tokenization

CONTROL

Control access to the data and centralize key management and policies

# Enterprise Centralized Manager



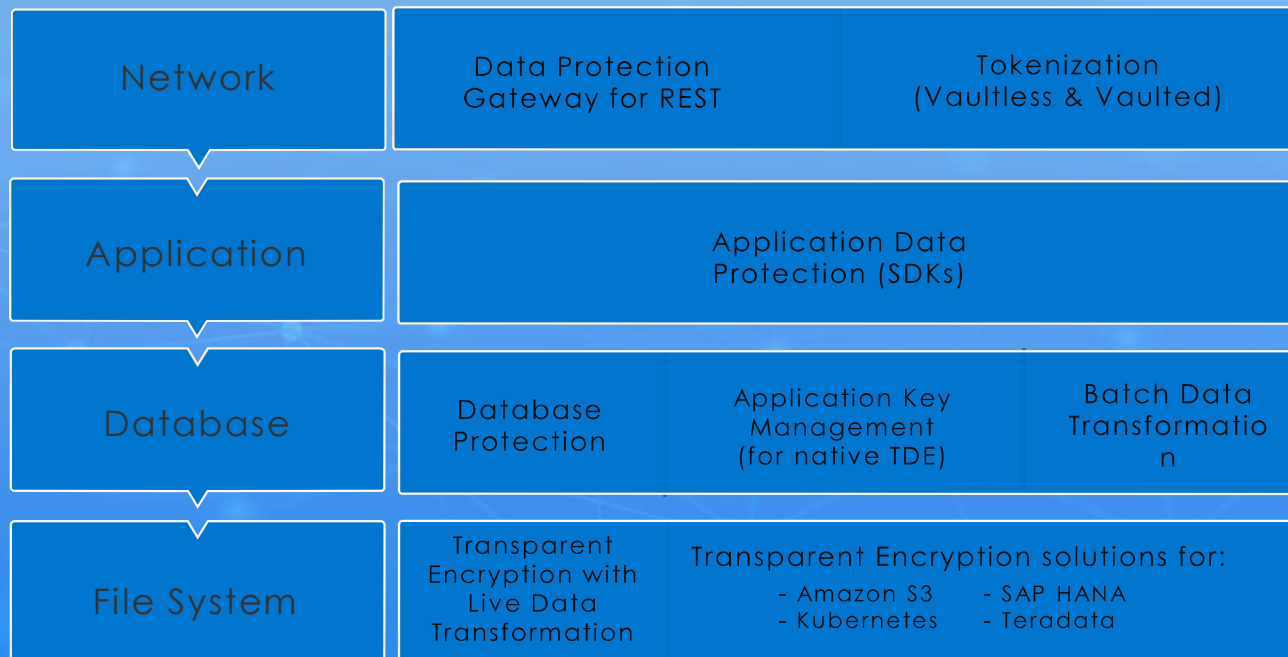
# Protect your sensitive data wherever it resides

Where

How

Protection Layer

CipherTrust Connectors

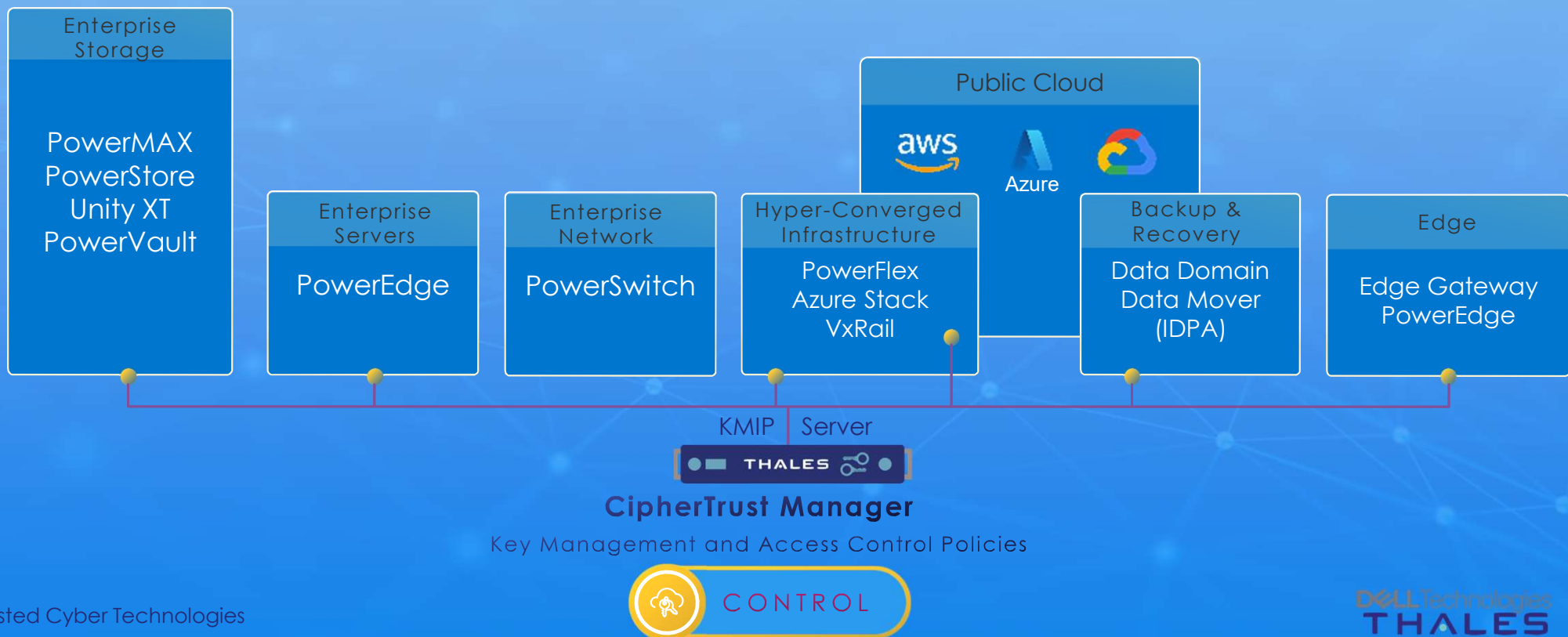


Solutions for each layer of the technology stack to match your security requirements and infrastructure



# CipherTrust & Dell KMIP integration

CipherTrust Manager works with a range of data storage, cloud/SaaS, and virtual environments using key management interoperability protocol (KMIP)



# Choice of deployment options



## On-premises

Physical or virtual appliances  
Control over your own infrastructure  
Meet audit and compliance requirements



## Hybrid

Single management interface across  
clustered physical and virtual appliances



## As a Service

Hosted offering allowing customers to  
consume CipherTrust services via monthly  
subscription in the commercial cloud  
(federal version pending)



## Common Benefits

Common user experience

Meet any operational expense model

High availability through clustering

# Next Steps and Q & A

Work with your Dell Partners to assist you in Architecting your solutions to work towards Zero Trust

- Devices, Applications, Datacenters, Multi-Clouds, Security and Key Management

## Next Steps

- Schedule a Security Assessment
- Schedule a Test Drive
- Contact Carahsoft & Your Technology Partner
- Contact your Dell team

