Trusted Hybrid Cloud

Technical Overview

Custom VS Reference Architectures

⚠

Custom Architectures

- Complex
- Lack of architectural review
- Long development and implementation times

Reference Architectures

- Simplified Deployments
- Peer reviewed architecture
- Quicker time from purchase to operations
- Reduced risk due to predictable outcomes

👍

Why Use NIST Design?

NIST
National Institute of
Standards and Technology

Trusted Hybrid Cloud

DELL Technologies
vmware

- NIST, Dell Technologies, VMware collaborative development
- Full adoption of NIST SP-800-53 Security Controls
- Validated and published by NIST
- Supports industry compliant workloads

Delivering Compliancy

Dell Technologies Trusted Hybrid Cloud

A hardware/software hyperconverged hybrid cloud solution that is delivered to help customers meet industry and government cybersecurity compliancy goals

The solution is delivered through the utilization of VMware Validated Design guidance with pre-defined solution blocks of technology from Dell Technologies and its industry leading partners

DELL Technologies

vmware™

RSA

FORNETIX

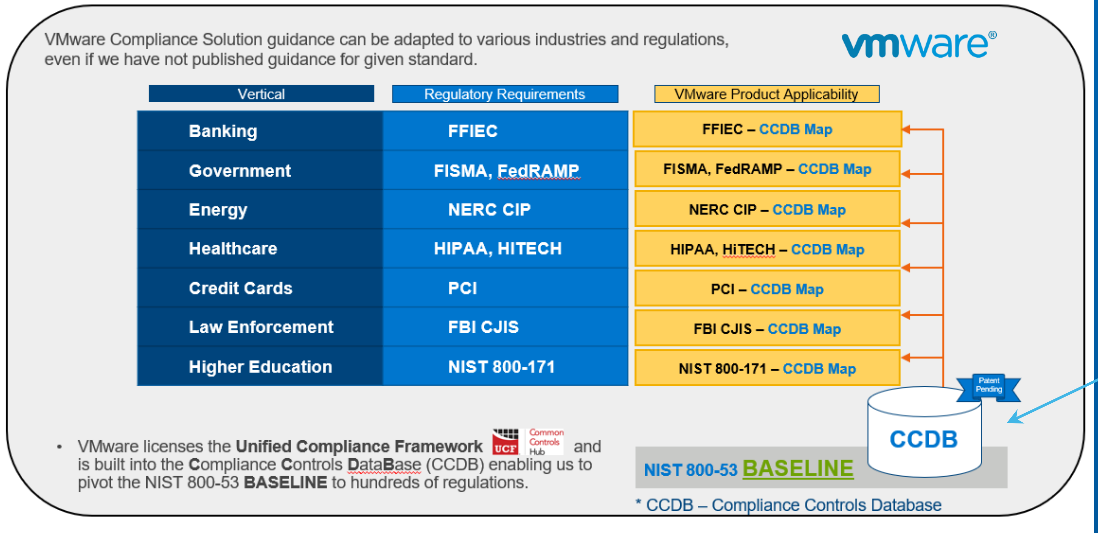
DXC.technology

Solution Overview

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Trusted Cloud: Hybrid Cloud IaaS Environments Validated Design

- SP1800-19A: Executive Summary
- SP1800-19B: Approach, Architecture, and Security Design
- SP1800-29C: How to Guides



VMware Compliance Solution guidance can be adapted to various industries and regulations, even if we have not published guidance for given standard.

vmware®

Vertical	Regulatory Requirements	VMware Product Applicability
Banking	FFIEC	FFIEC – CCDB Map
Government	FISMA, FedRAMP	FISMA, FedRAMP – CCDB Map
Energy	NERC CIP	NERC CIP – CCDB Map
Healthcare	HIPAA, HITECH	HIPAA, HiTECH – CCDB Map
Credit Cards	PCI	PCI – CCDB Map
Law Enforcement	FBI CJIS	FBI CJIS – CCDB Map
Higher Education	NIST 800-171	NIST 800-171 – CCDB Map

Patent Pending

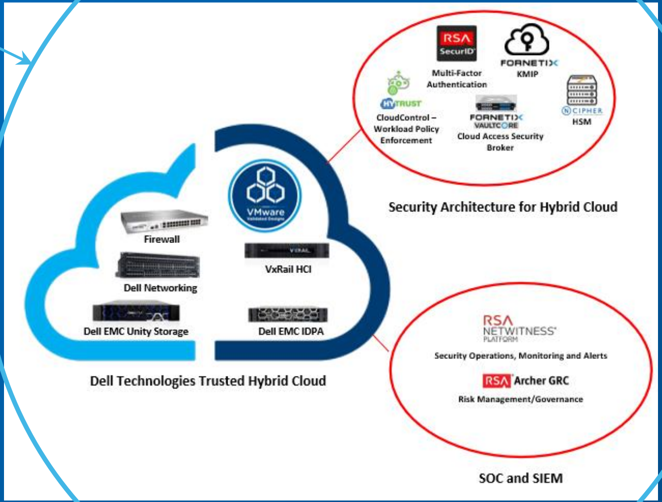
CCDB

NIST 800-53 BASELINE

- VMware licenses the **Unified Compliance Framework** UCF Common Controls Hub and is built into the **C**ompliance **C**ontrols **D**ata**B**ase (CCDB) enabling us to pivot the NIST 800-53 **BASELINE** to hundreds of regulations.

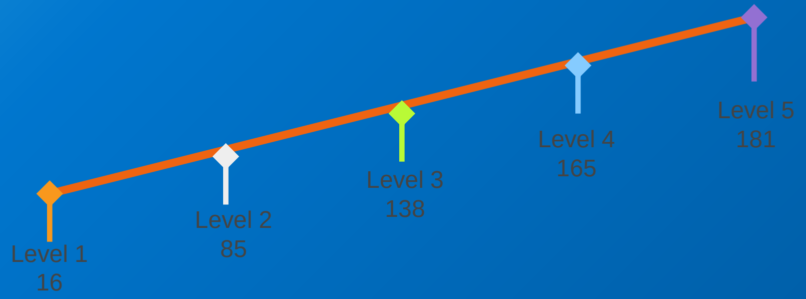
* CCDB – Compliance Controls Database

Dell Technologies Trusted Hybrid Cloud


RSA SecurID
Multi-Factor Authentication
FORNETIX KMIP
HYTRUST
CloudControl – Workload Policy Enforcement
FORNETIX VAULTCORE
Cloud Access Security Broker
NCIPHER
HSM
Security Architecture for Hybrid Cloud
VMware Validated Designs
Firewall
Dell Networking
VxRail HCI
Dell EMC Unity Storage
Dell EMC IDPA
Dell Technologies Trusted Hybrid Cloud
RSA NETWITNESS PLATFORM
Security Operations, Monitoring and Alerts
RSA Archer GRC
Risk Management/Governance
SOC and SIEM

DELL Technologies

CMMC Heatmap based on VVD on VxRail



Level 1
16

Level 2
85

Level 3
138

Level 4
165

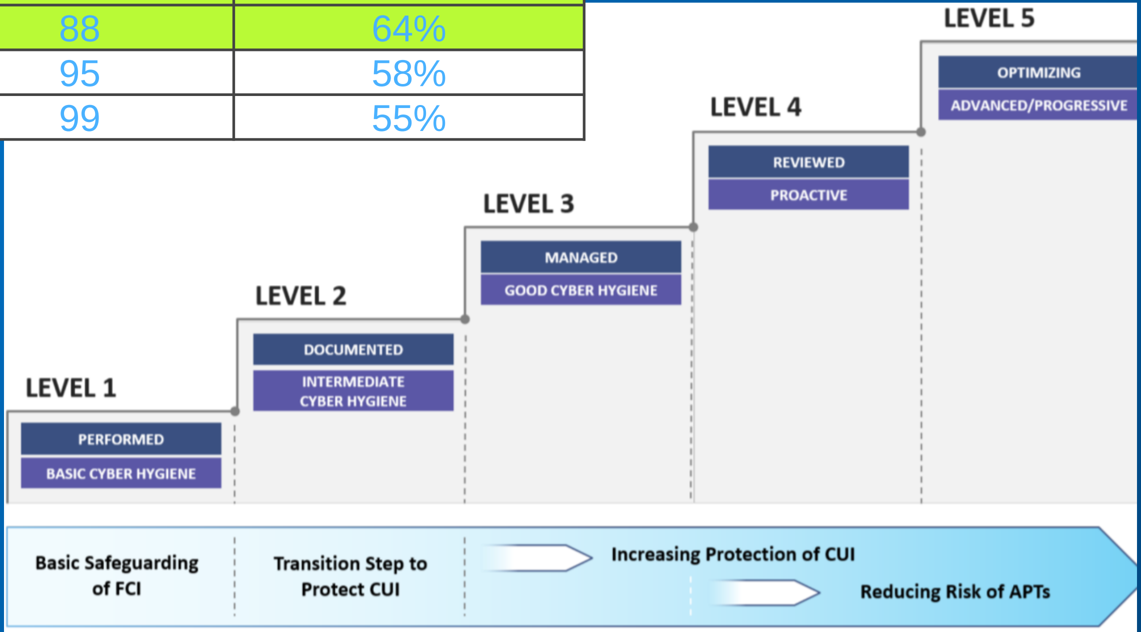
Level 5
181

NIST	vCenter	ESXi	NSX	vSAN	VxRail	vRA	vRO	vROPS	vRLI	SRM
AC	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦	🟧 ⬜ 🟩 🟦
AM	🟦									
AT					🟧 ⬜					
AU	⬜ 🟩 🟪	⬜ 🟩 🟪	⬜ 🟩 🟪	⬜ 🟩 🟪	⬜ 🟩 🟪	⬜ 🟩 🟪	⬜ 🟪	⬜ 🟩 🟪	⬜ 🟩 🟦 🟪	⬜ 🟩 🟪
CM		⬜		⬜	⬜	⬜ 🟩	⬜	⬜		
IA	⬜ 🟩	⬜ 🟩	⬜		⬜ 🟩			⬜		⬜
IR								🟩	⬜ 🟩	
MA		⬜	⬜							
MP	🟩	🟩		🟩S	🟩					
PE			🟧			🟧			🟧	
SC	⬜ 🟩	⬜ 🟩	⬜ 🟩 🟦	🟩		🟩	🟩	🟩	🟩	🟩
SI	🟧 ⬜ 🟪	🟧 ⬜	⬜ 🟪			🟩			⬜ 🟪	

No applicability: CA, PS, RE, RM, SA

CMMC Journey

CMMC Level	Controls	Applicability	% Applicability
1	16	8	50%
2	85	54	64%
3	138	88	64%
4	165	95	58%
5	186	99	55%



Benefits

- Save 2,000 – 6,000 hours on compliance mapping alone
- Optimize SDDC deployment within 4-6 weeks
- Accelerate Level 1, 2, and 3 towards CMMC documentation
- Shift focus to Level 4 and Level 5 via automation, reducing APT risk
- Enhance SDDC via engineered scripts, automation, and simplified architecture
- Unlock the potential of Software Defined cybersecurity

DELLTechnologies

Component Solution

Dell Technologies Trusted Hybrid Cloud

Hardened Hardware Infrastructure

DELL Technologies

- VxRail
- Dell S-Series Switches
- Dell EMC UnityXT
- Data Domain, Avamar

Enterprise Key Management & HW Encrypted Validation

FORNETIX

- VaultCore
- nCipher HSM

Hardened Virtual Infrastructure

vmware

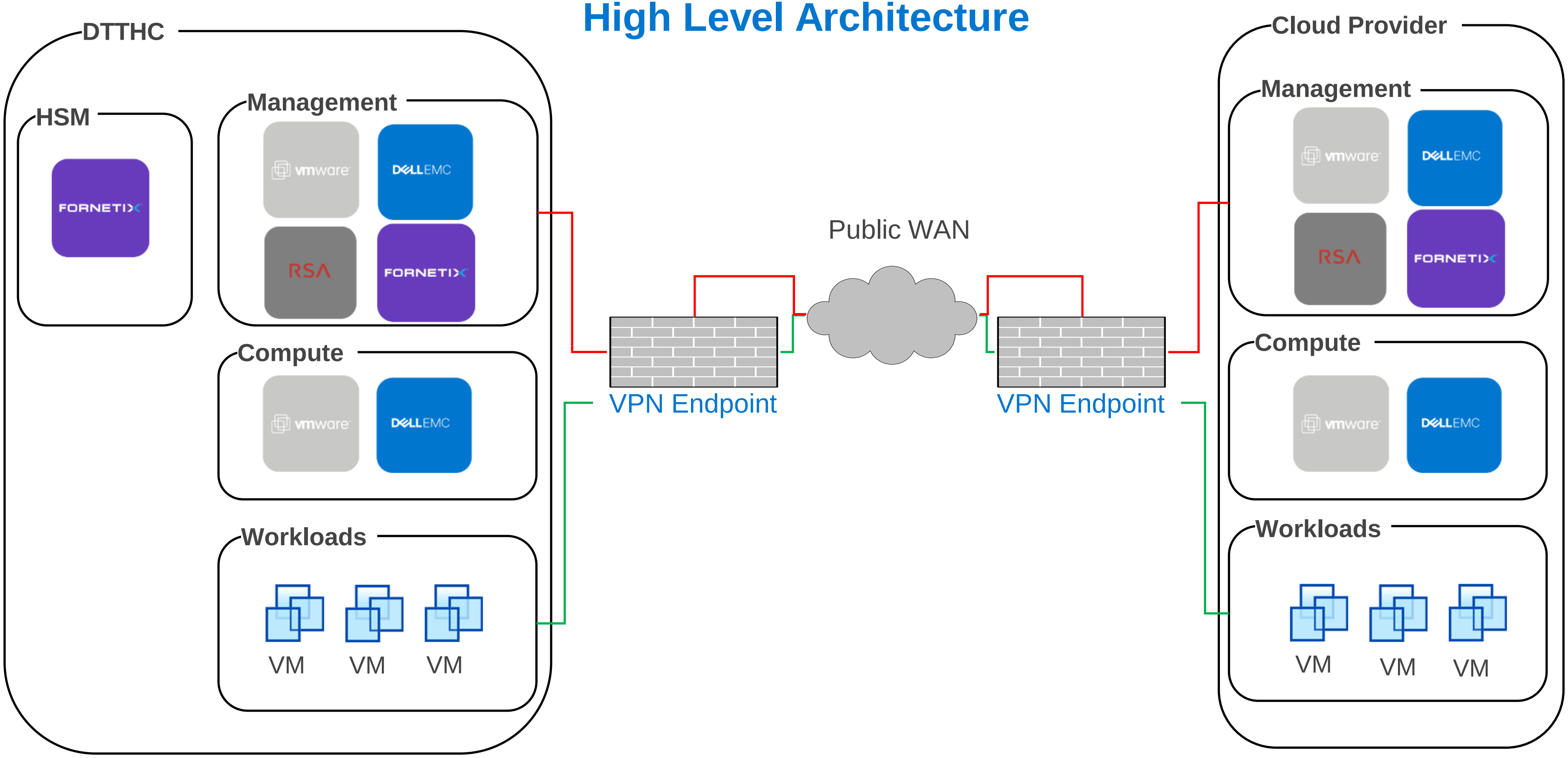
- Validated Design
- vSphere 6.7
- Cloud Builder 1.0

Multi-Factor Authentication, SOC, SIEM

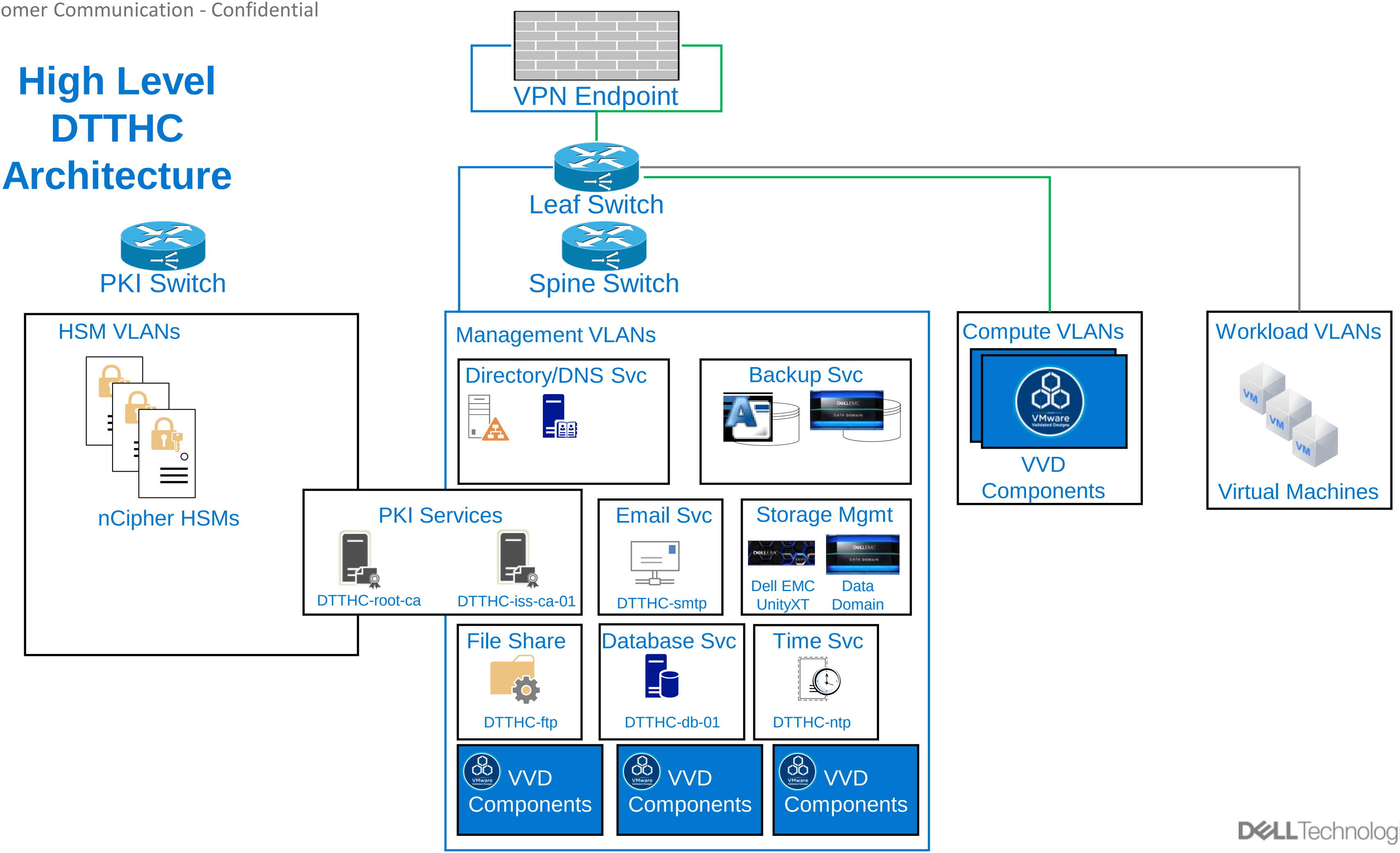
RSA

- SecurID
- NetWitness
- Archer

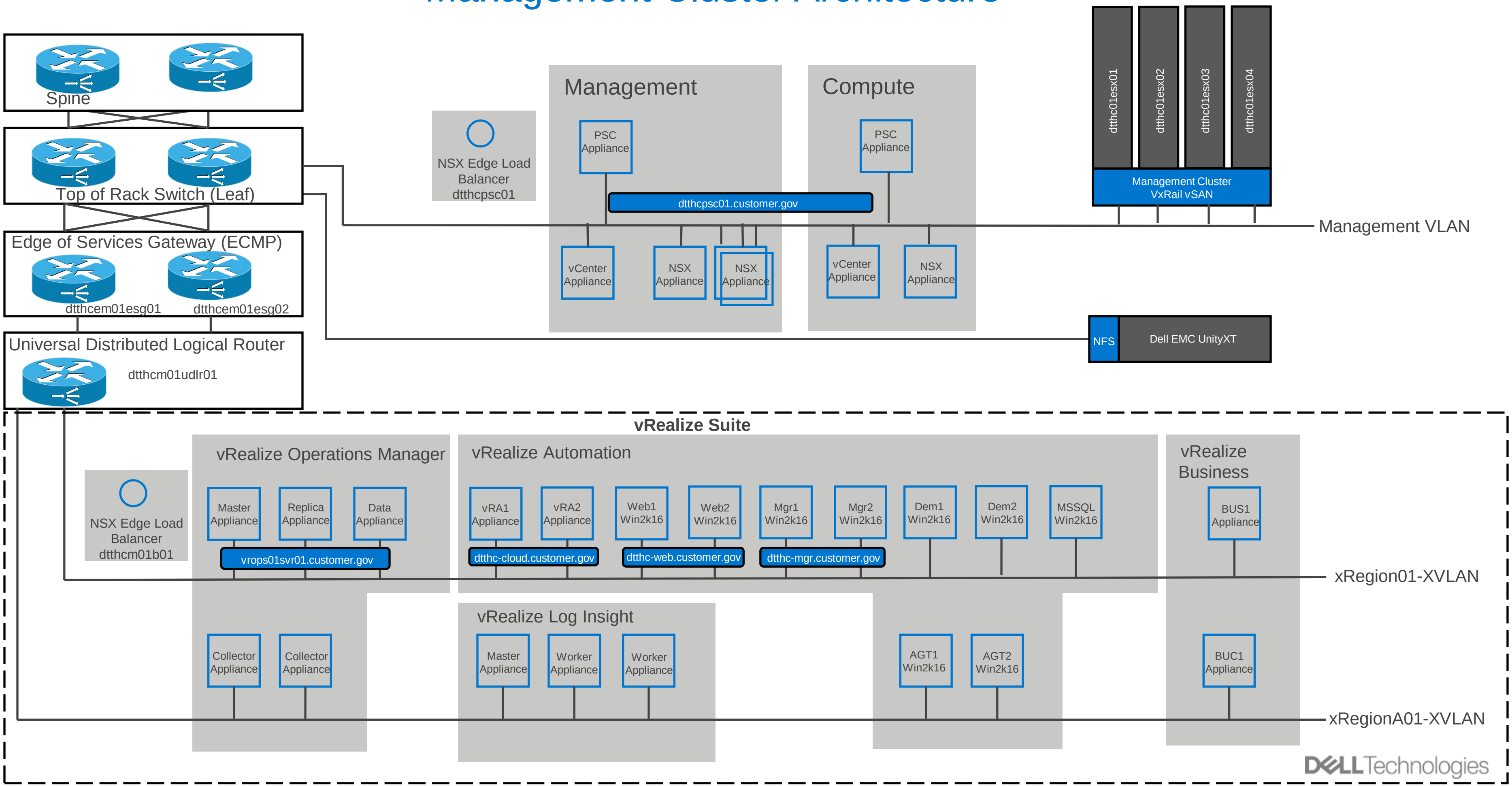
High Level Architecture



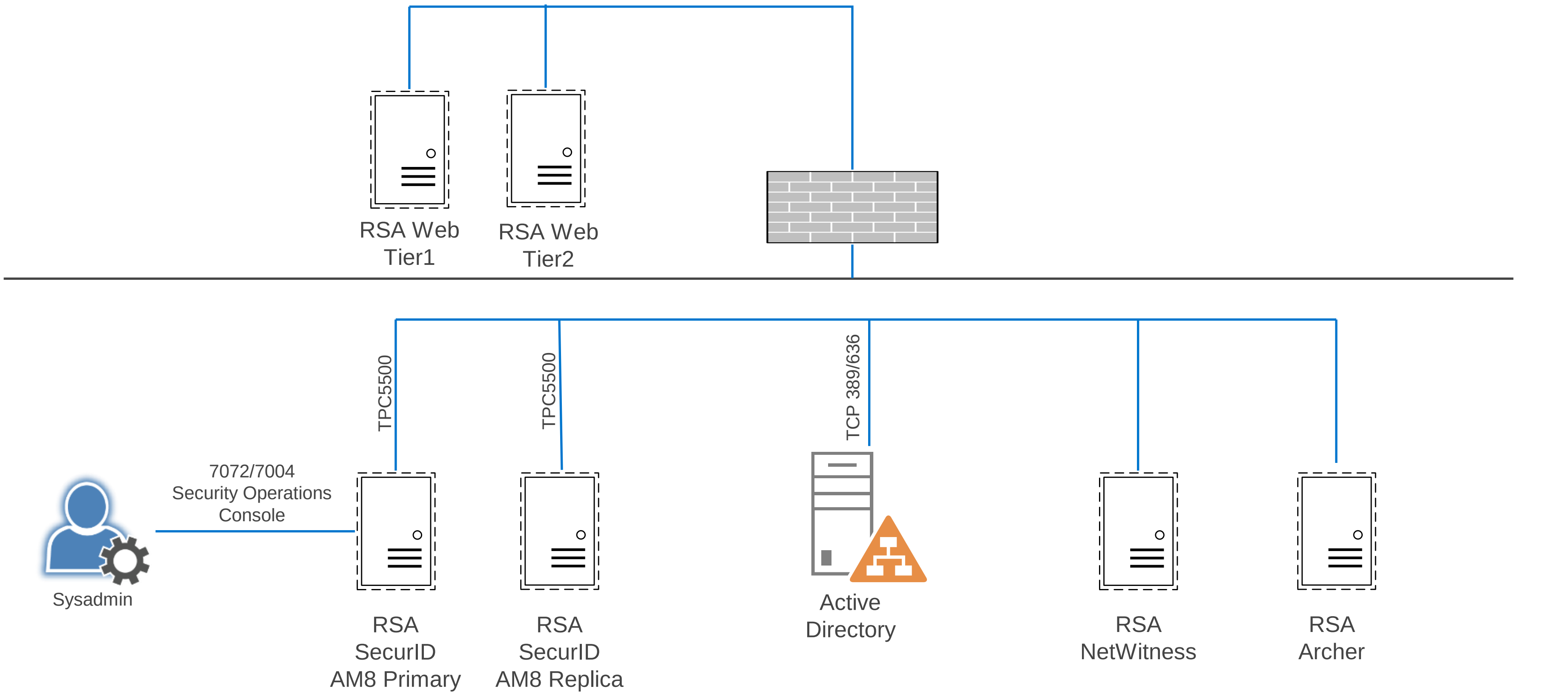
High Level DTTHC Architecture



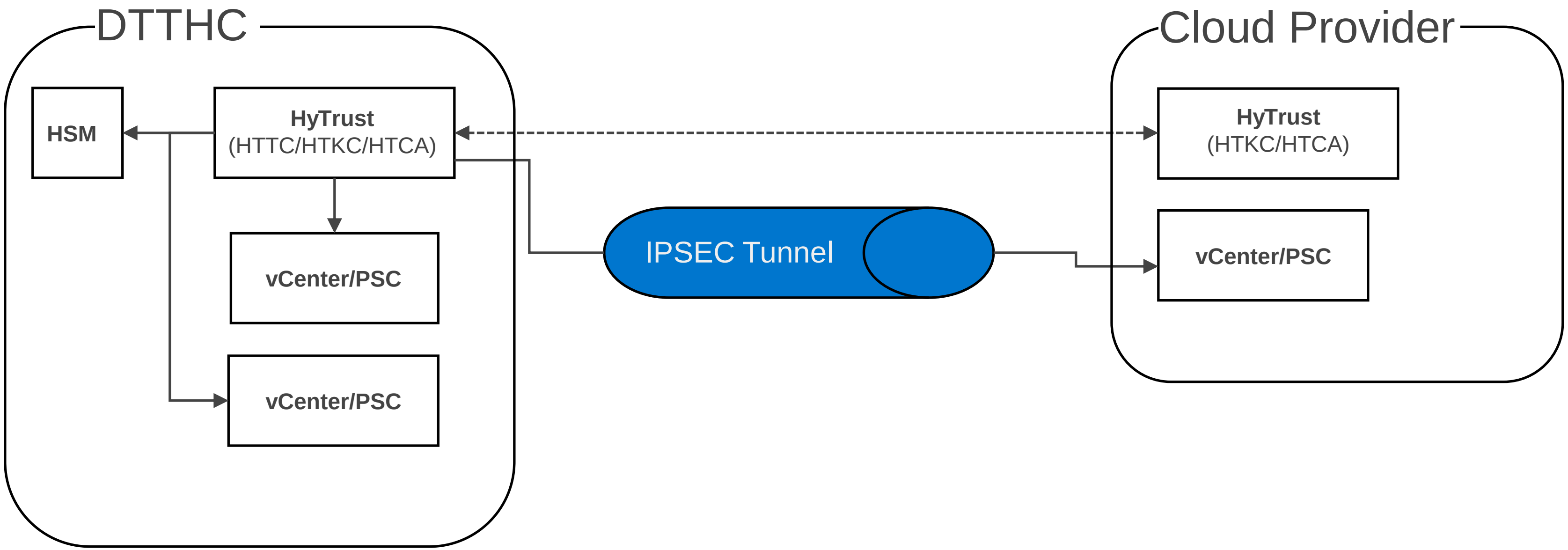
Management Cluster Architecture



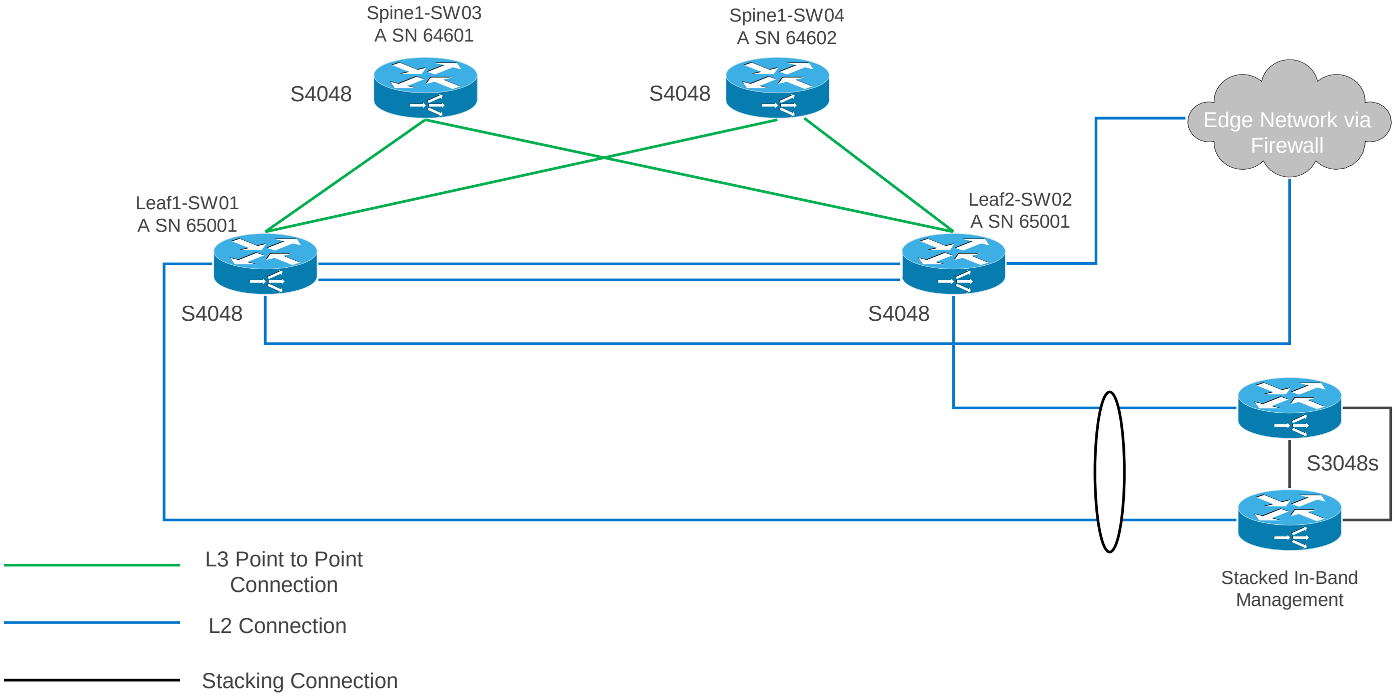
RSA Cluster Architecture



HyTrust Architecture



DTTHC Layer 3 Leaf – Spine Network Diagram



Spine1-SW03
A SN 64601
S4048

Spine1-SW04
A SN 64602
S4048

Edge Network via Firewall

Leaf1-SW01
A SN 65001
S4048

Leaf2-SW02
A SN 65001
S4048

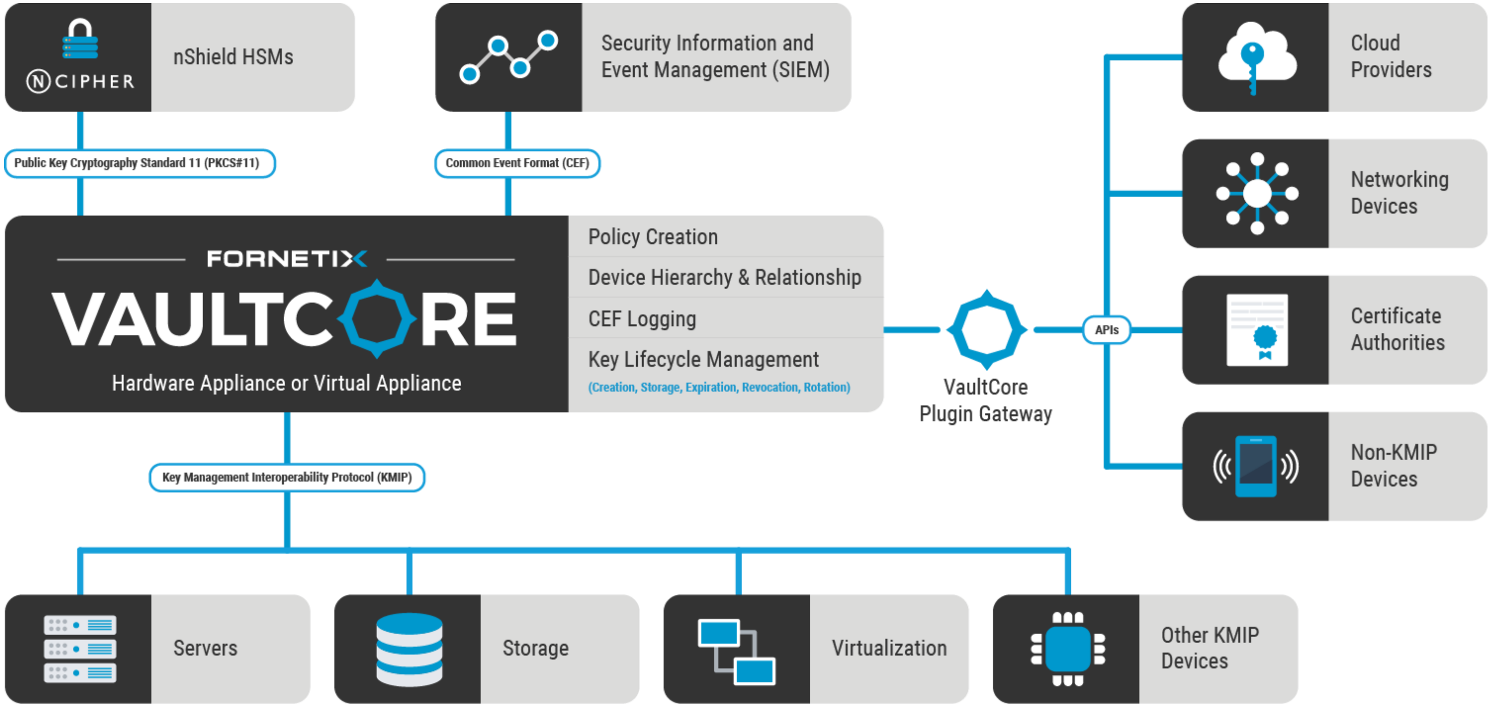
S3048s
Stacked In-Band Management

L3 Point to Point Connection

L2 Connection

Stacking Connection

Fornetix & nCipher Architecture


nCIPHER
nShield HSMs
Security Information and Event Management (SIEM)
Public Key Cryptography Standard 11 (PKCS#11)
Common Event Format (CEF)
FORNETIX
VAULTCORE
Hardware Appliance or Virtual Appliance
Policy Creation
Device Hierarchy & Relationship
CEF Logging
Key Lifecycle Management
(Creation, Storage, Expiration, Revocation, Rotation)
VaultCore Plugin Gateway
APIs
Cloud Providers
Networking Devices
Certificate Authorities
Non-KMIP Devices
Key Management Interoperability Protocol (KMIP)
Servers
Storage
Virtualization
Other KMIP Devices

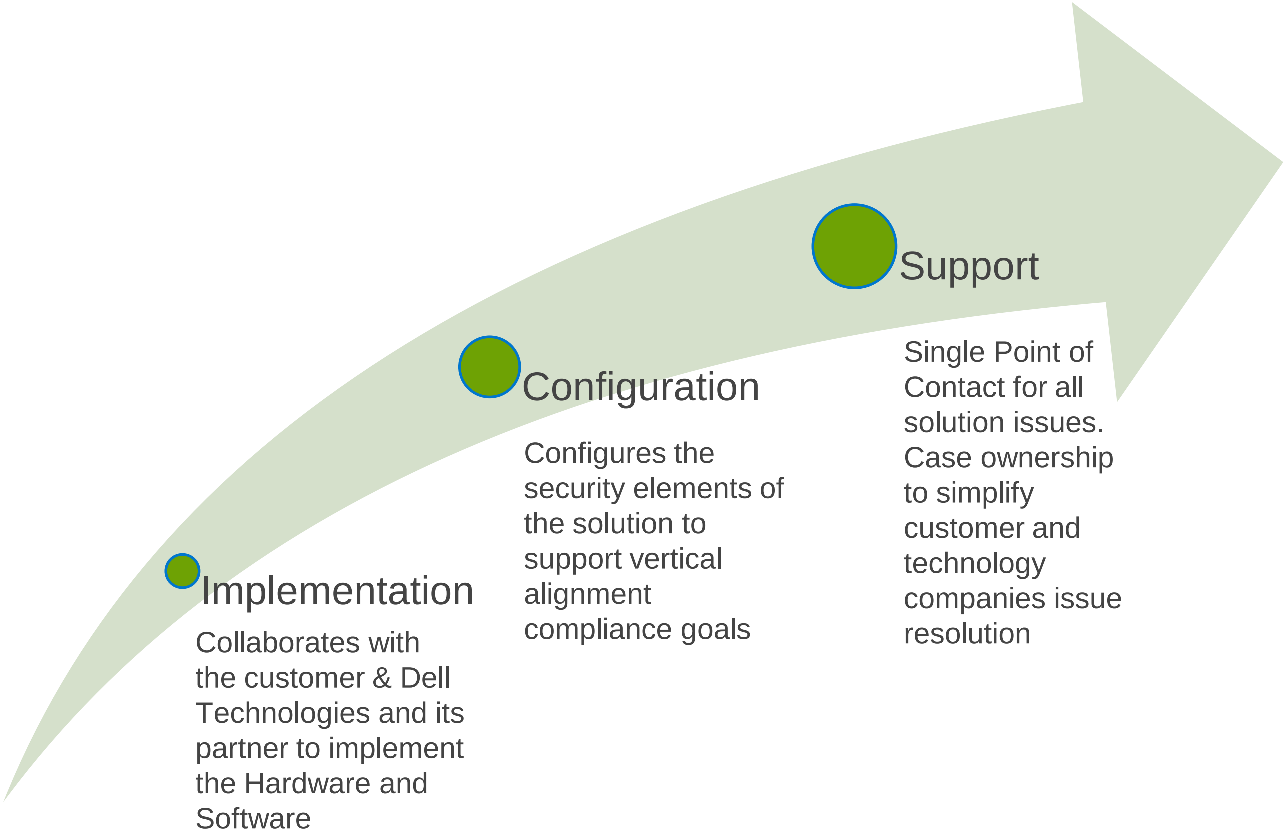
Implementation and Configuration Management Services

- Site scoping and assessment for DTTHC implementation
- Full service description review of the hardware, and software services with the customer site managers and IT project managers.
- Schedule development and progress reporting for each of phase of site establishment with customer site managers and IT project managers :
  - Phase 1:
    - Site readiness validation from customer.
    - Base HW/SW installation and wiring.
  - Phase 2:
    - Base SW configuration
    - Advanced security hardening of all HW/SW components to compliance standards
    - Documentation of overall solution architecture to include technical diagrams, security posture assessments, and compliance mappings.
  - Phase 3:
    - Penetration testing and security scanning
    - Solution security readiness reporting.
    - Finalized documentation on solution capability to support technical requirements for compliance.
  - Phase 4:
    - Hand off of solution to customer operations.

Customer Support Services

- 24/7/365 Phone support for customer calls tied to the DTTHC solution.
- Case ownership for all cases to include level 1 trouble shooting and issue investigation.
- 4hr parts SLA
- U.S. Citizen for U.S. Federal Deals
- Customer case status reporting to customer on the following timelines:
  - Level 1 (High Priority): Every 2 hrs
  - Level 2 (Med Priority): Daily
  - Level 3 (Low): Weekly
- Escalation to L3 of vendor specific issues to include advanced HW/SW vendor issues.
  - Continue to own case and reporting timelines outlined above
- Monthly case reporting to customer

Service Coverage



Implementation

Collaborates with the customer & Dell Technologies and its partner to implement the Hardware and Software

Configuration

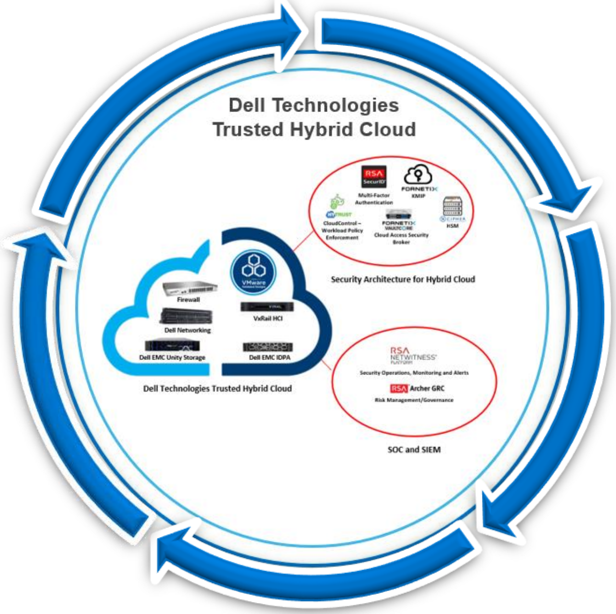
Configures the security elements of the solution to support vertical alignment compliance goals

Support

Single Point of Contact for all solution issues. Case ownership to simplify customer and technology companies issue resolution

Adopting a Risk Management Approach

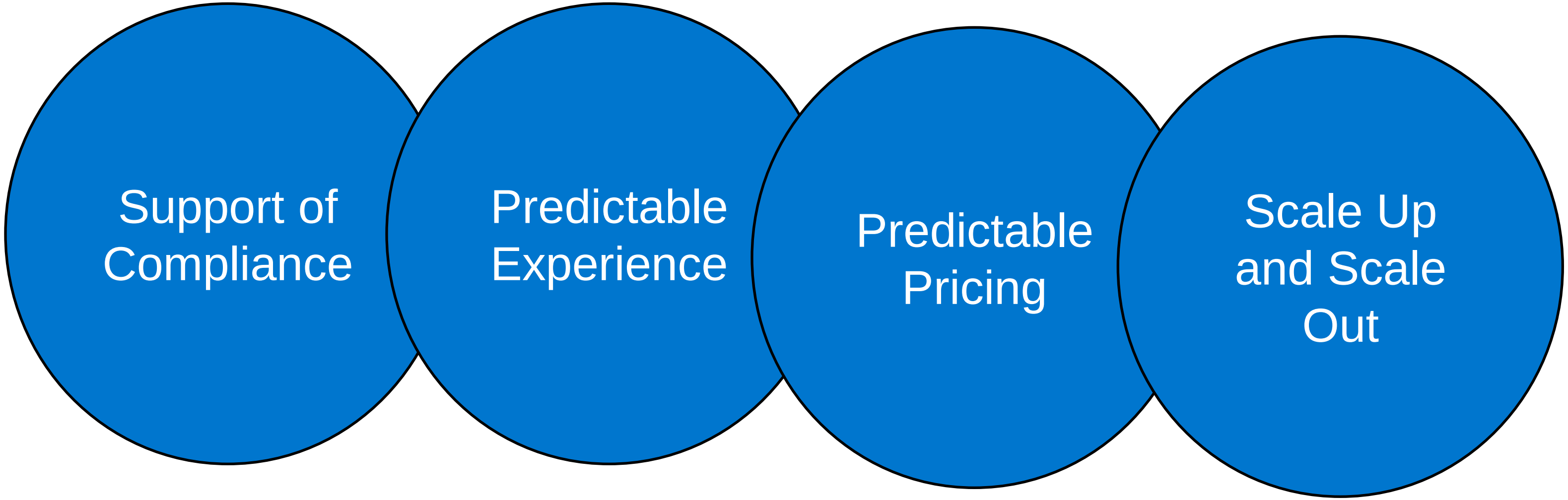
Recurring
Assessments


Dell Technologies
Trusted Hybrid Cloud
RSA SecurID
Multi-Factor Authentication
FORNETIX KMIP
HYTRUST
CloudControl – Workload Policy Enforcement
FORNETIX VAULTCORE
Cloud Access Security Broker
CIPHER
HSM
Security Architecture for Hybrid Cloud
VMware
Firewall
VxRail HCI
Dell Networking
Dell EMC Unity Storage
Dell EMC IDPA
Dell Technologies Trusted Hybrid Cloud
RSA NETWITNESS PLATFORM
Security Operations, Monitoring and Alerts
RSA Archer GRC
Risk Management/Governance
SOC and SIEM

- Full compliance setting reporting at implementation
- Capability to deliver recurring assessment for configuration compliance
- Tools to support Risk Assessment and Change Management processes

DELL Technologies

Value to Mission



Support of Compliance

Predictable Experience

Predictable Pricing

Scale Up and Scale Out

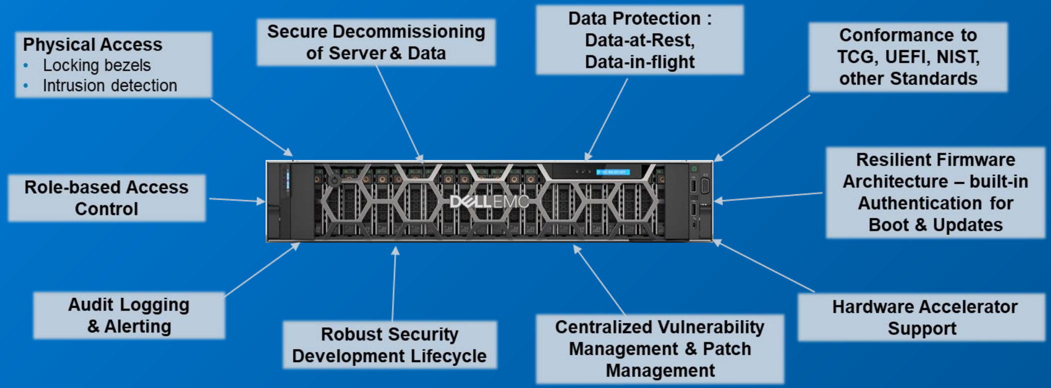
PowerEdge 14G

Domain Checklist

- ✓ Access Control
- ✓ Audit & Accountability
- ✓ Identification & Authentication
- ✓ Media Protection
- ✓ Physical Protection
- ✓ System and Comms Protection
- ✓ System and Info Integrity

Paired with OpenManage

- ✓ Asset Management
- ✓ Configuration Management
- ✓ Maintenance
- ✓ Manage Info Sec Continuity
- ✓ Security Assessment
- ✓ Situational Awareness



Physical Access
- Locking bezels
- Intrusion detection

Secure Decommissioning of Server & Data

Data Protection : Data-at-Rest, Data-in-flight

Conformance to TCG, UEFI, NIST, other Standards

Role-based Access Control

Resilient Firmware Architecture – built-in Authentication for Boot & Updates

Audit Logging & Alerting

Robust Security Development Lifecycle

Centralized Vulnerability Management & Patch Management

Hardware Accelerator Support

Security Needs to be Built-in, Not Bolted-on

System Lockdown

- Virtual lock for preventing configuration or firmware changes
- Alerts when configuration or firmware deviates from baselines

Hardware Root of Trust

- An immutable silicon-based root of trust to securely boot iDRAC and BIOS firmware
- Rapid recovery to a trusted image when authentication fails

Secure Default Password

- Prevents against inadvertent exposure of new iDRAC's on unprotected networks
- Encourages stronger password policies (rather than the tendency to use generic default passwords)

Dynamic USB Port Enable

- Allows USB port disable for normal operation in secure environments
- Dynamically can be unlocked via iDRAC authentication when needed without rebooting the server

OS Image Rapid Recovery

- Allows booting of a trusted backup OS image stored in hidden, protected storage

System Erase

- Quickly and securely erase internal server storage devices including HDD, SSD, and NVMe drives
- Wipe all user configuration and log file information

VxRail

Domain Checklist

- ✓ Access Control
- ✓ Audit & Accountability
- ✓ Identification & Authentication
- ✓ Media Protection
- ✓ Physical Protection
- ✓ System and Comms Protection
- ✓ System and Info Integrity
- ✓ Asset Management
- ✓ Configuration Management
- ✓ Maintenance
- ✓ Manage Info Sec Continuity
- ✓ Security Assessment
- ✓ Situational Awareness

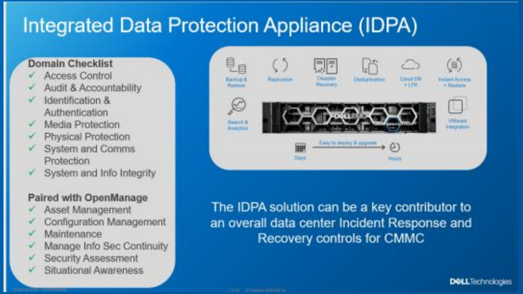
- FIPS 140-2 D@RE
- DISA STIG Hardening

The Secure Virtualization infrastructure of VMware

vmware®

vSphere, vSAN, vCenter, vRealize, Optional NSX

Capability to Add Virtualized Data Protection



Integrated Data Protection Appliance (IDPA)

Domain Checklist

- ✓ Access Control
- ✓ Audit & Accountability
- ✓ Identification & Authentication
- ✓ Media Protection
- ✓ Physical Protection
- ✓ System and Comms Protection
- ✓ System and Info Integrity

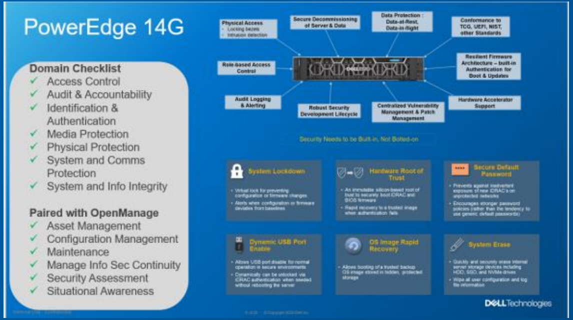
Paired with OpenManage

- ✓ Asset Management
- ✓ Configuration Management
- ✓ Maintenance
- ✓ Manage Info Sec Continuity
- ✓ Security Assessment
- ✓ Situational Awareness

The IDPA solution can be a key contributor to an overall data center Incident Response and Recovery controls for CMMC

DELL Technologies

All the HW Security of PowerEdge 14G Chassis



PowerEdge 14G

Domain Checklist

- ✓ Access Control
- ✓ Audit & Accountability
- ✓ Identification & Authentication
- ✓ Media Protection
- ✓ Physical Protection
- ✓ System and Comms Protection
- ✓ System and Info Integrity

Paired with OpenManage

- ✓ Asset Management
- ✓ Configuration Management
- ✓ Maintenance
- ✓ Manage Info Sec Continuity
- ✓ Security Assessment
- ✓ Situational Awareness

Physical Access
- Locking bezels
- Intrusion detection
Secure Decommissioning of Server & Data
Data Protection : Data-at-Rest, Data-in-flight
Conformance to TCG, UEFI, NIST, other Standards
Role-based Access Control
Resilient Firmware Architecture – built-in Authentication for Boot & Updates
Audit Logging & Alerting
Robust Security Development Lifecycle
Centralized Vulnerability Management & Patch Management
Hardware Accelerator Support
Security Needs to be Built-in, Not Bolted-on

System Lockdown

- Virtual lock for preventing configuration or firmware changes
- Alerts when configuration or firmware deviates from baselines

Hardware Root of Trust

- An immutable silicon-based root of trust to securely boot iDRAC and BIOS firmware
- Rapid recovery to a trusted image when authentication fails

Secure Default Password

- Prevents against inadvertent exposure of new iDRAC's on unprotected networks
- Encourages stronger password policies (rather than the tendency to use generic default passwords)

Dynamic USB Port Enable

- Allows USB port disable for normal operation in secure environments
- Dynamically can be unlocked via iDRAC authentication when needed without rebooting the server

OS Image Rapid Recovery

- Allows booting of a trusted backup OS image stored in hidden, protected storage

System Erase

- Quickly and securely erase internal server storage devices including HDD, SSD, and NVMe drives
- Wipe all user configuration and log file information

DELL Technologies

DELL Technologies

Storage

Domain Checklist

- ✓ Access Control
- ✓ Audit & Accountability
- ✓ Identification & Authentication
- ✓ Media Protection
- ✓ Physical Protection
- ✓ System and Comms Protection
- ✓ System and Info Integrity

PowerMax w/ Unisphere

- ✓ Asset Management
- ✓ Configuration Management
- ✓ Maintenance
- ✓ Manage Info Sec Continuity
- ✓ Security Assessment
- ✓ Situational Awareness

Dell EMC UnityXT

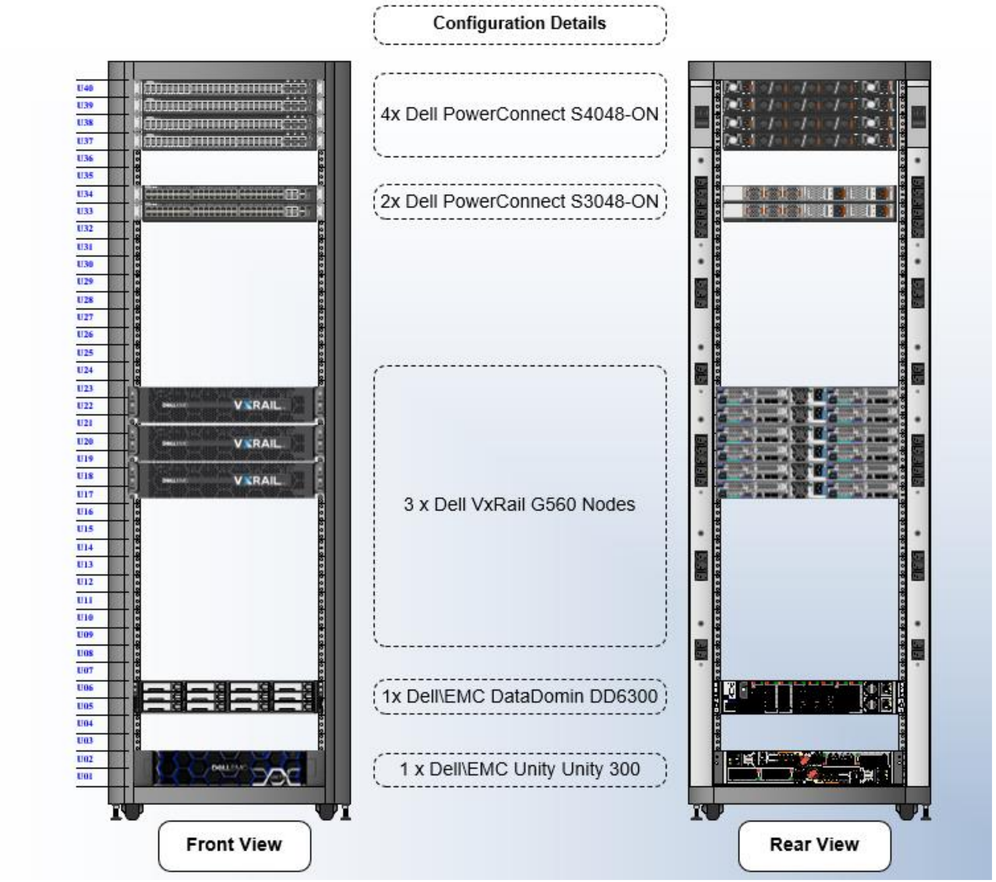
- FIPS 140-2 D@RE
- Data Protection via Snapshot and Replication
- High Availability and Redundancy
- Simple Security Hardening
- DISA APL Achievement

Dell EMC PowerMax

- FIPS 140-2 D@RE
- Data Protection via Snapshot and Replication
- High Availability and Redundancy
- Tamper Proof Audit Logging
- Centralized Inventory, Configuration, and Monitoring via Unisphere

DELL Technologies

Dell EMC Rack Elevations



Configuration Details

4x Dell PowerConnect S4048-ON

2x Dell PowerConnect S3048-ON

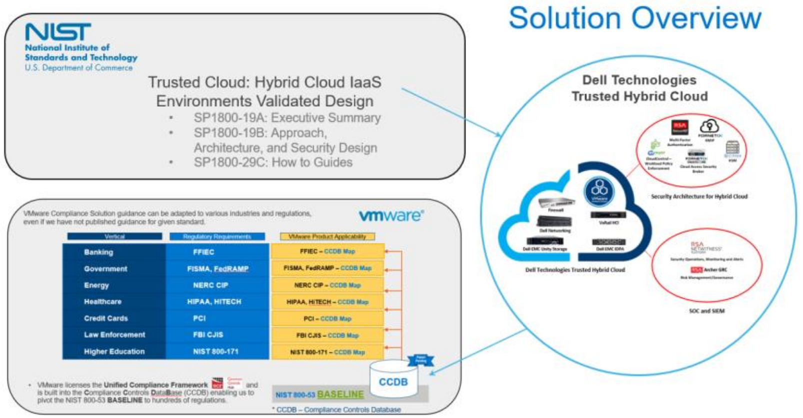
3 x Dell VxRail G560 Nodes

1x Dell\EMC DataDomin DD6300

1 x Dell\EMC Unity Unity 300

Time to Business or Mission Value

- Use of Pre-Configured Building Blocks
- Pre-coordinated partner collaboration for scoping, design, and delivery
- Documentation packages that support compliancy reporting requirements to help with auditing and reporting.



NIST National Institute of Standards and Technology U.S. Department of Commerce

Trusted Cloud: Hybrid Cloud IaaS Environments Validated Design

- SP1800-19A: Executive Summary
- SP1800-19B: Approach, Architecture, and Security Design
- SP1800-29C: How to Guides

VMware Compliance Solution guidance can be adapted to various industries and regulations, even if we have not published guidance for given standard.

Vertical	Regulatory Requirements	VMware Product Applicability
Banking	FFIEC	FFIEC – CCDB Map
Government	FISMA, FedRAMP	FISMA, FedRAMP – CCDB Map
Energy	NERC CIP	NERC CIP – CCDB Map
Healthcare	HIPAA, HITECH	HIPAA, HITECH – CCDB Map
Credit Cards	PCI	PCI – CCDB Map
Law Enforcement	FBI CJIS	FBI CJIS – CCDB Map
Higher Education	NIST 800-171	NIST 800-171 – CCDB Map

- VMware licenses the **Unified Compliance Framework** and is built into the Compliance Controls DataBase (CCDB) enabling us to pivot the NIST 800-53 **BASELINE** to hundreds of regulations.

* CCDB – Compliance Controls Database

vmware
CCDB
NIST 800-53 BASELINE
Solution Overview
Dell Technologies Trusted Hybrid Cloud
Multi-Factor Authentication
FORNETIX KMIP
CloudControl – Workload Policy Enforcement
Cloud Access Security Broker
HSM
Security Architecture for Hybrid Cloud
Firewall
VxRail HCI
Dell Networking
Dell EMC Unity Storage
Dell EMC IDPA
Dell Technologies Trusted Hybrid Cloud
RSA NETWITNESS
Security Operations, Monitoring and Alerts
RSA Archer GRC
Risk Management/Governance
SOC and SIEM