DELL Technologies

Solution Brief

Trusted Hybrid Cloud

Balancing Cybersecurity Compliance and Operational Requirements.

Achieving Parallel Goals

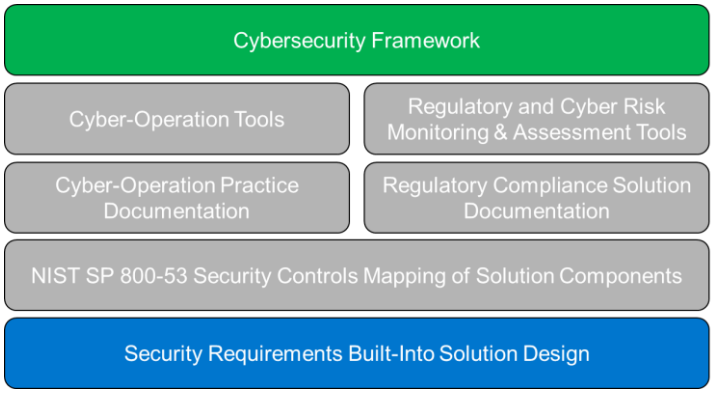
- Reduced IT costs through unification of cybersecurity operations and compliancy solutions.
- Detailed documentation sets supporting architecture, deployment, operation.
- 3rd Party security controls and penetration testing verification.
- Sustainable, repeatable and auditable regulatory compliance verification and reporting
- Single pane of glass for the management and monitoring of cloud workloads, including software configurations and vulnerabilities.
- Data protection and encryption key management enforcement focused on trust-based and geolocation-based/resource pools, and secure migration of cloud workloads.
- Key management and key store controlled by the organization, not the cloud service provider.
- Persistent data flow segmentation before and after the trust-based and geolocation based/resource pools secure migration.
- Industry sector and/or organizational business compliance enforcement for regulated workloads between the on-premises private and hybrid/public clouds

Overcoming the Challenge

IT organizations continuously work to balance focus, funding and resources to protect business critical data from the ever-emerging cybersecurity threats against their IT infrastructures. Implementing and maintaining an effective cybersecurity framework that accounts for data that is continuously expanding at the edge/IOT to the data center and into the cloud has never been more important.

Dell Technologies Trusted Hybrid Cloud

Dell Technologies has developed a cloud-based architecture that can be deployed both in Public, Private, and Hybrid scenarios that utilizes the same core architecture and components that can meet both compliance and operational cybersecurity requirements. The solution utilizes best of breed hardware and software from the Dell Technologies family allowing customers to run on-demand configurable pool of shared computing resources within their own architecture.



Dell Technologies Trusted Hybrid Cloud Solution established the NIST SP 800-53 security controls as part of the architecture design requirements. By implementing security control requirements as a design requirement, they become a feature deliverable of the solution and ensure accountability and documentation is achieved across the design process and is built-in VS being bolted on.

VMware has established a practice of mapping the controls of their solutions into a common control hub database tool. The tool uses the mapped controls to generate documentation sets for various operational and compliancy requirements. This capability was extended across all Dell Technology elements of the solution.

DELL EMC vmware RSA FORNETIX

Solution Overview

The Dell Technologies Trusted Hybrid Cloud utilizes solutions across the Dell Technologies portfolio including Dell EMC VxRail, Unity XT, and Dell Networking plus solutions from VMware and RSA.

VxRail is built on top of the latest Dell PowerEdge servers with embedded hardware and system-level security features to protect the infrastructure with layers of defense. Breaches are quickly detected, allowing the system to recover to a trusted baseline.

Dell Networking SmartFabric OS10 is a transformational software platform that provides networking hardware abstraction through a common set of APIs.

Dell EMC Unity XT storage provides critical security features, including Integrated Data Protection, encryption, file storage, and replication.

VMware Validated Design VMware Validated Design is a family of solutions for data center designs that span compute, storage, networking, and management, serving as a blueprint for your Software-Defined Data Center (SDDC) implementation. The documentation of VMware Validated Design consists of succeeding deliverables for all stages of the SDDC life cycle.

Dell Data Protection is delivered through the Data Domain Operating System (DD OS) with Avamar is the intelligence that powers Dell EMC Data Domain. It provides the agility, security and reliability, delivering scalable, high-speed, and cloud enabled protection storage for backup, archive and disaster recovery.

RSA SecurID uses identity insights, threat intelligence and business context to provide secure access to all of your users, across all of your applications, from the ground to the cloud.

RSA NetWitness Platform provides cyber operation tools that apply advanced technology to enable security teams to work more efficiently and effectively. It uses behavioral analysis, data science techniques and threat intelligence to help analysts detect and resolve both known and unknown attacks. It also uses machine learning to automate and orchestrate the entire incident response lifecycle.

RSA Archer provides the capability to better manage data protection requirements associated with industry standards and global regulations. Improve the classification and assess relationships between risks and controls that pertain to managing data.

Fornetix VaultCore is an encryption key management system that automates the full encryption key lifecycle. It enables secure management of up to hundreds of millions of keys across the entire enterprise from infrastructure to end point with little impact to performance. VaultCore is equipped to employ FIPS 140-2 level 2 validated root of trust.

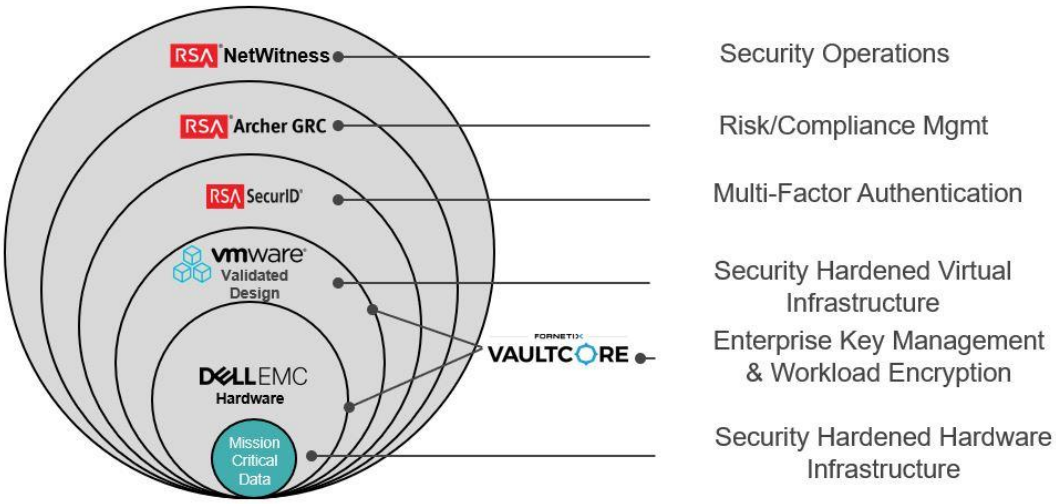


Figure 1 Security from the Center Out

All the components have security control mapping to ensure full support of a comprehensive security design and compliance documentation.

For more information on the solution please download the “h18115 02-20 Balancing Security Operations and Compliance” whitepaper from the Dell website. For sales availability contact your Sales Representative.