Dell VxRail: Comprehensive Security by Design

October 2023

H19058.3

White Paper

Abstract

This document describes integrated and optional security features, best practices, and proven techniques for securing your VxRail enironment from Core, Edge, and Cloud.

DELL Technologies

Contents

Executive summary

Overview

In today's world, business organizations and individuals have become accustomed to accessing the information they need 24 hours a day, seven days a week, often within seconds of making a request. To illustrate, an ad marketing study conducted by Google found that 53% of website sessions are terminated if pages take longer than three seconds to load.

Simultaneously, there is a significant and growing risk to preventing your business from being able to meet these demanding goals: the rising frequency and sophistication of cyber attacks. In 2021, ransomware attacks increased by 13% year over year, **as large an increase as in the previous five years combined**. Unlike other types of attacks, a ransomware attacker does not have to resell or otherwise exploit the data in your network.

A 2021 analysis by Verizon reported that an attacker may be interested in interrupting your business by encrypting the data and denying access to it.

When combining the criticality of data and the growing threat, being able to manage your cybersecurity risk is more important than ever. VxRail is the market-leading Hyperconverged Infrastructure (HCI) product, jointly engineered with VMware, with security built in at every step of the development life cycle, from the supply chain to software development, test, maintenance, and support. VxRail delivers an agile infrastructure with full stack integrity and end-to-end life cycle management to drive operational efficiencies and reduce risks, to enable your team to focus on your business.

Product security features from Dell Technologies and VMware are combined seamlessly in VxRail. This gives your business industry-leading flexibility in choosing the right options to manage your risk, enable your workforce, and deliver a seamless customer experience. In this document, we describe VxRail's approach to security in the following sections:

1. **Dell Advantages:** Describes Dell Technologies' commitment to develop secure software, secure the supply chain, and respond to security vulnerabilities
2. **Protect:** Provides an overview of the VxRail and VMware combined feature set, which can be enabled to avoid or stop a malicious attack
3. **Detect**: We describe the tools and interfaces we provide to monitor your VxRail cluster for malicious behavior or vulnerabilities
4. **Recover:** An overview of the Data Protection, High Availability, and Recovery features that can be enabled or integrated with your cluster to assure rapid business recovery in the event of an attack, to take the negotiating leverage away from the attacker
5. **Compatible standards and certifications**:VxRail's security development life cycle is intrinsically hardened in accordance with the NIST 800-53 standards. This enables us to help your organization comply with most industry standards, such as PCI/DSS, NERC-CIP, HIPAA, ISO, and others. This section provides the certifications VxRail has achieved.

6. **References**: We cannot cover all the technical details in this document, but we provide additional resources for you to learn the next layers of detail.

VxRail can help manage security and business risk, handle security breaches, recover from a ransomware attack, and build secure applications. This document describes the commitment to security that Dell Technologies delivers to enable you to move forward confidently into the multi-cloud/hybrid cloud era.

Revisions

Date	Part number/ revision	Description
September 2021		7.0.240 release updates
April 2022		7.0.350 release updates
September 2022		7.0.400 release updates
February 2023	H19058.1	Updated hardware availability in the 'VxRail: Recover' section.
May 2023	H19058.2	Updated information about Key Management Server
October 2023	H19058.3	Updated *VxRail STIG hardening package* section

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: William Leslie

Contributors: David Glynn, Vic Dery

Note: For links to other documentation for this topic, see the Dell Technologies Info Hub for VxRail.

Dell advantages

Secure Development Lifecycle

Delivering a comprehensive set of security features requires security to be prioritized at each stage of development. This process is called the Dell's Secure Development Lifecycle (SDL), which defines security controls that Dell product teams adopt while developing new features and functionality. Dell collaborates through many industry standard venues such as SAFECode, Building Security In Maturity Model (BSIMM), and IEEE Center for Secure Design to ensure that industry practices are followed.

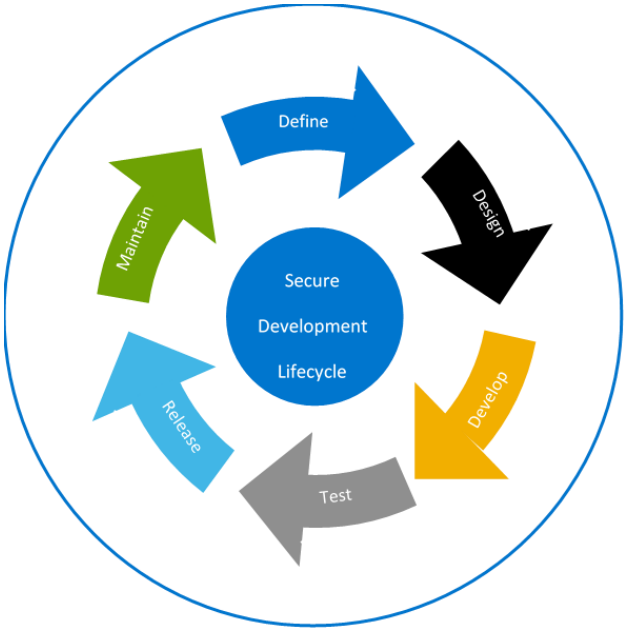


Figure 1. Secure development lifecycle

VxRail's Product Development includes security that is integrated through the product life cycle. Our product features are designed with security in mind, with our concepts and designs analyzed to assess the potential security impact. During development, we perform threat modeling, code reviews, and scanning of third-party components. Prior to release, we scan the software to ensure that open vulnerabilities have been updated, malware is not present, and the data can be transmitted and received securely.

Dell has identified a baseline set of security capabilities to be implemented across its portfolio. These baseline security capabilities help Dell products to be easily integrated with customers' security infrastructures and meet the customers' security objectives and compliance requirements. Dell executives from the business, the Product & Application Security Office (PAS), and other key stakeholders participate in this review process. The process reviews many factors, including the results of an internal security assessment of the product. The SDL is part of a broader set of processes within the secure design standard. The secure design standard is the benchmark for building security into Dell products.

The standard relates to the security of all product functionality and describes mandatory security functionality, which must be built into any product that is delivered by Dell to customers. This standard enables Dell products to meet customers rigorous security requirements, including:

- Help customers meet regulatory requirements
- Minimize the risks to Dell products and customer environments from security vulnerabilities.
- Source code protection identifies how to properly secure Dell engineering systems that contain source code to product-related intellectual property and ensure the integrity of products deployed to customer environments.

VxRail software lifecycle management and vulnerability response

One of the most critical actions an organization can take is to keep software updated. Updates and patches do not only fix issues that might lead to downtime or improve performance; they often fix security vulnerabilities. There is tremendous collaboration within the security community. VxRail being co-engineered with VMware, we are notified early on plans for security fixes, which enables the VxRail team to validate and prepare pre-qualified security patches quickly.

VxRail HCI system is the only system where all software components are engineered, tested, and released as a bundle. VxRail software bundles may include updates to BIOS, firmware, hypervisor, vSphere, or any included management components. When vulnerabilities are discovered, fixes are quickly developed to mitigate threats regardless of where they are. Update bundles are extensively tested on VxRail hardware platform and the entire VxRail software stack before being released to customers. When VMware makes a patch generally available (GA) for a critical level vulnerability, the VxRail team targets 14 days to validate and release a new VxRail update package and often provides them more quickly. See the following KB article for more information, VxRail Dell EMC: VxRail Synchronous Release Commitment for vSphere Releases | Dell US (requires login to view). Administrators are notified through the HCI System Software when updates are available and can also subscribe to Product and Security Advisories on the Dell Support Site. The administrator can download the update bundle directly and initiate or schedule an orchestrated update process. Updates are performed as rolling processes while the system remains online, serving the business. If a reboot is required, the VMs are automatically migrated to other nodes in the cluster before continuing.

Once our customers receive their Dell product, the security program does not end there because new vulnerabilities—particularly software and firmware-related—are discovered regularly across the industry. For this reason, Dell established a Product Security Incident Response Team (PSIRT), responsible for coordinating the response and disclosure for all identified product vulnerabilities per Dell's Vulnerability Response Policy. Dell strives to provide customers with timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities.

Typically, security updates are released to customers as new threats are encountered. Dell's Security Advisories and Notices are posted on the Security Advisories and Notices site.

Like the rest of our product security practices, Dell Vulnerability Response Practices are aligned to the Forum for Incident Response and Security Teams (FIRST), and international standards efforts involving vulnerability disclosure and handling, such as ISO 29147 and ISO 30111.

Supply chain risk management

Successful product security programs are comprehensive and extend to outsourced components and software. Integrity tests within the supply chain are essential for building and preserving trust. Dell Technologies has a formal Supply Chain Risk Management program that ensures the hardware and software components that are used in the company's products originate from properly vetted sources. Supply chain security is applying preventive and detective control measures that protect physical and digital assets, inventory, information, intellectual property, and people. Addressing information, personnel, and physical security helps provide supply chain security by reducing opportunities for the malicious introduction of malware and counterfeit components into the supply chain. Cybercriminals have also increased the targeting of supply chains with ransomware to extort organizations.

Proactive verification, validation, and security testing activities throughout the life cycle help ensure secure software and reduce the likelihood of malware or coding vulnerabilities being inserted into the software. A robust cybersecurity program improves software integrity by preventing unauthorized access to source code and minimizing the potential for malware to be introduced into a product before it is shipped to the customer. These measures are tightly aligned with Software Assurance Forum for Excellence in Code (SAFECode) guidelines[1] and ISO 27034[2].

Secured Component Verification

Another supply chain control available this year is Secured Component Verification (SCV), a Dell capability that provides last-leg assurance of product integrity from the time an order is fulfilled at the Dell factory to end-user delivery. Once a client or server product is built, a manifest of installed components will be generated, cryptographically signed by a Dell Certificate Authority, and stored securely within the system. Once the product is received, the customer, with a designated SCV Validation application, allowing them to verify and validate that no unauthorized system modifications have been made to the components.

[1] The Software Assurance Forum for Excellence in Code1 (SAFECode)

[2] ISO/IEC 27034

.

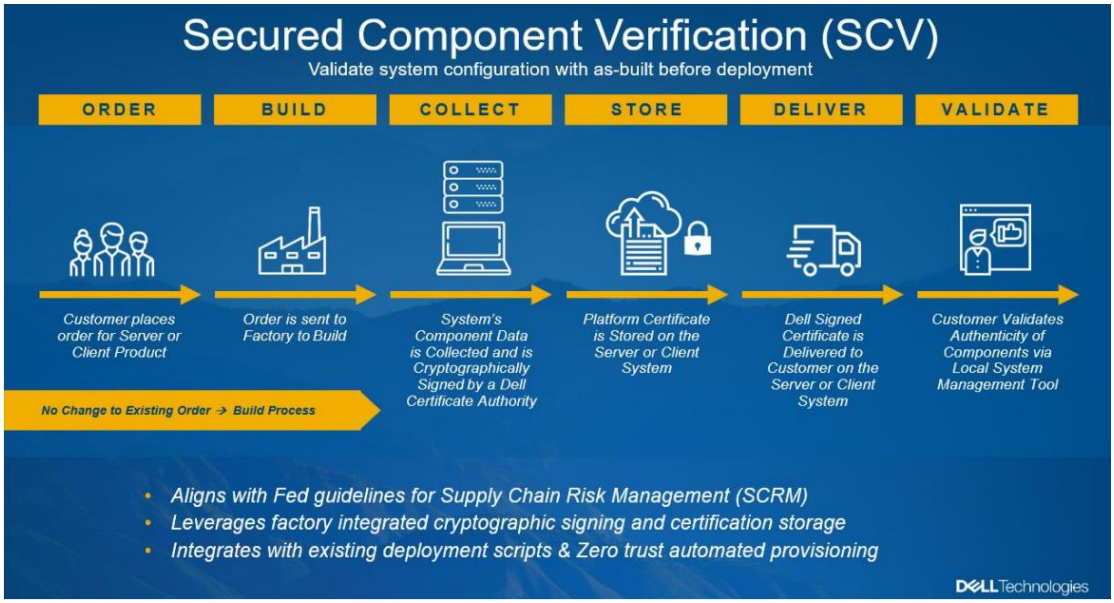


Figure 2. Secured component verification

VxRail: Protect

VxRail's has a wide range of security capabilities to protect your data infrastructure from cyberattacks, or ensure that the data is protected if a successful breach occurs. There are many layers of protection in VxRail, from the security features embedded in the PowerEdge hardware, to the virtualization software developed by VMware in the Application Layer, to the VxRail HCI software which serves as a secure link between these layers. Together, these work to protect critical components, such as the BiOS, Firmware, and the data stored in VSAN.

- Some of the key features (not an exhaustive set) will be discussed in this section:
- User Authentication and Authorization
- Secure Root of Trust
- vSAN encryption
- Signed LCM update bundles
- STIG Hardening

Dell hardware

VxRail is built on top of the Dell PowerEdge server platform that has embedded hardware and system-level security features to protect the infrastructure with layers of defense. Some of the differentiated security features in PowerEdge servers include:

System lockdown prevents unauthorized or inadvertent changes. This industry-first feature prevents configuration changes that create security vulnerabilities and expose sensitive data.

The cyber-resilient architecture with features such as UEFI Secure Boot, BIOS Recovery capabilities, and signed firmware provides enhanced protection against attacks.

System Erase can discover server-attached storage, including hard disk drives (HDDs), solid state drives (SSDs), self-encrypting drives (SEDs), Instant Secure Erase (ISE), and nonvolatile memory drives (NVMe's). Data stored on ISE, SED, and NVMe devices can be made inaccessible using cryptographic erase, while devices such as non-ISE SATA HDDs can be erased using data overwrite.

Dell PowerEdge servers are the critical hardware that makes up the nodes in a VxRail cluster. Each node's CPU, memory, and disk resources provide the pooled resources for the cluster, and the network interfaces provide connectivity. The secure Dell PowerEdge servers are therefore the foundation for VxRail security.

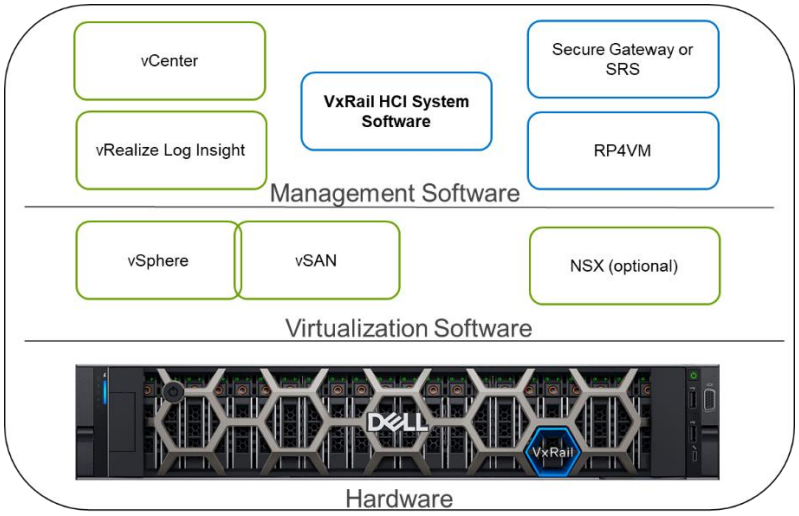


Figure 3. Security built into every layer of VxRail hardware, virtualization software, and management software

PowerEdge servers have an integrated remote access controller, called iDRAC. iDRAC uses secure communication, authentication, and role-based access controls to enable secure remote management and configuration of the physical system. With configurable alerts, iDRAC can send event information to your Security Incident and Event Management (SIEM) system whenever the hardware is accessed, or the configuration is changed. Detecting and reporting unauthorized changes protects the integrity of a VxRail. For more information about the security of Dell PowerEdge servers, see Cyber Resilient Security in Dell PowerEdge Servers.

PowerEdge servers use cryptographically signed and verified firmware to build a system of trust. Leveraging security technologies built right into the silicon. Capabilities like Intel's Trusted Execution Technology (TXT) verify that the server performs only the intended version of firmware, BIOS, and hypervisor while preventing the undetected introduction of malware. The following figure illustrates the hardware Root of Trust.

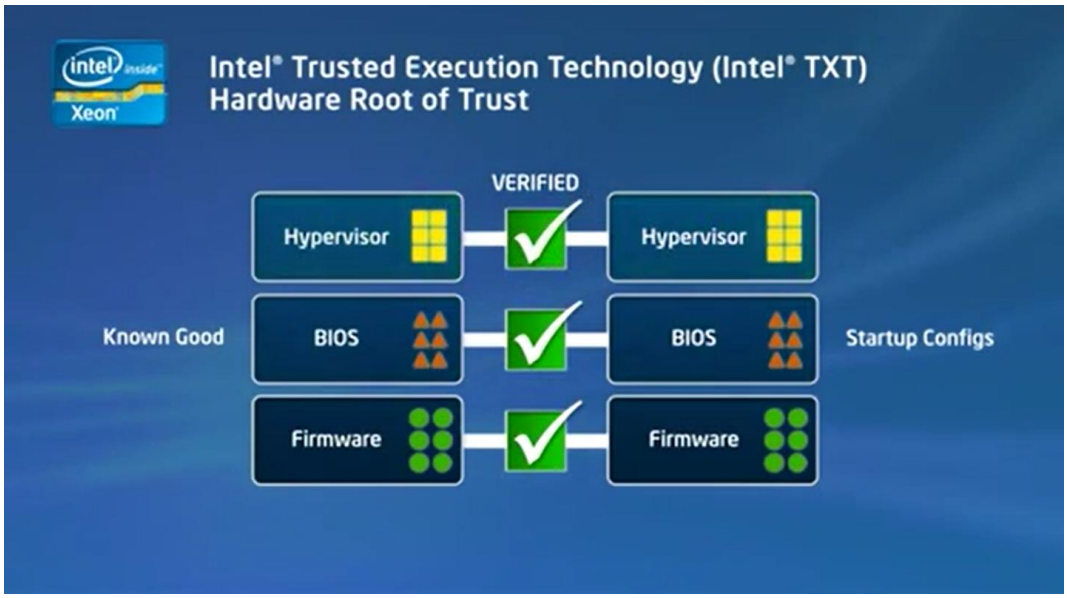


Figure 4. Hardware Root of Trust

VxRail can achieve even higher protection levels of server integrity by configuring the nodes with an optional Trusted Platform Management (TPM) module. TPM is an international standard for secure crypto-processors, a dedicated microcontroller that is designed to provide high security for cryptography keys, and an option for all VxRail processors.

VxRail physical location security

Physical security is an essential part of any comprehensive security solution. Because a VxRail may be deployed outside of a traditional data center, physical security (for example, bezel locks) can take on even greater importance. To prevent malware or infected software from being introduced from a USB drive, the USB ports on a VxRail can be disabled and then enabled only when needed.

VxRail nodes also monitor for other events such as chassis openings, parts failure or replacement, firmware changes, and temperature warnings. This information is recorded in the iDRAC Lifecycle Log. A chassis does not have to be opened frequently after it is put into production. Tracking such activity could be an indicator of an attempt to compromise the system.

Dell VxRail HCI system software

VxRail HCI system software is the foundation for the value differentiating the capabilities of VxRail. From an infrastructure stack perspective, the management software runs as a virtual machine on top of the VMware software and the PowerEdge server to allow VxRail to act as a singular unified system.

Digitally signed lifecycle management

VxRail lifecycle management upgrade packages include digital signatures. Digital signatures create a virtual fingerprint that is unique to packages. The use of digital signatures provides a secure way to ensure that the upgrade package is authentic and valid. VxRail lifecycle management bundle is calculated using the SHA384 hashing algorithm and stored in a manifest file which is digitally signed, thus ensuring the integrity of the lifecycle management upgrade package and assurance that the source is Dell

Technologies. The customer can follow a SolVe procedure to validate the digital signature and message digests in the manifest.

Files that cannot be cryptographically signed, such as firmware, should be verified using the SHA256 hashing algorithm.

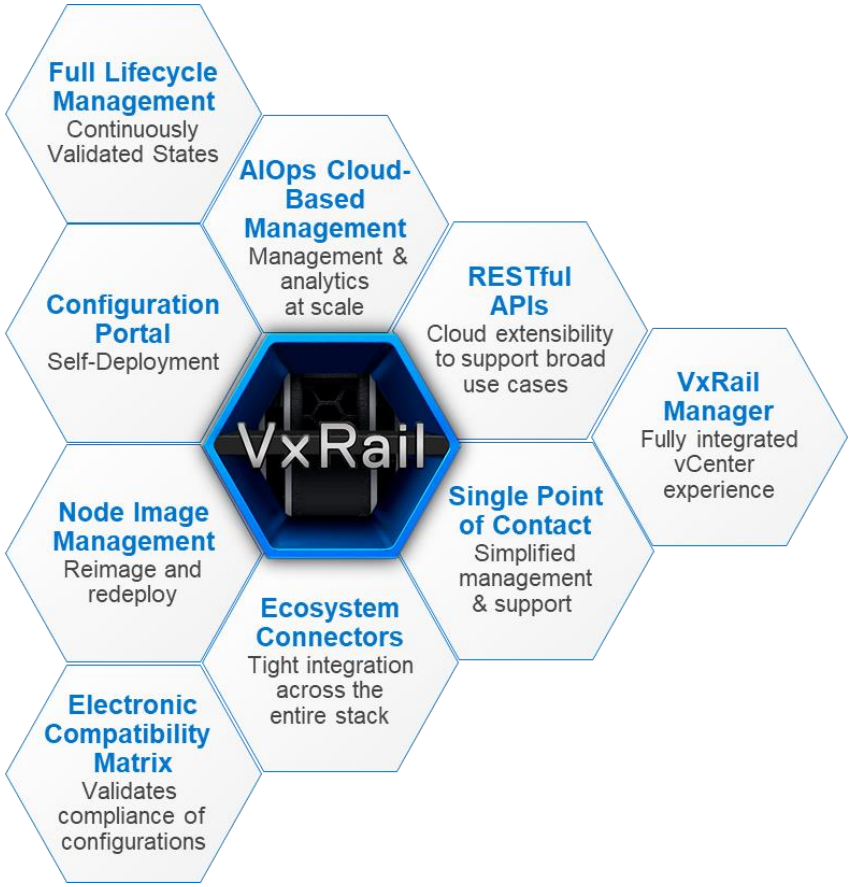


Figure 5. VxRail HCI system software key services

Continuously Validated States: VxRail runs on pre-tested and validated software and firmware for the entire VxRail stack, including the VMware software and PowerEdge server components. In addition, VxRail lifecycle management capabilities ensure that VxRail clusters are running in that known good state throughout its entire lifecycle as the cluster goes through continuous changes to take advantage of the latest VMware software innovation, security, or recovery. The term “Continuously Validated States" encapsulates the configuration stability delivered by VxRail clusters through the lifecycle management process.

Electronic Compatibility Matrix: With all these different software and hardware components in the stack, the VxRail team is continuously testing and validating against the entire stack so that whatever preferred state the user determines from the VMware compatibility matrix has been validated in a Continuously Validated State. In addition, VxRail uses this matrix to ensure the cluster configuration stays in compliance. These benefits drastically reduce the testing effort and resources that a customer would have to invest while also giving the customer the peace of mind required to predictably and securely evolve their VxRail clusters without impacting application workloads.

Ecosystem connectors: To build an extensive Electronic Compatibility Matrix, VxRail has to communicate with ecosystem members in the stack, including vSphere, vSAN, vCenter, and the PowerEdge server and multiple hardware components within. The connectors allow VxRail to know the software and firmware versions running in each component and lifecycle manage those components. In addition, the automation and orchestration capabilities enable VxRail to be managed as a singular unified system.

VxRail Manager: The primary management user interface for VxRail is the vCenter plugin-in called VxRail Manager. Providing a fully integrated vCenter experience, VxRail users perform all VxRail activity through this interface.

VMware software

An important part of maintaining security is ensuring that all the relevant security configuration elements are implemented on all the objects in an environment. An individual VxRail cluster can have up to 64 physical nodes, and multiple VxRail clusters can be managed by one vCenter, thus supporting thousands of VMs. Even a simple change—if it must be configured on all the VMs—could take a significant amount of time to enact. In addition, when performing repetitive tasks, people are prone to make mistakes. This is where automation becomes critical.

Automation allows an environment to have fewer configuration errors and more consistent configuration while increasing efficiency and reducing the time between when a decision is made and implemented, increasing the time to value those decisions.

Compatible tools like vRealize Automation, which allows the automation of vSphere and vSAN. vRealize Automation can also be used to validate that the security configuration has not drifted from its appropriate settings. In addition, because vRealize Automation is a standard VMware tool, many IT virtualization teams already know how to work with vRealize Automation and have created profiles that will work with a VxRail cluster.

VMware key virtualization and management software

The VMware software suite provides VxRail with a highly available, resilient, on-demand virtualized infrastructure. ESXi, vSAN, and vCenter Server are core components of vSphere. ESXi is a hypervisor that is installed on a physical VxRail server node in the factory that enables a single physical server to host multiple logical servers or VMs. vSAN is the software-defined storage that is used by the VMs, and VMware vCenter Server is the management application for ESXi hosts, vSAN, and VMs.

Like Dell, VMware follows a rigorous Secure Software Development Lifecycle process and Security Response Center. VxRail is jointly developed and supported with VMware, ensuring that all components in the solution are designed, built, tested, and deployed with security as a top priority. For more information, see VMware Product Security.

VMware ESXi hypervisor

In VxRail, the ESXi hypervisor hosts the VM on cluster nodes. VMs are secure and portable, and each VM is a complete system with processors, memory, networking, storage, and BIOS. VMs are isolated from one another, so when a guest operating system running on a VM fails, other VMs on the same physical host are not affected and continue to run. VMs share access to CPUs and ESXi is responsible for CPU scheduling. Also, ESXi assigns VMs a region of usable memory and manages shared access to the physical network cards and disk controllers that are associated with the physical host. All

X86-based operating systems are supported, and VMs on the same physical server hardware can run different operating systems and applications.

VxRail virtual networking security

Dynamic virtual environments such as VxRail often benefit from the flexibility that software defined security services provide.

VxRail uses VMware Distributed Virtual Switches that segment traffic by default using separate VLANs for Management, vSAN, vMotion, and application traffic. The vSAN and vMotion networks are private, non-routable networks. Depending on the applications supported by a VxRail network, traffic could be further segmented based on different applications, production and non-production traffic, or other requirements.

The Distributed Virtual Switch on a VxRail is configured by default with vSphere Network I/O Control (NIOC). NIOC allows physical bandwidth to be allocated for different VLANs. Some cyberattacks, such as a denial of service and worms, can lead to the overuse of resources. This can cause a denial of resources to other services that are not directly under attack. NIOC can guarantee that other services will have the network bandwidth that they need to maintain their integrity in the event of an attack on other services. NIOC settings are automatically configured following recommended best practices when the system is initialized. The Dell Network Guide includes details of the NIOC settings for the default VxRail VLANs.

Each VxRail node has a separate physical Ethernet port for the iDRAC hardware management interface. Physically segmenting this network makes it difficult for attackers to gain access to hardware management. Also, if a distributed denial-of-service attack occurs, this physically segmented network will not be affected, limiting the scope of a potential attack.

VMware NSX (optional)

The easiest way to provide advanced capabilities on VxRail is with VMware NSX. NSX requires an optional software license as it is not included with VxRail by default. NSX is a powerful complete network virtualization and security platform that allows administrators to create entire virtual networks. Which decouples from the underlying hardware and enables customers to implement advanced network security services such as micro segmentation that have not been feasible to implement using hardware-based approaches.

Administrators have the flexibility to independently implement NSX security features with VxRail without having to implement any software defined networking. This opens the door for customers to leverage NSX without disrupting existing networking topologies and operating models. With NSX, VxRail administrators can configure micro-segmentation to secure and isolate different tenant workloads, control ingress, and egress and provide enhanced security for all workloads, including traditional multitier applications and general purpose VM as well as VDI environments.

The benefits of using NSX with VxRail include the ability to incorporate intrinsic network security into the virtualized infrastructure stack. Customers can deliver granular protection with network segmentation and micro-segmentation to individual workloads, create context-aware security policies, and leverage IDS/IPS to defend against lateral threats.

All of this can be implemented easily and seamlessly using an available simplified management with security experience that is integrated with the vSphere stack and managed centrally through the vSphere HTML5 Web Client and NSX Manager plug-in respectively.

UEFI secure boot

UEFI secure boot protects the operating system from corruption and rootkit attacks. UEFI secure boot validates that the VxManager operating system, firmware, boot loader, and VMkernel are all digitally signed by a trusted authority. UEFI secure boot for ESXi validates that the VMware Install Bundles (VIBs) are cryptographically signed. This ensures that the server boot stack runs all genuine software and has not been changed or substituted.

Software checksum

A key part of data integrity is validating that the data that is retrieved from storage has not been altered since it was written. VxRail uses block level end-to-end data integrity checksum by default. The checksum is created when the data is written. The checksum is verified on reads, and if the checksum shows that the data had changed from when it was written, it is reconstructed from other members of the RAID group. vSAN also uses a proactive scrubber mechanism to detect and correct potential data corruption, even on infrequently accessed data.

Storage Policy Based Management (SPBM)

vSAN is policy-driven and designed to simplify storage provisioning and management. vSAN storage policies are based on rule sets that define storage requirements for VMs. Administrators can dynamically change a VM storage policy as requirements change. Examples of SPBM rules are the number of faults to tolerate, the data protection technique to use, and whether storage-level checksums are enabled.

Encryption

Preventing sensitive information from reaching the wrong people while ensuring appropriate, authorized access to a company's data is a fundamental problem summed up as confidentiality or privacy. VxRail addresses the confidentiality of data in use, data in motion, and data at rest.

vSphere encryption

Individual VMs can be encrypted using vSphere Encryption, and VMs in motion can be encrypted using vMotion encryption. This encryption is embedded into the VMware solution and can be used without the use of any additional third-party software. The keys for vSphere encryption are controlled at the hypervisor level; thus, VMs do not have access to them.

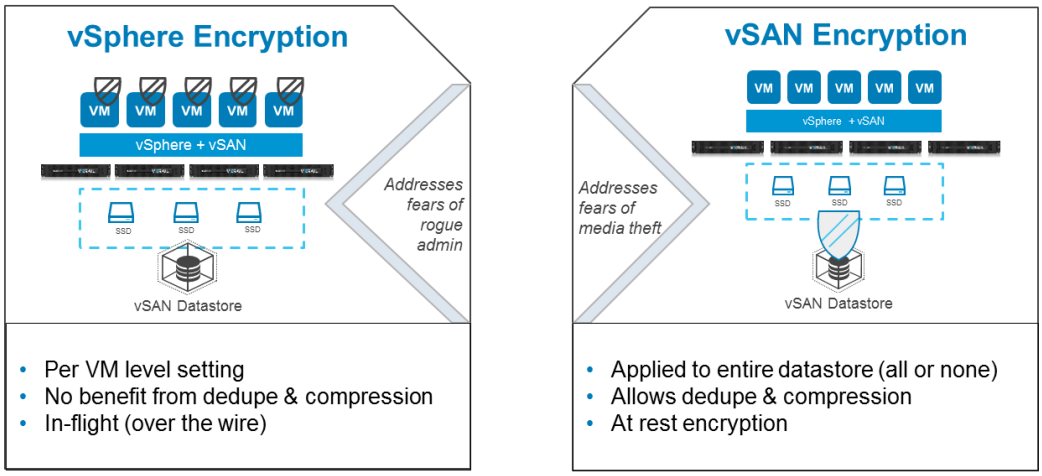
VM Encryption provides the flexibility to enable encryption on a per-VM basis, which means a single cluster can have encrypted and non-encrypted VMs. VM Encryption follows the VM wherever it is hosted. So even if the VM were moved to a datastore outside VxRail, it would remain encrypted.

VxRail supports encrypted vMotion, where VMs are encrypted when they are moved between hosts. This includes vMotion migrations within a VxRail and vMotion migrations to or from a VxRail cluster within a vCenter instance. Encrypted vMotion can be used with

vSAN encryption to have data at rest encryption and data-in-transit encryption. Encrypted vMotion is enforced for VMs with vSphere Encryption enabled.

vSAN encryption

Data-at-rest encryption (D@RE) from vSAN, which offers FIPS 140-2 verified security, can be used with VxRail to encrypt a datastore. In addition to protecting your workloads, vSAN encryption is the easiest and most flexible way to encrypt data at rest because the entire vSAN datastore is encrypted with a single setting. This encryption is cluster-wide for all VMs using the datastore. Encrypted VM data typically does not benefit from space-reduction techniques such as deduplication or compression. However, with vSAN, encryption is performed after deduplication and compression, so the full benefit of these space reduction techniques is maintained.



Both require use of a supported external key management server (KMS)

Figure 6. VM encryption vs. vSAN encryption

Key Management Server (KMS)

Except for Encrypted vMotion, where vSphere provides the temporary keys that are used to encrypt the data in motion, a Key Management Server (KMS) is required for the secure generation, storage, and distribution of the encryption keys. When encryption is enabled, vCenter establishes a trust relationship with the KMS, and then passes the KMS connection information to the ESXi hosts. The ESXi hosts request encryption keys directly from the KMS and perform the data encryption and decryption. vCenter connectivity is only required for the initial setup.

Because the KMS is a critical component of the security infrastructure, it should have the same level of redundancy and protection that is typically applied to other critical infrastructure components, Such as DNS, NTP, and Active Directory. It is important to remember that the KMS should be run physically separate from the elements that it encrypts. During startup, the ESXi hosts will request the keys from the KMS. If the KMS is unavailable, the system cannot complete the startup.

VxRail and VMware support KMSs that are compatible with Key Management Interoperability Protocol (KMIP) v1.1 or higher. VMware maintains a Compatibility Guide of KMSs that have been validated with vSphere here: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms

Within vSphere, encryption is handled by a common set of FIPS 140-2 validated modules. These common modules are designed, implemented, and validated by the VMware Secure Development Lifecycle. Having a set of common modules for encryption allows VxRail to make encryption easier to implement, manage, and support.

Encryption is enabled on VxRail through a simple configuration setting in vCenter. Access controls ensure that only authorized individuals are allowed to enable or disable encryption. A "No Cryptography Administrator" role empowers an administrator to do everyday administrative tasks but without the authority to alter encryption settings.

Encryption is a powerful tool for protecting the confidentiality of information, and VxRail has built in encryption capabilities to protect data in use, in motion, and at rest. However, the data security that is provided by encryption is only as good as the generation, protection, and management of the keys used in the encryption process.

Encryption keys must be available when they are needed, and access to the keys during decryption activities must be preserved for the lifetime of the data. The proper management of encryption keys is essential to the effective use of cryptography. Many organizations centralize key management across the enterprise to simplify management, enforce policy, and provide reporting and auditing for compliance.

VxRail and vSphere support the Key Management Interoperability Protocol (KMIP), allowing it to work with many enterprise key management systems. For organizations that have existing key management services, VxRail and vSphere easily integrate, providing a single point of key management across the enterprise. VMware offers a list of compatible key management servers.

VxRail Manager FIPS 140-2 Level 1

As part of FIPS 140-2 Level 1 compliance, VxRail added the following capabilities to VxRail Manager virtual appliance as of VxRail 7.0.010 release.

- VxRail Manager - Implemented the Dell OpenSSL FIPS validated crypto modules to protect data-in-transit
- VxRail Manager - FIPS mode enabled in VxRail Manager operating system
- VxRail Manager - Storage of keys and credentials using Dell BSAFE Crypto-C Micro Edition and two FIPS validated cryptographic modules using AES 256-bit

Note: Dell uses the Dell FIPS-compliant crypto module.

Hardware based encryption

In VxRail satellite nodes, hardware based encryption is supported through support of Self-Encrypting Drives, or SED’s. SED’s protect against physical theft of drives, and the subsequent compromise of data privacy. If a cyber-criminal were to attempt to access the data stored on the drive, he or she will not know the required locking key passphrase and therefore be thwarted from accessing the encrypted drive data.

To support key management for the SED’s, VxRail has a solution called Secure Enterprise Key Manager (SEKM). SEKM enables the customer to use either an external Key Management Server (KMS) or the iDRAC Key Manager to manage the keys that encrypt or decrypt SEDs on the VxRail appliance.

Note: Hardware encryption (SED's) is available using iDRAC through the Native Key Provider with VxRail satellite nodes. Please contact your Dell sales rep for use in vSAN based VxRail nodes.

Lockdown mode

For environments needing even greater security with flexibility, lockdown mode can be configured for the ESXi. In lockdown mode, the ability to perform management operations on individual hosts is further limited, forcing management task completion to occur through vCenter where they can be logged against the user who performed them.

Lockdown in "Normal" mode allows a select group of users to be on an allow list, enabling them to manage the servers locally instead of through vCenter; this allow list must include VxRail management accounts.

In strict lockdown mode, no users are allowed to manage the servers locally. VxRail does not support lockdown in "Strict" mode.

Secure management with HTTPS

Unsecured management traffic is a significant security risk. Because of that, VxRail management interfaces communicate over a TLS channel with various components vCenter, iDRAC, and HCI System software components to ensure the data-in-flight is secure over HTTPS protocol. Reference support material for current TLS versions as they are subject to change. In addition, access to the command line of the ESXi servers must use SSH.

VxRail STIG hardening package

Configuring security can be a complex, error-prone process with many of the same risks that it seeks to mitigate. Many organizations use Security Technical Implementation Guidelines (STIG) or Security Readiness Guide (SRG) documents, as published by Defense Information Systems Agency (DISA) as a baseline to harden their systems. To help our customers meet their security and regulatory requirements, Dell Technologies makes an automated hardening package available to VxRail customers, at no additional charge.

The STIG package includes an assessment index with details out each STIG control level, and a hardening guide. Customers can perform the hardening scripts or these scripts can be run by Dell Professional Services, as a service engagement. Individual SRG/STIGs that are covered by the package include:

- Application Security Development
- Application Server SRG
- VMware vSphere ESXi
- VMware vSphere vCenter
- VMware vSphere Virtual Machine
- Apache Tomcat Application Serve
- PostgreSQL

- Network Device management

Note: For specific versions see the VxRail Security Configuration Guide link directly below

As an added benefit, the STIG package has user options to harden individual system components, individual nodes, or entire VxRail clusters. Dell Technologies is committed to generating applicable updates to the package when new STIG documents become available through DISA.

VxRail running VxRail 7.x are compatible with the VxRail STIG hardening package requirements. See VxRail STIG Compliance Guide and automated hardening scripts for more information. A valid Dell Support login is required for access.

VxRail: Detect

Across all industries, organizations are modernizing and transforming how they operate and deliver differentiated products and services. Where data resides, how it is accessed, and the number of devices, from Cloud to Core to the Edge all need to be monitored. What one does not monitor, one cannot detect (attr. Anonomys). Security will always be a part of IT, focusing on authentication, firewalls, compliance, and cybercriminals. Security is no longer a set of projects but a continuous life cycle that requires constant review and analysis. Dell Technologies believes that security never slows you down and instead accelerates innovation, allowing you to think in new, strategic ways and seize the opportunity.

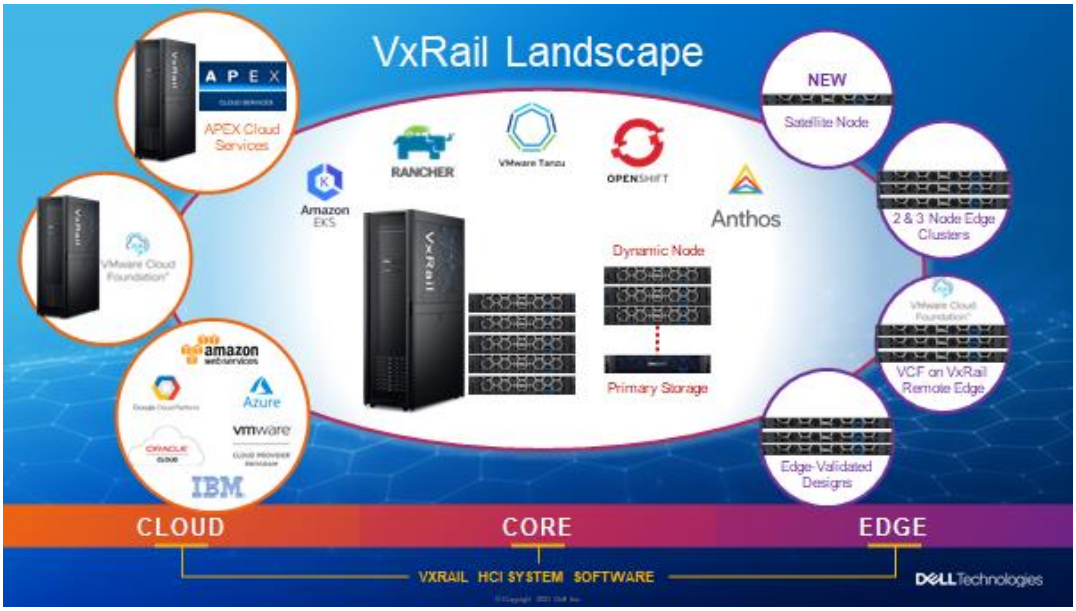


Figure 7. From Cloud to Core to Edge

Dell VxRail is no exception to providing a fast and simple path to this security transformation from Cloud to Core to Edge. VxRail delivers an agile infrastructure with full stack integrity and end-to-end lifecycle management to drive operational efficiencies, reduce risks, and enable teams to focus on the business. Adoption of VxRail systems that break down operational silos and enable continuous innovation through rapid provisioning and deployment of workloads results in significant cost savings and operational

efficiencies, enabling IT organizations to drive business opportunities rather than only support business operations. VxRail is built for VMware, with VMware, to enhance VMware. VxRail is the first and only HCI system jointly engineered with VMware to eliminate the operational complexity of deploying, provisioning, managing, monitoring, and updating of VxRail HCI.

VMware vRealize Log Insight

VMware vRealize Log Insight monitors system events and provides ongoing holistic notifications about the virtual environment and hardware state. vRealize Log Insight delivers real-time automated log management for VxRail with log monitoring, intelligent grouping, and analytics to simplify troubleshooting at scale across VxRail physical, virtual, and cloud environments. Centralized logging is a fundamental requirement of a secure infrastructure. VxRail easily integrates using the industry standard Syslog protocol for customers who already have a logging facility or SIEM.

VxRail authentication, authorization, and accounting

As Zero Trust design is the north star of designing and delivering more secure offerings, the VxRail product team engineers in significant Authentication, Authorization, and Accounting (AAA) capabilities into the VxRail HCI System Software. AAA is designed to control access, ensuring the right person is using the system, provide what level of access they have, and log activity to account for what has been done and by whom. Role Based Authentication Control (RBAC) is an example of one of the ways this is built into the management framework of VxRail.

Authentication

Authentication to HCI System Software is handled by vCenter SSO, mediating access to the vCenter plug-in and by the VxRail API. vCenter supports the organization's centralized identity management system in accordance with authentication security policies.

Organizations often centralize identity management using directory services such as Microsoft Active Directory (AD) or LDAP. If VxRail is a stand-alone environment and not part of a domain, users and passwords can be managed locally in vSphere and iDRAC. From a best practice's stance, it would be recommended to use centralized authentication.

Many environments strengthen their identity management using multi-factor authentication that requires an additional level of identity verification, including certificates, smartcards, or security tokens, in addition to a username and password. VxRail fully supports multi-factor authentication (MFA) for both the domain and locally managed users through vSphere integration with partner MFA solutions.

Often there may be different individuals responsible for the physical servers, VxRail lifecycle management, and the management of the server, storage, and network virtualization environment. VxRail uses fine-grained, role-based access controls for iDRAC, HCI System Software, and vSphere. iDRAC also supports Secure Enterprise Key Management (SEKM), which works on encrypted drives across data centers, remote locations, and in the cloud, and provides extra protection beyond Local Key Manager.

Identity and Access Management

VxRail supports local vSphere user accounts, AD or LDAP integration, vCenter single sign-on, and Active Directory Federation Services (ADFS). Although it is possible to have a stand-alone VxRail, most environments integrate with enterprise Identity and Access

Management (IAM) systems that use directory services such as Microsoft Active Directory.

Authorization

Using the “principle of least privilege” (POLP), a user is granted the required rights to perform their role but no more than is needed. vSphere includes several predefined roles that are used to grant appropriate privilege. For example, a user may be granted the role of vSphere Administrator, HCIA Management, or both. The HCIA Management role grants a user privilege to perform VxRail lifecycle management tasks from VxRail management plug-in within vCenter. vSphere Administrator grants privilege to perform Administrator tasks in vCenter. vSphere allows an even granular level of access control by the creation of custom roles. For example, a privileged user may be granted the ability to acknowledge an alarm or create a storage profile but not deploy VMs.

Roles are associated with users and groups and with specific objects, where an object is a thing or group of things. For example, a user or group might have permission to acknowledge alerts for a particular VM or port, but not other objects. Also, restrictive roles such as No Access may be assigned to users, preventing them from seeing specific areas within vCenter. Multiple users or groups can be granted the same or different levels of access to the same object. Permissions granted to a child object can be used to override permissions inherited from a parent object.

vCenter Server Role-Based access control supports the granular security principles of “Least Privilege” and "Separation of Responsibility” and allows the security administrator to enhance security by defining precise permissions based on the systems management structure organization.

Accounting

Understanding changes in configuration and component status is vital to keeping systems secure and available. Changes may be the result of a temporary fix causing a configuration drift. For example, if someone updates a component of the VxRail software’s continuously validated state without using VxRail LCM or vLCM to perform the upgrade with the VxRail software download. Or these changes could be an indication of a possible intrusion. Proactively monitoring infrastructure is an important security activity.

Timely detection when an intrusion happens can mean the difference between a brief interruption where the attacker is unable to compromise any critical systems, and an intrusion that persists for months leading to the compromise of multiple critical systems. Failure to maintain a system of audit logs may not provide adequate information about the attack to determine severity.

The challenge with monitoring the information is that it comes from many different sources—an individual VM, a physical server, the virtualization infrastructure, the network, security components, or the applications themselves. Making sense of this information requires a consolidated view of activity and changes. VxRail includes vRealize Log Insight. Log Insight compiles VMware logs, including servers, network devices, storage, and applications. As the graphic below shows, Log Insight creates a dashboard with graphs based on the data in the logs. This helps the administrator quickly and easily examine the root cause of the issue.

Correlating all of this information is one of the many reasons that VxRail uses the industry standard Network Time Protocol (NTP) to keep all the component clocks synchronized.

CloudIQ

CloudIQ combines proactive monitoring, machine learning, and predictive analytics so you can take quick action and simplify operations of your on-premises infrastructure and data protection in the cloud. It is included with many Dell offerings to enable our customers a way to manage a broader set of their infrastructure real estate to make more efficient decisions. CloudIQ supports a broad range of Dell Technologies products including: Storage, data protection, converged and hyperconverged infraastucture, networking and APEX services. CloudIQ supports VxRail by providing multiple cluster views, including: health score, system configuration, capacity, and performance. These views provide information across the cluster, and system health issues provide recommended remediations or links to relevant Knowledge Base (KB) articles.

Telemetry data sent to Cloud IQ is secured by end-to-end Transport Layer Security (TLS) 256-bit encrypted tunnels, and is handled in accordance with Dell's customer data policy. No customer data is sent, only data generated by the customer's systems. Customers control which systems send information over these channels. Further technical detail on CloudIQ's security posture is available in the CloudIQ Security Paper.

VxRail users can access CloudIQ using their Dell support credentials.

VxRail: Recover

Business continuity is critical to ensure ongoing operations for your customers, investors, regulators, and employees. By proper management of your organization's risk of data theft or loss, you can save capital expense, operational expense, and corporate reputation. VxRail's joint engineering with VMware, including, software lifecycle management, vSphere availability features, proactive monitoring, integrated recovery, and physical security of the hardware and secure system configuration ensure maximum system availability. In combination with VxRail hardware resiliency, for which Dell VxRail is designed for 99.9999%[3] hardware availability, customers experience more uptime for their workloads.

In the event of a business interruption due to a security breach, VxRail has validated integration with a multitude of disaster recovery options, from zero-latency, continuously available solutions, such as a stretched cluster architecture, to Archival cold-storage with Dell's Data Protection portfolio. By providing diverse disaster recovery options, at differing recovery latencies and expense levels, VxRail can be a valued partner in your business' risk management plan.

VMware vCenter Server

vCenter Server provides management for VxRail, server virtualization, and vSAN storage. A single vCenter instance can scale to enterprise levels, supporting hundreds of VxRail nodes and thousands of VM. VxRail can either use an instance of vCenter that is

[3] Based on Dell Technologies analysis of VxRail 660F a) in 2- to 4-node clusters configured with N + 1 redundancy, and b) in 4- to 16-node clusters configured with N + 2 redundancy.

deployed within VxRail cluster or use an existing vCenter instance. For more information, see the Dell VxRail vCenter Server Planning Guide.

vCenter provides a logical hierarchy of data centers, clusters, and hosts. This hierarchy facilitates segmenting resources by use case or lines of business and allows resources to move dynamically as needed. This is all done from a single intuitive interface.

vCenter Server provides VM and resource services, such as inventory service, task scheduling, statistics logging, alarm and event management, and VM provisioning and configuration. vCenter Server also provides advanced availability features, including:

- **vSphere vMotion**: Enables live VM workload migration with zero downtime
- **vSphere Distributed Resource Scheduler (DRS)**: Continuously balances and optimizes VM compute resource allocation across nodes in the cluster
- **vSphere High Availability (HA):** Provides VM failover and restart capabilities

VxRail with vSphere availability features

VxRail leverages the integrated vSphere availability features, including vSphere High Availability (HA), vSphere Distributed Resource Scheduler (DRS), and vSAN stretched clusters. These capabilities support VxRail automated software and provide continuous availability of services that are hosted on VxRail. Therefore, it is recommended that customers use versions of vSphere that include these availability features to reduce the potential need for recovery.

vSphere HA monitors running VMs in a VxRail cluster. If a VM or node fails, HA restarts the VM on another node elsewhere in the cluster. A VM can fail for several reasons, including a cyberattack, underlying hardware failure, or corrupted software. Although VMware HA does not prevent outages, it minimizes the time it takes to restore services.

vSphere DRS spreads the workload of VMs across all the nodes in the cluster. As VM resource demands change, DRS can migrate VM workloads using vSphere vMotion to another node in the cluster, so that the changing workload is more evenly balanced, and no single node is over burdened. Cyberattacks can cause resource issues for VMs not targeted by the attack. Cyberattacks often cause heavy resource utilization by the VM being attacked. Therefore, heavy utilization of resources at the host level impacts the resources available for other VMs on that host. DRS protects VMs by migrating them away from resource-constrained hosts, enabling the VMs to continue to provide services.

vSAN stretched cluster extends a VxRail cluster across two sites for a higher level of availability. Only a single instance of a VM exists. However, full copies of its data are maintained at both sites. If the current site that the VM is running on becomes unavailable, the VM will be restarted at the other site.

Data protection

Strong security defenses are critical, but a robust and trusted recovery plan is equally important. Backup and replications are the cornerstones of recovery after a breach. In order to aid in recovery, HCI System Software includes file-based backup and restore. All VxRail models incorporate a starter pack for Dell RecoverPoint for VM (RecoverPoint for Virtual Machines), which provides best-in-class local and remote replication and granular recovery.

HCI System Software file-based backup and restore protects against the accidental deletion of or the internal corruption of the virtual machine. Backups can be configured to occur regularly or on an as-needed basis. This is an all-inclusive feature that backs up files inside the vSAN datastore, so additional hardware and software are not required.

With RecoverPoint for Virtual Machines, if, for example, a VM is compromised or data is damaged or ransomed, the VM and dataset quickly roll back to the point in time prior to the attack, allowing the business to quickly recover. Installed directly from VxRail Manager, RecoverPoint for Virtual Machines is deployed, and day-to-day monitoring occurs through the familiar vCenter plug-in. Recovery is easy and performed using the vSphere interface.

For organizations that require enhanced, comprehensive data protection capabilities, VxRail supports options including Dell Data Protection Suite for VMware, Dell PowerProtect, and Dell Data Domain Virtual Edition.

Lastly, VxRail provides file-based backups of VxRail HCI System Software help ensure business continuity in the rare event VxRail VM has to be rebuilt.

vSAN secure disk wipe

vSAN Secure disk wipe is a feature to securely retire or re-purposing the disks that are used in a vSAN environment. The secure disk wipe feature is based on NIST standards. Drives must be decommissioned from the vSAN disk group to use this feature. This will work on a single or multiple disks simultaneously, but magnetic disks are not supported (flash and NVMe only).

VM Snapshots

VM snapshots are used to create a point-in-time copy of a virtual disk to provide a quick rollback at the virtual machine level. VM snapshots are used for both the creation and recovery from backups. The recovery process would roll back the data to some point-in-time based on the snapshots configured. Snapshots can also be used by backup software to allow point time backups without interrupting the normal operation of the VM. Snapshot should not be considered a complete backup solution but rather a tool that is used as part of disaster recovery strategies.

For further information about using snapshots in vSphere environments, see Using Snapshots to Manage Virtual Machines.

VxRail: Compatible standards and certifications

VxRail is a robust and flexible hyperconverged infrastructure that can be configured to enable organizations to satisfy compliance regulations. While some HCI vendors may claim compatibility, Dell is pursuing full certification for the security standards that are important to our customers. Contact your Dell representative to discuss how VxRail meets even the most stringent business and regulatory requirements. The following list describes a few of the standards and certifications that apply to VxRail:

FIPS 140-2 Data-at-Rest Encryption: The Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) establishes requirements and standards for the hardware and software components of cryptography modules. FIPS 140-2 is required by the U.S. government and other regulated industries, such as financial and health care

institutions that collect, store, transfer, share, and disseminate sensitive but unclassified information

Common Criteria EAL 2+: Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for system security certification. Common Criteria evaluations are performed on system security products and systems to evaluate the system's security features and provide a confidence level for the product's security features through Security Assurance Requirements (SARs) or Evaluation Assurance Level (EALs). Common Criteria Certification cannot guarantee security, but it can ensure that claims about security attributes are independently verified. PowerEdge servers and vSphere components that are used by VxRail currently hold a full certification.

NIST Cybersecurity Framework: The NIST Framework for Improving Critical Infrastructure is a voluntary guideline that is developed to help organizations improve the cybersecurity, risk management, and resilience of their systems. NIST conferred with a broad range of partners from government, industry, and academia for over a year to build a consensus-based set of sound guidelines and practices. Special Publication 800-131A presents recommendations for encryption key length. (See more information in following sections.)

DISA-STIG: The U.S. Department of Defense (DOD), Defense Information Systems Agency (DISA), develops configuration standards known as Security Technical Implementation Guides (STIGS) as one of the ways to maintain the security of DOD IT infrastructure. These guides provide technical guidance to lock down information systems and/or software that might otherwise be vulnerable to an attack. Dell offers manual and automated steps for configuring VxRail to comply with DoD Information Network (DISA) STIG requirements.

Commercial National Security Algorithm Suite (CNSA): Previously known as Suite B, The Commercial National Security Algorithm Suite (CNSA Suite) will provide new algorithms for those customers who are looking for mitigations to perform, replacing the current Suite B algorithms. The current versions of ESXi and vCenter used with VxRail support CNSA.

Section 508 VPAT: The United States Access Board Section 508 Standards apply to electronic, and information technology procured by the federal government and defines access requirements for people with physical, sensory, or cognitive disabilities. Both the PowerEdge Server and vSphere software components used by VxRail comply with section 508 VPAT.

Trade Adjustment Assistance (TAA): The Trade Adjustment Assistance Program is a federal program that provides a path for employment growth and opportunity through aid to U.S. workers who have lost their jobs due to foreign trade. When sold as a system, VxRail is TAA compliant.

IPv6: IPv6 is the next generation protocol used by the Internet. In addition to resolving the addressing limitations of IPv4, IPv6 has several security benefits, and many environments are moving toward adopting IPv6. VxRail passed USGv6 interoperability testing for IPv6 in dual stack mode and the higher standard for IPv6 Ready testing.

NIST Cybersecurity Framework and VxRail

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of system security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. This voluntary framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps promote the protection and resilience of critical infrastructure. VxRail provides capabilities that align to the NIST framework, although a complete framework would require a customer's organizational input into certain areas, such as Reponse communications.

The NIST CSF core material is organized into five functions, which are subdivided into the categories that are shown in the following figure:

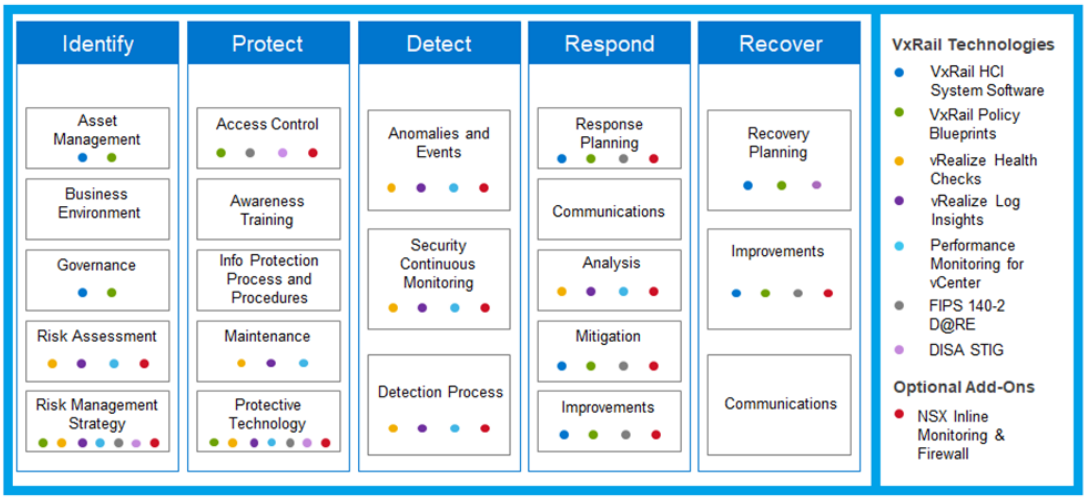


Figure 8. National Institute of Standards and Technology, Cybersecurity Framework

See the NIST website for more information about the NIST CSF.

Conclusion

Security transformation begins with a secure IT infrastructure. VxRail provides a secure, modern infrastructure from the Core to Edge to the Cloud. A hyperconverged infrastructure, VxRail is designed, engineered, built, and managed as a single product to reduce the possible attack surface by reducing the number of components that are involved in the infrastructure. VxRail software lifecycle management bundles may include updates to BIOS, firmware, hypervisor, vSphere, or any of the included management components that make updating the complete software stack much simpler, and that reduce the vulnerability to attacks.

Fully protecting an environment from today's threats requires "defense in-depth" with multiple layers of security. The networks connecting the applications and services that run on VxRail to the users that consume them must be protected, and the applications and services themselves must be secured. Firewalls, intrusion detection and prevention systems, antivirus/malware, endpoint protection, as well as security operations and management are all part of a multilayer defense.

Dell Technologies understands security and has experts worldwide who can help you assess your environment and design a security plan to meet your unique requirements. Contact your Dell Technologies representative for more information.

References

Dell Technologies documentation

The following documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

CloudIQ Security Paper

Cyber Resilient Security in 14th generation of Dell PowerEdge servers

Dell CloudIQ: A Detailed Review

Dell Technologies MyService360 overview

Dell Technologies Product Security practices

Dell Security and Trust Center

Dell Vulnerability Response Policy

Dell VxRail Network Guide

Dell VxRail System Tech Book

Secure Development at Dell

Security Features of the integrated Dell Remote Access Controller (iDRAC)

Secure Connect Gateway security white paper

VMware documentation

The following VMware documentation provides additional helpful information:

List of compatible key management servers

VMware Compatibility Guide

VMware Cloud Foundation on VxRail Architecture Guide

VMware FIPS Certifications

VMware Product Security

Verizon Report on Incident Classification Patterns

Using Snapshots to Manage Virtual Machines

VMware blog vSAN 7 Update 1 data-in-transit encryption and Secure Disk Wipe

VMware Key Management

VMware NSX-T

VMware vSAN

VMware vRealize Log Insight

VMware Secure Development Lifecycle

VMware's Using SpoofGuard guide

vSphere 6.7 and 7.0 Security Guides

Additional documentation

The following documentation provides additional and relevant information:

CloudIQ web portal

NIST Cyber Security Framework

Video links

The following YouTube videos provide additional and relevant information:

VxRail Security Hardening and Compliance

VxRail Security Overview