ABSTRACT

VxRail™ Appliance, the ideal platform for IT infrastructure and security transformation, provides layers of protection to keep your data and business applications secure. Only the Dell Technologies family of companies can provide the full end-to-end solutions required to keep up with today’s evolving threat landscape. This guide covers both integrated and optional security features, best practices, and proven techniques for securing your VxRail.

April 2018
TABLE OF CONTENTS

INTRODUCTION .......................................................................................................................... 4

THE CURRENT STATE OF SECURITY ......................................................................................... 4

SECURITY TRANSFORMATION BEGINS WITH DELL TECHNOLOGIES .............................. 5

BUILDING TRUST WITH DELL EMC PRODUCT SECURITY PROGRAMS ....................... 6
  Secure Development LifeCycle (SDL) ...................................................................................... 7
  Secure Development ............................................................................................................. 8
  Dell EMC Vulnerability Response ....................................................................................... 8
  Supply Chain Risk Management ......................................................................................... 9
  Industry Collaboration to Improve Product Security .............................................................. 9
  Participation in Industry Product Security Groups ............................................................. 9

VXRAIL: RESILIENT, SECURE, MODERN INFRASTRUCTURE ........................................ 10
  Intel® Trusted Infrastructure Platform .................................................................................. 10
  Dell EMC PowerEdge Servers ............................................................................................. 11
  VMware vSphere ................................................................................................................ 12
  VMware vCenter Server ..................................................................................................... 12
  VMware ESXI Hypervisor .................................................................................................... 13
  VMware virtual Networking ............................................................................................... 13
  VMware vSAN .................................................................................................................... 13
    Storage Policy Based Management (SPBM) .................................................................. 14
  Dell EMC VxRail Manager ................................................................................................ 14
  VMware vRealize Log Insight ......................................................................................... 15

VXRAIL SECURITY MANAGEMENT ...................................................................................... 15
  Confidentiality ................................................................................................................... 15
    VxRail Encryption ......................................................................................................... 15
    Network Segmentation .................................................................................................. 16
    VxRail Software Defined Networking Using the Optional NSX-V .................................. 17
  Lockdown Mode ................................................................................................................ 18
  Secure Management with HTTPS ..................................................................................... 18
  Integrity .............................................................................................................................. 18
INTRODUCTION

Across all industries and the public sector, 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 that need to be protected are expanding at an exponential rate. Digital transformation is changing everything from online services such as banking and retail, to real-time results from medical devices and online voter registration.

Traditional enterprises are under more pressure than ever to modernize their IT infrastructure. As application ecosystems become more complex, traditional enterprises must transform IT to deliver greater efficiency, predictability, and business agility. The Dell EMC VxRail™ Appliance, the only fully integrated, preconfigured, and pretested VMware hyper-converged family of appliances on the market, is built for the modern IT infrastructure. VxRail is jointly engineered with VMware, delivered as a single product and supported by Dell EMC. This hyper-converged platform is simple to manage and allows organizations to start small and scale out. Combined with Dell EMC PowerEdge server options, VxRail offers configuration choices to meet any use case.

Not only does Dell EMC VxRail provide clear benefits for the modern infrastructure, it is designed and built for enterprise-class security. Ask any CIO or IT manager, and security will top their list of concerns. Safeguarding a company’s data has long been a primary focus of IT organizations, but today that information security has become a boardroom issue. Traditional data protection techniques are no longer adequate and must be adapted to address deep and evolving threats. An adaptable and unified approach is required, and Dell Technologies is uniquely positioned to work with our customers to help them transform their IT infrastructure and security operations so they can transform their business and realize their digital future.

THE CURRENT STATE OF SECURITY

The reality is IT organizations need to do more to secure their data from security threats. The number of security breaches are escalating as people and things become more connected and IT environments become more distributed.

Organizations must continue to protect themselves against traditional threats such as malware, phishing, and network attacks while defending against new, more advanced, persistent, and targeted threats such as:

- Criminals who specifically target personal, health, and payment information for financial gain, hold data for ransom, and/or to damage the reputation of an organization
- State sponsored cyber-terrorism who disrupt critical IT and public infrastructure and attempt to interfere with the democratic process
- Unscrupulous organizations attempting to gain advantage by stealing data analytics, proprietary designs, formulas, and digital works

These types of attacks are different from traditional threats in that they are targeted and well planned. Often criminals spend months or even years doing reconnaissance, scanning for vulnerabilities, planning an attack, and then tunneling in and out of an organization’s network undetected. Often, they operate in foreign countries, beyond the reach of law, and if caught, there are few repercussions. As a result, criminals thrive and companies are sometimes breached multiple times by the same criminals.

Today’s evolving threat landscape requires a shift in the approach to prevent or mitigate these threats. Outdated infrastructure is difficult to defend, and point products from multiple vendors add complexity and increase the risk of vulnerabilities that can be exploited. Some enterprise customers have reported having as many as 60 to 90 vendors as part of their security program. That level of complexity offers multiple points of entry for would-be wrong-doers.

While a layered defense with multiple levels of security is required, these elements all must work in concert. Security transformation begins with a defendable, modern infrastructure such as the VxRail Appliance that has been designed and built with security in mind. Because of VxRail’s simplicity and security by design approach, VxRail is able to reduce complexity by reducing the need for multivendor add-on products.

According to Risk Based Security, a security analytics company, 5,207 publicly-disclosed data compromise events were reported in 2017, with over 7.8 billion records exposed. Breaches often go unreported for months, causing...
widespread impact. As a result, governing bodies around the world are driving more accountability for data protection and privacy by implementing sweeping regulations. A few of the recent mandates driven by security and privacy concerns include:

- Payment Card Industry Data Security Standard (DSS) – protections for credit card holders
- General Data Protection Regulation (GDPR) – a European Union data privacy regulation
- The German Bundesdatenschutzgesetz (BDSG) – German federal government data protection act
- Sarbanes-Oxley Act (SOX) – Protection of sensitive data related to financial reporting in public companies
- Gramm-Leach-Bliley Act (GLBA) – Protection of nonpublic personal information (NPPI) in the financial services industry
- Health Insurance Portability & Accountability Act (HIPAA) – Protection of electronic patient healthcare data and information

There are often significant legal and financial penalties for non-compliance, and while costly, those penalties may have less impact on a business than a breach may have on the company’s reputation; people are less likely to do business with a company that has been breached.

SECURITY TRANSFORMATION BEGINS WITH DELL TECHNOLOGIES

On top of the resilient, secure, and modern infrastructure provided by VxRail lie advanced security operations that adapt to ever-evolving threats. RSA incident response software and SecureWorks advanced services provide converged visibility and understanding of what is going on in real-time across physical and virtual networks. Threat intelligence and advanced analytics incorporate real-time threat feeds and analysis to help identify threats and make faster, more effective decisions. Rapid response and remediation leverage automated action and response decision support for faster containment across the entire attack surface. Figure 1 below illustrates the Dell Technologies approach to IT and security transformation.

Figure 1: Dell Technologies’ Approach to IT and Security Transformation
RSA Archer provides unified business risk management to help organizations understand which risks are worth taking. Understanding the risks that exist and proactively contextualizing them helps businesses prioritize the most critical actions. Risk management mitigates the financial, operational, and reputational impacts of a cyber-attack in real-time.

BUILDING TRUST WITH DELL EMC PRODUCT SECURITY PROGRAMS

Dell EMC began formulating its product security policies in 2002 when the company’s focus shifted from being primarily a storage hardware vendor to an enterprise-class software provider. The company rolled out its vulnerability response program in 2004 and established a company-wide Product Security Policy in 2005. The policy enacts broad but clear security standards encompassing the complete range of Dell EMC products. This policy was continuously updated, and in 2007, it was integrated into the company’s new Security Development Lifecycle (SDL). SDL instilled a series of measurable and repeatable security practices into every step of product development and deployment. Figure 2 below shows the evolution of Dell EMC’s product security policies.

Dell EMC continues to regularly update its Product Security Policy and Security Development Lifecycle practices. In 2012, the company also formalized a supply chain risk management program to extend security practices to Dell EMC’s suppliers of product components.

With the VxRail Appliance, Dell EMC continues its commitment to security. VxRail’s development lifecycle follows the Dell Secure product development process and Security Development Lifecycle overlay. The Dell EMC Security Development Lifecycle follows a rigorous approach to secure product development and involves executive-level risk management before products are shipped to market. Additionally, VMware vSphere—a significant part of VxRail hyper-converged infrastructure—has also been developed using a similar Security Development Lifecycle.
SECURE DEVELOPMENT LIFECYCLE (SDL)

The Dell EMC Security Development Lifecycle (SDL) outlines the set of activities required throughout the product lifecycle to build security resiliency and consistent security capabilities into the products and to promptly respond to externally reported security vulnerabilities. Aligned with industry best practices, the Dell EMC SDL is based on a set of controls that are implemented by the product R&D organizations. Figure 3 shows some of the typical activities performed as part of the SDL.

![Dell EMC SDL Activities](image)

*Figure 3: Dell EMC SDL Activities*

The implementation and validation of these controls is driven by security champions within the product R&D organizations who work in close collaboration with the Product Security Office (PSO) security advisors. Figure 4 illustrates how this SDL maps onto a typical Agile lifecycle.

![SDL and a Typical Agile Lifecycle](image)

*Figure 4: SDL and a Typical Agile Lifecycle*
The scorecard is a mechanism used throughout Dell EMC’s business to capture the security posture of a product/solution when it reaches its release Directed Availability/General Availability (DA/GA) date.

SECURE DEVELOPMENT
Dell EMC’s comprehensive approach to secure development focuses on minimizing the risk of vulnerabilities in our products. This comprehensive approach to secure software development goes across policy, people, processes, and technology and includes the following:

- The Dell EMC internal product security standard is the Dell EMC product security policy, which is a common reference for Dell EMC product organizations to benchmark product security against market expectations and industry best practices.
- Dell EMC engineering teams are a security-aware engineering community. All engineers attend a role-based security engineering program to train on job-specific security best practices and how to use relevant resources. Dell EMC strives to create a security-aware culture across its entire engineering community.
- Dell EMC development process is secure and repeatable. SDL overlays standard development processes to achieve a high degree of compliance with the Dell EMC product security policy.
- Dell EMC development teams build on the best-in-class security technologies. Dell EMC has developed a set of software, standards, specifications, and designs for common software security elements such as authentication, authorization, audit and accountability, cryptography, and key management using state-of-the-art RSA technology. Where appropriate, open interfaces are used, allowing integration with customers’ existing security architectures.
- Dell EMC’s Security Development Lifecycle overlays security on standard development processes to achieve a high degree of compliance with the Dell EMC product security policy. The Dell EMC Security Development Lifecycle follows a rigorous approach to secure product development that involves executive-level risk management before our products are shipped to market.
- The SDL is part of a wider set of processes that exist within the secure design standard. The secure design standard is the standard for building security into the design and architecture of Dell EMC products. The standard relates to the security of all product functionality and describes mandatory security functionality, which must be built into any product delivered by Dell EMC to customers. This standard enables EMC products to:
  - Meet demanding customer security requirements,
  - Help customers meet regulatory requirements such as PCI or FISMA, etc.,
  - Minimize the risks of Dell EMC products and customer environments from security vulnerabilities.
- Source code protection identifies how to properly protect Dell EMC engineering systems that contain product source code to product-related intellectual property and ensure the integrity of products deployed to customer environments.

DELL EMC VULNERABILITY RESPONSE
Security vulnerabilities in any system component can be used by attackers to infiltrate and compromise the entire IT infrastructure. The time between the initial discovery of vulnerabilities and the availability of a fix becomes a race between the attackers and the defenders. A top priority for Dell EMC is to shorten this time gap to reduce risk.

The Dell EMC Product Security Response Center (PSRC) is responsible for coordinating the response and disclosure for all externally identified Dell EMC product vulnerabilities. The PSRC provides customers with timely information, guidance, and mitigation strategies to address threats from vulnerabilities.

Anyone can notify Dell EMC of potential security flaws in its products through the company’s website or by email. Every notice is investigated, validated, remediated, and reported according to industry guidelines.
Dell EMC releases information about product vulnerabilities to all customers simultaneously. The company’s advisories identify the severity of vulnerabilities and spread the information using multiple standardized reporting systems. Like the rest of our product security practices, Dell EMC’s disclosure policy is based on industry best practices.

**SUPPLY CHAIN RISK MANAGEMENT**
Successful product security programs are comprehensive and extend to outsourced components and software. Integrity tests within the supply chain are an essential component of building and preserving trust. Dell EMC has a formal Supply Chain Risk Management program that ensures the hardware components used in the company’s products originate from properly vetted sources.

The company’s Security Development Lifecycle extends to all types of software, including assessing the security practices of firmware suppliers. Dell EMC’s product return procedures include erasing disks that may have once held customer data.

**INDUSTRY COLLABORATION TO IMPROVE PRODUCT SECURITY**
Dell EMC believes a collaborative approach is the most efficient and effective way to deal with security threats that constantly emerge and can quickly spread among organizations through today’s densely interconnected systems.

Considering the heightened risks, technology providers must set aside their competing aims in the marketplace when it comes to product security. No single vendor can solve all IT product security problems by itself. IT security is a collective, collaborative endeavor. Dell EMC believes collaborating with other companies is essential to ensuring that the marketplace remains a venue where everyone can flourish.

Having spent decades in product security has helped Dell EMC establish a rich history of successful improvements and insights, and the company openly shares what it has learned with its customers, peers, and partners. Dell EMC understands a customer’s IT system doesn’t run solely on Dell EMC products, so we’re committed to improving the security of the ecosystem wherever a product operates. That means being an active participant and positive contributor throughout the industry.

Dell EMC’s long commitment to advancing product security has created a sense of obligation to assist and promote newer industry members. The company’s product security leaders facilitate the open exchange of ideas at conferences, through blog posts, and in other social and formal venues.

**PARTICIPATION IN INDUSTRY PRODUCT SECURITY GROUPS**
Dell EMC is active in product security groups, where it both learns and teaches progressive best practices and cultivates a sense of communal responsibility for product security. Dell EMC’s industry affiliations include:

- **BSIMM** – The Building Security in Maturity Model evaluates the industry’s software security initiatives, so organizations can see where their security efforts stand and how they should evolve. Dell EMC is one of only 11 firms worldwide that has contributed to BSIMM studies twice.

- **The Open Group** – This 400-member consortium runs respected certification programs for IT personnel, products, and services to design and improve IT standards. The Open Group works to understand current and emerging IT requirements and establish or share best practices to meet them.

- **SAFECode** – The Software Assurance Forum for Excellence in Code, co-founded by Dell EMC, is an industry-led effort to identify and promote best practices for delivering more secure and reliable software, hardware, and services. Reference the SAFECode guide [Fundamental Practices for Secure Software Development](#) for more information on the Essential Elements of a Secure Development Lifecycle Program.
CSA – The Cloud Security Alliance is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. Dell EMC is an Executive Member of the Cloud Security Alliance.

FIRST – The Forum of Incident Response and Security Teams is a recognized global leader in incident response. Dell EMC is a FIRST team member.

VXRAIL: RESILIENT, SECURE, MODERN INFRASTRUCTURE

Dell EMC VxRail Appliance is a resilient, secure, and modern hyper-converged infrastructure system. With flexible configuration options, it is capable of securely hosting the most demanding workloads and datasets. Still, like any device attached to the network, VxRail is a potential target. However, because the VxRail Appliance is engineered, built, configured, and maintained following the Dell EMC Secure Development Lifecycle, it effectively defends against cyber-attacks to help ensure business continuance.

To win the race against the continually evolving security threat landscape, VxRail is built to adapt. Jointly developed with VMware, VxRail has the adaptability to defend against current and future threats. VxRail is built on the current generation of Dell PowerEdge servers and the latest Intel® Xeon® Scalable Processors that provides a secure platform and flexible configuration options. vSphere provides storage and server virtualization. As workload requirements grow, VxRail easily scales. As regulations change, VxRail flexible configuration options enable it to quickly adapt.

INTEL® TRUSTED INFRASTRUCTURE PLATFORM

The current generation of VxRail Appliances are built on the 14th generation of Dell EMC PowerEdge servers, powered by the latest Intel® Xeon® Scalable Processors. With Intel, building security technologies into the platform is a priority and is driving generational improvements to make the platforms more secure and suitable for hosting increasingly sensitive and regulated workloads. Integrating security into the platform itself lowers cost and complexity, offers efficiency and usability benefits, and complements traditional security solutions. Every generation of Intel platform delivers functionality that further increases the ability to protect infrastructure in the face of growing threats and regulation.

Security begins with a foundation of trust built on top of a secure platform. Without trust in the platform, anything upstream cannot be trusted. Intel-innovated technologies protect the platform from power-on through the stack of hypervisor, VMs, OS, and applications.

Most breaches are after an organization’s most valuable asset—its data. Therefore, protecting data is vital to protecting the enterprise—wherever that data resides and at any stage in its lifecycle. But protecting should not compromise productivity and performance. Many companies are reluctant to introduce critical capabilities for protection because it slows down the business. But with Intel technologies built right into the silicon, it runs faster than software and it presents a much smaller attack surface than software-based security technologies. Figure 5 below illustrates Intel’s ongoing commitment to data center security.
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. Differentiated security features in PowerEdge servers include:

- **System lockdown to prevent 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 SecureBoot, BIOS Recovery capabilities, and signed firmware provides enhanced protection against attacks.**

- **The server level System Erase feature ensures privacy by quickly and securely erasing all user data from drive and all non-volatile memory when a server is retired.**

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

PowerEdge servers have an integrated remote access controller referred to as 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 on the **Cyber Resilient Security in 14th Generation of Dell EMC PowerEdge**, see Dell EMC’s recently published technical whitepaper.)

PowerEdge servers use cryptographically signed and verified firmware to build a system of trust. Capabilities like Intel’s Trusted Execution Technology (TXT), verify that the server executes only the intended version of firmware, BIOS, and hypervisor while preventing the undetected introduction of malware. Figure 6 below illustrates the 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 cryptoprocessors, a dedicated microcontroller that is designed to provide high security for cryptography keys and an option for all VxRail nodes.

**VMWARE VSPHERE**

The VMware vSphere 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 installed on a physical VxRail server node in the factory that enables a single physical server to host multiple logical servers or virtual machines (VMs). vSAN is the software-defined storage used by the VMs, and VMware vCenter Server is the management application for ESXi hosts, vSAN, and VMs.

Like Dell EMC, VMware follows a rigorous Secure Software Development Lifecycle process and Security Response Center. VxRail is jointly developed and supported with VMware ensuring all components included in the solution are designed, built, tested, and deployed with security as a top priority. (For more information on VMware Product Security, reference the link to the whitepaper in Appendix A.)

**VMWARE VCENTER SERVER**

vCenter Server is the primary point of management for both server virtualization and vSAN storage. A single vCenter instance can scale to enterprise levels, supporting hundreds of VxRail nodes and thousands of virtual machines. VxRail can either use an instance of vCenter that is deployed with VxRail, or use an existing vCenter instance.

vCenter provides a logical hierarchy of datacenters, 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 virtual machine (VM) failover and restart capabilities

VMWARE ESXi HYPervisor
In VxRail, the ESXi hypervisor hosts the virtual machines (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. In addition, ESXi assigns VMs a region of usable memory and provides shared access to the physical network cards and disk controllers associated with the physical host. All X86-based operating systems are supported and virtual machines on the same physical server hardware can run different operating systems and applications.

VMWARE VIRTUAL NETWORKING
A fundamental security requirement is to isolate network traffic. On VxRail, vSphere’s virtual networking capabilities provide flexible connectivity and isolations. VxRail VMs communicate with each other using the VMware Virtual Distributed Switch (VDS), which functions as a single, logical switch that spans multiple nodes in the same cluster. VDS uses standard network protocols and VLAN implementations, and it forwards frames at the data-link layer.

VDS is configured in vCenter Server at the datacenter level, maintaining a secure and consistent network configuration as VMs migrate across multiple hosts. The VxRail Appliance relies on VDS for appliance traffic, and vSAN relies on VDS for its storage-virtualization capabilities.

Optionally, the VxRail can be configured with NSX to provide software defined network security and finer level access control using micro-segmentation.

VMWARE VSAN
VxRail Appliances are powered by VMware vSAN for enterprise-class software-defined storage. vSAN aggregates the locally attached disks of hosts in a vSphere cluster to create a pool of distributed shared storage. Capacity is scaled up by adding additional disks to the cluster and scaled out by adding additional VxRail nodes. vSAN is fully integrated with vSphere, and it works seamlessly with other vSphere features.

vSAN is notable for its efficiency and performance. vSAN is self-optimizing and balances allocation based on workload, utilization, and resource availability. vSAN delivers a high performance, flash-optimized, resilient hyper-converged infrastructure suitable for a variety of workloads. Enterprise-class storage features include:

• Efficient data-reduction technology, including deduplication and compression as well as erasure coding

• QoS policies to control workload consumption based on user-defined limits

• Data-integrity and data-protection technology, including software checksums and fault domains

• Enhanced security with native vSAN data-at-rest-encryption

With vSAN, VxRail disks on each node are automatically organized into disk groups with a single Solid State Drive (and one or more capacity drives). These disk groups are used to form a single vSAN Datastore, which is visible across the VxRail cluster.

VxRail provides two different vSAN node-storage configuration options: a hybrid configuration that uses both flash SSDs and mechanical HDDs, and an all-flash SSD configuration. The hybrid configuration uses flash SSDs for caching and mechanical HDDs for capacity and persistent data storage. The all-flash configuration uses flash SSDs for both the caching and capacity. Figure 7 illustrates the basic concepts of vSAN.
vSAN is configured when the VxRail cluster is first initialized and is managed through vCenter. During the VxRail Appliance initialization process, vSAN creates a distributed shared datastore from the locally attached disks on each ESXi node. The amount of storage in the datastore is an aggregate of all the capacity drives in the cluster. The orchestrated vSAN configuration and verification performed as part of system initialization ensures consistent and predictable performance and a system configuration that follows best practices.

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 requirement 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.

DELL EMC VXRAIL MANAGER

vSphere vCenter web client is used for day-to-day operations of the VxRail. VxRail Manager is used for cluster (system) lifecycle management and serviceability of the clusters. VxRail Manager is used to initially configure the cluster, monitor hardware components, perform graceful cluster shutdown, expand the cluster by adding nodes, and update software. Through this interface, administrators can work with the Dell EMC support organization, view community posts, and see recent service-related articles. With its intuitive user interface, VxRail manager reduces complexity, and automation reduces risk and ensures the cluster is configured and securely maintained following best practices.

Figure 7: The Basic Concepts of vSAN
VMWARE VREALIZE LOG INSIGHT

Bundled with VxRail, VMware vRealize Log Insight monitors system events and provides ongoing holistic notifications about the state of the virtual environment and appliance hardware. vRealize Log Insight delivers real-time automated log management for the VxRail Appliance 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 secure infrastructure. For customers who already have a logging facility or a SIEM, VxRail easily integrates using the industry standard syslog protocol.

VXRAIL SECURITY MANAGEMENT

Secure system configuration and management of the VxRail follow the principals of the Confidentiality-Integrity-Availability (CIA) triad.

CONFIDENTIALITY

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 confidentiality of data in use, data in motion, and data at rest several different ways.

VXRAIL ENCRYPTION

Encryption protects the confidentiality of information by encoding it to make it unintelligible to unauthorized recipients. With VxRail, data on the datastore can be encrypted using native vSAN encryption, individual VMs can be encrypted using vSphere Encryption, and VMs in motion can be encrypted using vMotion encryption. Additional levels of encryption may be configured based on the application requirements.

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. Normally, encrypted data does not benefit from space-reduction techniques such as deduplication or compression. But with vSAN, encryption is performed after deduplication and compression, so it takes full advantage of these space reduction techniques.

VM Encryption provides the flexibility to enable encryption on a per-VM basis, which means a single cluster may have encrypted and non-encrypted VMs. VM Encryption follows the VM wherever it is hosted. So even if the VM was moved to a datastore outside the VxRail, it would remain encrypted. In addition, because data is encrypted at the VM layer, it remains encrypted when data is transported over the network as part of a vMotion migration. While VM encryption will work with vSAN deduplication and compression, there’s unlikely to be any space-saving benefit because the data is encrypted before it gets to vSAN. Figure 8 below summarizes the difference between VM encryption and vSAN encryption.
In addition, VxRail supports encrypted vMotion where VMs are encrypted when they are moved between hosts. This includes vMotion migrations within a VxRail as well as vMotion migrations to or from a VxRail. Encrypted vMotion could be used with vSAN encryption to have both data at rest encryption and data in flight encryption.

With the exception of vMotion Encryption, 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 on 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 typically applied to other critical infrastructure components, such as DNS, NTP, and Active Directory. It’s important to remember 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 will not be able to complete the startup.

VxRail and VMware support KMSs that are compatible with the KMIP 1.1 standard such as Dell EMC CloudLink. VMware maintains a that have been validated with vSphere.

Within vSphere, encryption is handled by a common set of modules that are FIPS 140-2 validated. 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 role named “No Cryptography Administrator,” allows an administrator to do normal administrative tasks without authority to alter encryption settings.

**NETWORK SEGMENTATION**

Network segmentation is used to isolate private network traffic from public traffic in order to reduce the attack surface. It is also an effective security control for limiting the movement of an attacker across networks.

VxRail is engineered with multiple levels of network segmentation, including physical segmentation of the hardware management network, virtual segmentation of application and infrastructure networks, and micro-segmentation at
the VM and application level with the optional NSX software from VMware. Through segmentation, the visibility of critical administrative tools is limited, preventing attackers from using them against a system. By default, appropriate network segmentation is automatically configured as part of the system initialization and the administrator has the flexibility to define additional levels of segmentation as required for the application environment. Best practices for network configuration are presented in Dell EMC VxRail Network Guide.

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 are configured by default with vSphere Network I/O Control (NIOC). NIOC allows physical bandwidth to be allocated for different VLANs. Some cyber-attacks, such as denial of service and worms, can lead to 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 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 EMC VxRail 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. In the event of a distributed denial of service attack, the physically segmented network will not be affected, limiting the scope of a potential attack.

**VXRAIL SOFTWARE DEFINED NETWORKING USING THE OPTIONAL NSX-V**

Dynamic virtual environment such as VxRail often benefit from the flexibility that Software Defined Network (SDN) services provide. The easiest ways to provide SDN on VxRail is with VMware NSX-V (NSX for vSphere), which is an optional software and not included with VxRail. NSX-V is a complete network virtualization and security platform that allows administrators to create entire virtual networks, including routers, firewalls, and load balancers. Because this software-defined network is decoupled from the underlying physical network infrastructure, it's not dependent on VxRail being attached to a particular switch vendor.

NSX-V with VxRail is an integrated security solution that reduces the need to deploy additional security hardware or software components. With NSX-V, VxRail administrators configure micro-segmentation to secure and isolate different tenant workloads, control ingress and egress, and provide enhanced security for all workloads including traditional multi-tier applications and general purpose virtual machine, as well as VDI environments. A few of the benefits of using NSX-V with VxRail include:

- The ability to apply security policies closest to the workload. Security policies are applied in software and the security controls move with the workload between hosts in the cluster.

- Simplified management with security is integrated with the vSphere stack and managed centrally through vSphere Web Client and NSX Manager plug-in.

- Consistent and automatic security controls using groups and policy. Workloads are automatically identified and dynamically placed within the correct security posture.

- Efficient implementation of security controls at the hypervisor level reduces application latency and bandwidth consumption when compared to external or perimeter-based security controls.

- DMZ-level isolation to control ingress and egress for both internal and external clients from the Internet using appropriate allow-and-deny rules to control traffic.

- Detection and blocking of spoofed virtual machine IP addresses using the SpoofGuard feature. (For more information on this capability reference VMware’s Using SpoofGuard documentation.)
• Identity Firewall that allows an NSX administrator to create Active Directory user-based DFW rules. (For more information on this capability reference the VMware NSX Documentation.)

• Integrates with third party security services such as Intrusion Detection and Intrusion Prevention (IDS/IDP).

NSX-V enhances the security posture of an environment and is compliant with the following certifications and standards:

• Common Criteria certification – EAL 2+
• ICSA Labs certified firewall
• FIPS 140-2
• Satisfaction of all NIST cybersecurity recommendations for protecting virtualized workloads

By leveraging the optional VMware NSX-V platform for security with VxRail, firewall and security policies are built in. This provides a truly converged appliance as opposed to security sitting externally at the perimeter. Deploying the NSX-V with VxRail further reduces the time it takes to deploy new application initiatives as security controls become part of the appliance, rather than additional hardware or software components that are bolted on. The “Security for Hyper-Converged Solutions” whitepaper offers more details on the NSX security feature of VxRail.

LOCKDOWN MODE
For environments needing even greater security, lockdown mode can be configured for the ESXi hosts. In lockdown mode, the ability to perform management operations on individual hosts is limited, forcing management task completion to occur through vCenter. In strict lockdown mode, no users are allowed to manage the servers locally. Normal lockdown mode allows a select group of users to be white-listed, enabling them to manage the servers locally instead of through vCenter.

SECURE MANAGEMENT WITH HTTPS
Unsecured management traffic is a significant security risk. Because of that, VxRail uses management interfaces secured with Transport Layer Security (TLS.) vCenter, iDRAC, and VxRail Manager all disable the clear text HTTP interface and require the use of HTTPS, which uses TLS. In addition, access to the command line of the ESXi servers must use SSH. Using SSH and HTTPS is a vital part of secure command and control for a VxRail.

INTEGRITY
Integrity of a company’s data is a fundamental requirement of business operations. VxRail ensures the integrity of your data by maintaining the consistency, accuracy, and trustworthiness of data over its lifecycle by controlling user access and built-in integrity features such as data checksums

VXRAIL AUTHENTICATION AND AUTHORIZATION
Authenticating a user’s identity and authorizing them with the appropriate level of access is a fundamental security control and VxRail supports options that work with most all security strategies.

Organizations often centralize identity management using directory services such as Microsoft Active Directory (AD) using LDAP. If the VxRail is a standalone environment and not part of a domain, users and passwords can be managed locally in vSphere and iDRAC.

Many environments strengthen their identity management using multi-factor authentication that requires an additional level of identity verification including certificates, smartcards, or security token such as RSA SecureID in addition to a username and password. VxRail fully supports multi-factor authentication for both domain and locally managed users.
Often there may be different individuals responsible for the physical servers, the VxRail lifecycle management, and the management of the server, storage, and network virtualization environment. Therefore, VxRail uses fine-grained, role-based access controls for iDRAC, VxRail Manager, and vSphere.

Using the principle of “least privileged,” a user is granted the required rights to perform their role but no more than is needed. vSphere includes a number of 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 Manager. vSphere Administrator grants privilege to perform Administrator tasks in vCenter. In addition, vSphere allows an even finer level of access control by the creation of custom roles. For example, a privilege user may be granted the ability to acknowledge an alarm or create a storage profile but not deploy virtual machines.

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. In addition, 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.

As shown in Figure 9 below, VxRail’s flexible access control supports the security principles of “Least Privilege” and “Separation of Responsibility,” and allows the security administrator to elevate security by defining precise permissions based on the systems management structure of an organization.

**Figure 9: vSphere Role-Based Authorization**

**SECURE BOOT**
Secure boot protects the operating system from corruption and root kit attacks. Secure boot validates that the firmware, boot loader, and VMkernel are all digitally signed by a trusted authority. In addition, secure boot for ESXi validates that the VMware Install Bundles (VIBs) are cryptographically signed. This ensures that the server boot stack is running all genuine software and that it has not been changed.

**SOFTWARE CHECKSUM**
A key part of data integrity is validating that the data 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 then verified on read, and if the checksum shows that the data has 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.

**AVAILABILITY**
Keeping your IT system updated, making sure hardware is functioning correctly, and providing adequate bandwidth are all keystones for maintaining availability of a company’s data to authorized users. VxRail software lifecycle management, vSphere availability features, proactive monitoring, and built-in recovery, as well as physical security of the hardware and secure system configuration ensure maximum system availability.

**VXRAIL SOFTWARE LIFECYCLE MANAGEMENT**
One of the most critical actions an organization can take to keep its IT infrastructure secure is to keep software updates and patches current. Updates and patches don’t just fix issues that might potentially lead to downtime or improve performance, they often fix security vulnerabilities. There is tremendous collaboration within the security community. When vulnerabilities become known, information is openly shared. But not everyone is on the same side, and it becomes a race between the defenders who are working to mitigate and remediate the threat and the attackers whose goal is to exploit the vulnerability.

VxRail software lifecycle management makes what could be complex and risky update operations easy to install and safe to implement. As a hyper-converged infrastructure system, all software components are engineered, tested, and released as a bundle. VxRail software bundles may include updates to BIOS, firmware, hypervisor, vSphere, or any of the included management components. If and when vulnerabilities are discovered, fixes are quickly developed to mitigate threats regardless of where they are. Update bundles are extensively tested on the VxRail hardware platform and the entire VxRail software stack before being released to customers.

Administrators are notified through the VxRail Manager when updates are available. The administrator can then download the update bundle directly and initiate 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 before continuing.

Not only does VxRail Manager lifecycle management reduce complexity, it makes the infrastructure more secure by reducing the time it takes to patch systems and removes the risk.

**VXRAIL VSphere AVAILABILITY FEATURES**
VxRail leverages many of the built-in vSphere availability features including VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS), and stretched clusters. These capabilities support VxRail automated software and provide continuous availability of services hosted on the VxRail. Therefore, it’s recommended that customers use versions of vSphere that include these capabilities.

VMware High Availability monitors running virtual machines in a VxRail cluster. If a machine fails, HA restarts on another machine elsewhere in the cluster. A virtual machine can fail for a number of reasons, including a cyber-attack, failure of the underlying hardware, or corrupted software. Although VMware HA does not prevent outages, it minimizes the time it takes to restore services.

VMware DRS will move a virtual machine when resources become scarce on the physical node where it’s running. Many cyber-attacks cause heavy utilization of resources, not just by the VM being attacked, but also by other VMs that share the same physical resources. DRS moves virtual machines away from attacks so that they can continue to provide services.

Availability may not be the first thing generally associated with security, but it provides two vital pieces of any complete security strategy. First, keeping services running—both the services that are under attack and the other services in the cluster—can minimize the impact of a security event. Second, if a security event results in an outage, the ability to restart services and recover data that may have been lost is essential. Tools like VMware HA and DRS are important components of an availability strategy.
MONITORING
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. 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. If you don’t maintain a system of audit logs, you may not even be able to determine whether you’ve been attacked. According to the 2015 Trustwave Global Security Report, only 19% of data breaches in 2014 were detected by the victim organization.

Configuration drift is a challenge that affects all systems. Systems may start with a secure configuration baseline but over time, changes can occur that may leave the system vulnerable. These changes can happen for a variety of reasons including a temporary change while troubleshooting or an approved change that should become part of the baseline configuration. Without monitoring, those changes become very hard to detect.

The challenge with monitoring the information comes from many different sources—an individual virtual machine, 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 as well as logs for the everything 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 drill down to the root cause of the issue. Figure 10 below shows the vRealize Log Insight dashboard.

Figure 10: vRealize Log Insight

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

For organizations that already have a log management system or Security Incident and Event Management (SIEM) system, VxRail easily integrates using standard syslog protocol.

VXRAIL PHYSICAL LOCATION SECURITY
Physical security is an important part of any comprehensive security solution. Because VxRalls may be deployed outside of a traditional data center, physical security can take on even greater importance. In order to prevent
malware or infected software from being introduced via a USB drive, the USB ports on a VxRail can be disabled and then enabled only when needed.

The 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. In many cases, a chassis need not be opened after it’s put into production and tracking such activity could be an indicator of an attempt to compromise the system.

**AUTOMATION**

An important part of maintaining security is assuring that all of the relevant security configuration elements are implemented on all of the objects in an environment. A VxRail can have up to 64 physical nodes and support thousands of virtual machines. Even a simple change—if it must be configured on all the virtual machines—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 consistent configurations while increasing efficiency and reducing the time between when a decision is made and when it is implemented, increasing the time to value of those decisions.

Compatible tools like VMware PowerCLI allow automation of vSphere and vSAN. These tools can be used to automate standard day-to-day operations such as the creation of virtual machines or storage policies. PowerCLI can also be used to validate that the security configuration has not drifted from its appropriate settings. If the configuration has changed, PowerCLI is able to reconfigure the ESXi servers, vCenter, or individual VMs so that they once again meet the required security configuration. In addition, because PowerCLI is a standard VMware tool, many IT virtualization teams already know how to work with PowerCLI and have created tools that will work with a VxRail cluster.

**SYSTEM RECOVERY**

A strong security defense is 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, VxRail Manager includes file-based backup and restore. All VxRail Appliances include a starter license for Dell EMC RecoverPoint for VM (RP4VM), which provides best-in-class local and remote replication and granular recovery.

VxRail Manager file-based backup and restore protects against the accidental deletion of the virtual appliance or the internal corruption of the appliance. Backups can be configured to transpire 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 RP4VM, if, for example, a virtual machine 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 Manger, RP4VM is quickly deployed, and day-to-day monitoring occurs through the familiar vCenter plug-in. Recovery is easy and performed using a familiar vSphere interface.

VxRail also integrates the ability to backup and restore VxRail Manager itself. This allows an administrator to quickly and easily revert back to a known good state as part of restoring the system post-intrusion.

**VXRAIL SECURE CONFIGURATION**

Configuring security can be a complex, error-prone process that has many of the same risks that it seeks to mitigate. Three different elements simplify the process of securing the VxRail infrastructure. First, vSphere has a “secure by default” approach to configuration. Second, Defense Information Security Agency Security Technical Implementation Guides (DISA STIGs) give a blueprint for security, and a variety of automation tools allow the monitoring and configuration of security parameters to be checked and configured as necessary. This enables the appropriate risk profile to be configured to correspond with the business needs. Finally, the ability to automate reverting the configuration back to a known secure state when unexpected changes occur is a vital part of VxRail security.
With vSphere 6.0, VMware began an initiative to make security the default setting for vSphere. This makes VxRail more secure straight out of the box. As part of this initiative, most recommended security settings were classified as either site specific or changed to a default to the secure setting. Settings that previously had to be changed after installation were updated so the secure setting became the default.

Configuration settings that are classified as site-specific cannot be configured by default. For example, the hostname of a remote syslog or NTP server. With VxRail, many of the settings that VMware classifies as site-specific are configured by VxRail Manager as part of the installation.

The United States Defense Information Systems Agency (DISA) develops and maintains Security Technical Implementation Guides (STIG) to provide the United States Department of Defense with implementable guidance on how to configure computer systems with an appropriately secure configuration. Many organizations use STIGs as a baseline to secure their systems. These STIGs provide a checklist in both a human readable PDF and an automated script. This enables automation tools to read the STIG and configure the environment to match the recommended configuration with minimal manual intervention. While existing VMware STIGs cover VxRail components including vSphere, ESXi and vSAN make implementation as easy as possible. Dell EMC is also pursuing a STIG specifically for VxRail.

Over time, configurations can drift to less secure positions. Because of this, it’s important to not only monitor the configuration but also automate restoration of the environment to the initial secure state. VxRail supports multiple different options depending on the level of automation required. VxRail has automated hardening tools that check the current configuration against a STIG, and if the configuration has changed, revert the configuration back to the known safe state. If a more extensive automation tool is required, VMware vRealize Suite works with VxRail environments to automate configuration management while maintaining governance and control. In addition, VMware offers AppDefense, a more application-focused tool that uses machine learning to gather information about a known good state for virtual machines and the applications they support. With this tool, when a variation from the known good state is detected, the administrator will be notified and a response can be automated from a library of incident response routines.

COMPATIBLE STANDARDS AND CERTIFICATIONS

VxRail is a robust and flexible hyper-converged infrastructure that can be configured to meet industry standards and security certifications. While some HCI vendors may claim compatibility, Dell EMC is actively pursuing full certification for the security standards that are important to our customers. Contact your Dell EMC representative to discuss how VxRail meets even the most stringent business and regulatory requirements. Below is a list of a few of the standards and certifications that apply to VxRail.

- **FIPS** – 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. It’s used 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. PowerEdge servers used by VxRail have been validated.

- **Common Criteria EAL 2+** – Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria evaluations are performed on computer 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 used by VxRail currently hold certification, and certification of the full VxRail solution is in progress.
- **NIST Cybersecurity Framework** – The NIST Framework for Improving Critical Infrastructure is a voluntary guideline 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. The PowerEdge servers and vSphere components used by VxRail currently are compliant.

- **NSA Suite B** – Suite B is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. The current versions of ESXi and vCenter used with VxRail support NSA Suite B.

- **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’ve lost their jobs as a result of foreign trade. When sold as a system, VxRail is TAA compliant.

- **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 EMC provides manual and automated steps for configuring VxRail Appliance to comply with DoD Information Network (DoDIN) STIG requirements.

- **IPv6** – IPv6 is the next generation protocol used by the Internet. In addition to resolving the addressing limitations of IPv4, IPv6 has a number of security benefits, and many environments are moving toward adopting IPv6. VxRail will support IPv6 in dual stack mode in an upcoming release.

- **Trusted Platform Module** – The Trusted Computing Group define the specification for Trusted Platform Module (TPM). The Dell PowerEdge servers used in the VxRail are available with either TPM 1.2 or 2.0. Both are certifications with FIPS 140-2, TCG, and Common Criteria security requirements. vSphere currently supports TPM1.2

**NIST CYBERSECURITY FRAMEWORK AND VXRAIL**

The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. 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.

The NIST CSF “core” material is organized into five “functions,” which are subdivided into categories as seen in Figure 11 below.
VxRail is designed with security built in and deployed following security best practices. Users are authenticated and authorized with the appropriate level of access. VxRail clusters are easily configured with data-at-rest encryption to safeguard the confidentiality of the information contained, default network configuration segments traffic, and with tools such as RecoverPoint for VM, ensuring that applications and services can be quickly recovered if the integrity of the data is compromised. These security features are fundamental and inherent to the VxRail Appliance.

However, protecting an environment from today’s threats requires “defense in-depth” with multiple layers of security. The networks that connect the applications and services that run on the VxRail Appliance to the users that consume them must be protected, and the applications and services themselves must also 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. Only Dell Technologies has the full breadth of technologies and services to help you fully secure your environment.

The size of your organization and where your organization is along its IT transformational journey will determine the appropriate approach. Some environments may be working within existing security frameworks while others can take advantage of the opportunity to transform their security operations as they transform their IT infrastructure. Organizations often leverage many different vendors as part of their security program, which adds complexity that increases risk. Included in the Dell Technology family are RSA and SecureWorks; both help you manage risk and protect your digital assets. Only Dell Technologies can provide a single vendor relationship with deep security expertise worldwide and an ecosystem of thousands of partners. Figure 12 below illustrates the Power of Dell to help you manage risk and protect your data.

Visit the [NIST website](https://www.nist.gov) for more information on the NIST CSF. (For more information on how VxRail aligns with the NIST CSF, review the paper [VxRail Features Supporting NIST Cyber Security Framework](https://www.dell.com) available on [dellmc.com](https://www.dellmc.com).)
IDENTITY AND ACCESS MANAGEMENT

VxRail supports local user accounts, LDAP integration, and single sign-on. Although it’s possible to have a standalone VxRail, most environments will integrate with enterprise Identity and Access Management (IAM) systems that use directory services such as Microsoft Active Directory. Multifactor authentication provides additional means of authentication along with simple user IDs and passwords to increase identity security. Typically, multifactor authentication includes something a user knows, such as a password, in combination with something they possess, such as a software token, fingerprint, access card, etc. RSA SecureID is one of the most widely used multifactor authentication. The RSA SecureID Suite not only provides a means of multi-factor authentication, it also provides access management, identity governance and user lifecycle management to strengthen security, ensure compliance, and improve identity management.

SECURITY INCIDENT AND EVENT MANAGEMENT

VxRail Appliance includes vRealize Log Insight to centralize log management for the system. For organizations that have an existing centralized log management facility, such as Splunk or a Security Incident and Event Management System (SIEM), VxRail can be easily integrated using the industry standard syslog interface. RSA NetWitness Suite provides log collection, analysis, and many other security features that enhance the security capabilities of VxRail.

For customers who don’t want to manage security events themselves, SecureWorks provides log management services for VxRail and virtually any critical information asset or security technology. SecureWorks collects and monitors the security information you need to keep your business secure. More importantly, SecureWorks’ deeply skilled security experts—working from their integrated Counter Threat Operation Centers—investigate and respond immediately to any malicious activity 24/7.

KEY MANAGEMENT SERVER

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 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're needed, and access to the keys during decryption activities must be preserved for the lifetime of the data. Therefore, 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. Dell EMC CloudLink provides KMIP-compliant key management as well as encryption for public, private, and hybrid clouds. 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.

OTHER SECURITY PARTNERS
Securing today’s IT infrastructure and digital assets is a complex undertaking. A single solution can’t offer a robust enough defense. This is why Dell Technologies offers an ecosystem of partners working together to address the unique risks and vulnerabilities of your environment. We recognize that the entire industry must work together to help our customers achieve their cybersecurity goals.

Dell EMC VxRail Appliance and VMware vSphere support open security standards and partners play a vital role in helping our customers transition to a secure, virtual, and multi-cloud IT world.

The “VMware Integrated Partner Solutions for Networking and Security” whitepaper linked in Appendix A includes a list of a few partner solutions for networking, security, and compliance that are integrated with VMware vSphere®, vCenter™, vShield Endpoint™, and vCloud® Networking and Security™ and lists the full set of vSphere supported applications and software. In addition to the EPSEC APIs for antivirus/antimalware protection provided by vShield Endpoint, the VMware vCloud Ecosystem Framework provides service insertion at the vNIC and virtual edge level. The VMware Compatibility Guide makes finding the right component easy.

CONCLUSION
Security transformation begins with secure IT infrastructure. VxRail provides a secure, modern infrastructure for today’s virtual world. A hyper-converged 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 makes updating the complete software stack much simpler, which reduces the vulnerability to attacks.

Fully protecting an environment from today’s threats requires “defense in-depth” with multiple layers of security. The networks that connect the applications and services that run on the VxRail Appliance to the users that consume them must be protected, and the applications and services themselves must also 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. Only Dell Technologies has the full breadth of technologies and services to help you fully secure your environment.

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.
APPENDIX A: REFERENCES
All links and references cited in this whitepaper are displayed below.


Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers: http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download


NIST Cyber Security Framework: https://www.nist.gov/cyberframework

Other Resources

Security Features of the integrated Dell Remote Access Controller (iDRAC): http://en.community.dell.com/techcenter/extras/m/white_papers/20444744/download

vSAN documentation: https://docs.vmware.com/en/VMware-vSAN/index.html


Four business transformations: https://www.youtube.com/watch?v=TcKJ39_4Rwc
VMware encryption certifications: https://www.vmware.com/security/certifications/fips.html


NIST certifications for FIPs 140-2 search by Vendor for Dell EMC and VMware: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search

VMware Secure Development Lifecycle: https://www.vmware.com/security/sdl.html

VMware Key Management: https://blogs.vmware.com/vsphere/2017/10/key-manager-concepts-toplogy-basics-vm-vsan-encryption.html
