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 document describes both integrated and optional security features, best practices, and proven techniques for securing your VxRail Appliance from the Core to the Edge to the Cloud.

Dell Technologies Solutions
Contents

Introduction .................................................................................................................................................. 4

Security transformation begins with Dell Technologies ................................................................. 4

Bridge to digital future ......................................................................................................................... 6
  Building trust with Dell EMC product security programs .......................................................... 7

VxRail: The foundation for data center modernization and IT transformation .................... 11
  Dell EMC PowerEdge servers ............................................................................................................ 12
  Dell EMC VxRail HCI system software .......................................................................................... 13
  VMware vSphere .............................................................................................................................. 15
  VMware vCenter Server ................................................................................................................... 15
  VMware ESXi hypervisor .................................................................................................................. 16
  VMware virtual networking ............................................................................................................... 16
  VMware vSAN ................................................................................................................................. 16
  VMware vRealize Log Insight .......................................................................................................... 18
  VMware Cloud Foundation—including NSX .................................................................................... 18

VxRail security capabilities .................................................................................................................. 18
  Data security .................................................................................................................................... 19
  System security ............................................................................................................................... 25
  VxRail STIG hardening package ...................................................................................................... 28
  VxRail ACE security overview ........................................................................................................ 29
  Compatible standards and certifications ......................................................................................... 32
  NIST Cybersecurity Framework and VxRail .................................................................................... 34

VxRail security solutions and partners ............................................................................................ 35
  Identity and Access Management ..................................................................................................... 36
  Security Incident and Event Management ....................................................................................... 36
  Key management server .................................................................................................................... 36
  Other security partners .................................................................................................................... 37

Conclusion ............................................................................................................................................. 37

References .............................................................................................................................................. 39
Introduction

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 Core to Edge to the Cloud at an exponential rate. Security will always be a part of IT; With a focus 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 security never slows you down and instead accelerates innovation, allowing you to think in new, strategic ways and seize the opportunity.

Dell EMC VxRail provides the fastest and simplest path to this security transformation from Core to Edge to Cloud. 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 the 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 simply support business operations. 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 the VxRail Hyper-converged Infrastructure.

VxRail has security built in at every level of the integrated technology stack. Starting with each processor and PowerEdge server through the VxRail HCI System Software including the integrated VMware software. Securing the Core, the Edge, and the Cloud, ensuring availability, integrity, and confidence for every workload - traditional and cloud native.

Security transformation begins with Dell Technologies

Security Transformation within Dell Technologies is about rethinking security and accelerate innovation. Dell Technologies is focused on all levels with security, from the collaborations between the Dell Technologies companies, down to the product developed and released. VxRail is no exception. It is built with the highest levels of product security assurance and provides fully integrated security capabilities that can be used by your organization to optimize cybersecurity resiliency from the edge to the core to the cloud to accelerate innovation.
Dell EMC VxRail Appliances: Comprehensive Security by Design

Forbes reported: based on Risk Based Security research newly published in the 2019 MidYear QuickView Data Breach Report, within the first six months of 2019, publicly disclosed breaches have seen more than 3,800 exposing an incredible 4.1 billion compromised records. Based on these numbers, breaches may surpass the 6,515 publicly-disclosed data compromise events that were reported in 2018 by the same company.

Dell Technologies can ensure that your security strategies keep pace with your modernization initiatives to reduce your business risk.

1. Unify security programs with overall business risk so you know which risks are worth taking.
2. Implement advanced security operations that adapt to the changing threat landscape, so you can respond effectively to threats.
3. Build a resilient modern infrastructure that protects your endpoints, network, applications, and data.
4. Rely on trusted advisory services to help you design and implement your security transformation program. Dell Technologies is uniquely positioned to help you address all of these areas.

While a layered defense with multiple levels of security is required, these elements all must work in concert. Security transformation begins with a cyber resilient, modern infrastructure such as the VxRail that has been designed and built with security in mind.

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. That level of complexity offers multiple points of entry for would-be wrong-doers.

Security Standard and compliance also needs to be considered. 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.

- Payment Card Industry Data Security Standard (PCI DSS) – protections for credit card holders
• General Data Protection Regulation (GDPR) – European Union data privacy regulation
• The German Bundesdatenschutzgesetz (BDSG) – in detail 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
• California Consumer Privacy Act (CCPA) - enhance privacy rights and consumer protection for residents of California (signed into law 6/28/2018)

Dell Technologies believes that Security Transformation is about having a trusted partner – a partner that helps manage your digital risk, provide managed security services and bring expertise, services, solutions, and products that secure the full stack, from infrastructure to applications, and streamline operations, making security an essential part of the business strategy.

Dell Technologies is a trusted security partner for security transformation. Whether the focus is on endpoints, data centers, developers, identities, security operations, cloud, or virtualization – security needs to be end-to-end and Dell Technologies can help. We can help tackle security and business risk, handle security breaches, recover from a ransomware attack, and build secure applications. Security means a lot of things to a lot of people – some bad, some good. But no matter what, Dell Technologies wants organizations to take us on the journey.

Bridge to digital future

We are at a moment, where IT is being used more than ever to solve business problems. Organizations are doing this by implement data analytics, artificial intelligence, new applications, and smart devices to generate enormous amounts of data. This data drives actionable insights and unique competitive advantages. Despite this, many organizations still lack a clear digital vision and strategy; they use outdated technology, creating constraint, and a culture resistant to change. Without a proper plan, risk and security often become an afterthought or simply never a part of the larger strategy discussion. At this pivotal point in technology, this reactive way of doing business can no longer stand. To accelerate innovation and realize the potential of their digital future, organizations must rethink how they understand security.

In the IT world, security is typically viewed more as an obstacle than as an accelerator of positive change. Day-to-day, the job can be thankless and management have a difficult seeing a return on their investment. Security staff must manage mounting threats, complicated systems, and maintain a working knowledge of an ever-changing landscape. The seemingly daily barrage of cyberattacks on the news only exacerbates this stress, as does the sinking feeling that everything your organization owns could be lost in a second. But security does not need to be this wrought with fear and frustration. Security has always sought to be more positive, to be more proactive, but this is only possible with the right mindset and technology. We cannot keep thinking of security and risk like we have in
the past. To put this shift in perspective, think about a car’s brakes. Initially, you may think that brakes only serve to slow you down, but brakes are also what enable you to go faster. They give you the confidence to accelerate while preparing you for the obstacles and road ahead. Security and risk also need to be seen as accelerators for the organizations and not something that slows you down.

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. In 2012, the company also formalized a supply chain risk management program to extend security practices to Dell EMC’s suppliers of product components. Dell EMC continues to evolve its product security programs at the leading edge of industry standards and processes.

With the VxRail, Dell EMC continues its commitment to security. The VxRail development lifecycle follows the Dell EMC Product Security 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 is a significant part of the VxRail hyper-converged infrastructure that has also been developed using a similar Security Development Lifecycle.

**Secure Development Lifecycle**

The Dell EMC Secure 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 SDL is based on a set of controls that are implemented by the product R&D organizations. The following figure shows some of the typical activities performed as part of the SDL.

![Dell EMC SDL Activities](Figure 2)
The implementation and validation of these controls are driven by security champions within the product R&D organizations who work in close collaboration with the Product Security Office (PSO) security advisors. The following figure illustrates how these SDL maps onto a typical Agile lifecycle.

![Figure 3. SDL and a Typical Agile Lifecycle](image)

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 software vulnerabilities and design weaknesses in products.

This comprehensive approach to secure software development goes across policy, people, processes, and technology and includes the following:

- Dell EMC product security policy 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 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
Dell EMC VxRail Appliances: Comprehensive Security by Design

White Paper

technology. Where appropriate, open interfaces are used, allowing integration with customers’ existing security architectures.

- Dell EMC’s SDL overlays security on standard development processes to achieve a high degree of compliance with the Dell EMC product security policy. The Dell EMC SDL 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 benchmark for building security into 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 Dell EMC products to:
  - Meet customers rigorous security requirements,
  - Help customers meet regulatory requirements, such as PCI, HIPPA, etc.,
  - Minimize the risks to Dell EMC products and customer environments from security vulnerabilities.
  - Source code protection identifies how to properly secure Dell EMC engineering systems that contain 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 minimize this time gap to reduce risk.

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

Anyone can notify Dell 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 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’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 Technologies has a formal Supply Chain Risk Management program that ensures the hardware components used in the company’s products originate from properly vetted sources.

Supply chain security is defined as the practice and application of preventive and detective control measures that protect physical assets, inventory, information, intellectual
property, and people. Addressing physical, information, and personnel security helps provide supply chain assurance by reducing opportunities for the malicious introduction of malware and counterfeit components into the supply chain.

Dell’s Supply Chain Risk Management framework (below) mirrors that of the comprehensive risk management framework of the National Infrastructure Protection Plan (NIPP), which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Dell’s framework incorporates an open feedback loop that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle. The following figure illustrates the supply chain risk management process:

![Figure 4. Dell supply chain risk management process](image)

**Industry collaboration to improve product security**

Dell Technologies 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 Technologies 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 Technologies 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 Technologies understands a customer’s IT system doesn’t run solely on Dell Technologies products, so we’re committed to improving the security of the ecosystem wherever a product operates. That means being an active participant and a positive contributor throughout the industry.

Dell Technologies long commitment to advancing product security has created an 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 Technologies 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 Technologies 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.

- **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.

- **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.

- **FIRST**—The Forum of Incident Response and Security Teams is a recognized global leader in incident response. Dell PSIRT is a FIRSTVxRail team member.

**VxRail: The foundation for data center modernization and IT transformation**
To win the race against the continually evolving security threat landscape, 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 processors technologies 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.

VxRail can help your organization optimize cyber-resiliency, manage risk, and meet compliance requirements no matter what industry sector your organization is operating in. VxRail is the only fully integrated, pre-configured, tested hyper-converged infrastructure appliance that is powered by VMware vSAN. Whether VxRail is deployed in the data center, at the edge, or as part of a hybrid cloud solution, VxRail provides a simpler, better, and more secure delivery of business-critical applications, VDI, and remote infrastructure. VxRail enables Dell EMC to provide the customer, with the capabilities needed to optimize cyber resiliency across your entire deployment. The following figure illustrates security built into the VxRail:

![Security built into VxRail](image)

**Dell EMC PowerEdge servers**

VxRail is built on top of the Dell PowerEdge server platform 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 UEFI Secure Boot, 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 the 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, see Cyber Resilient Security in 14th Generation of Dell EMC PowerEdge.

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 executes 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:

![Hardware Root of Trust](image)

**Figure 6. 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 v1.2 and v2.0). 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.

Dell EMC VxRail HCI system software

The VxRail HCI system software is the foundation for the value differentiating the capabilities of VxRail. From an infrastructure stack perspective, it is the management software that runs on top of the VMware software and the PowerEdge server to allow the VxRail to act as a singular unified system.
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. VxRail lifecycle management capabilities ensure that the 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 fixes, or bug fixes. The term Continuously Validated States encapsulates the configuration stability delivered by VxRail clusters.

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

Ecosystem connectors—In order to build an extensive Electronic Compatibility Matrix, VxRail needs to be able to communicate with ecosystem members in the stack which includes vSphere, vSAN, vCenter, and the PowerEdge server and multiple hardware components within. The connectors allow VxRail to know the software/firmware versions running in each component and lifecycle manage those components. 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. VxRail users can perform any VxRail activity through this interface including initial cluster configuration, monitoring hardware components, performing graceful cluster shutdown, expanding the cluster by adding nodes, and updating the VxRail HCI System Software. It provides a fully integrated vCenter experience.

VxRail ACE (Analytical Consulting Engine) Global Orchestration—As enhancements are made to improve VxRail lifecycle management experience, much of it will depend on the analytical computing capabilities in VxRail ACE Global Orchestration. ACE stands for Analytical Consulting Engine. Through the advanced telemetry that HCI System Software gathers about the VxRail clusters, ACE is used to deliver AI-driven insights that will allow users to proactively manage their clusters to improve performance and availability. AI-driven insights are also driving more active multi-cluster management capabilities in ACE,
which is an area where HCI users will have an increasing interest as they expand their HCI footprint, and management at scale becomes a necessity.

**REST APIs**—VxRail benefits for lifecycle management ideally positions VxRail as the infrastructure platform of choice as the focus on simplifying IT operations plays a critical role in allowing IT teams to focus on cloud-based IT service delivery models. Making the VxRail platform extensible via APIs enables customers to build on top of infrastructure-as-a-service solutions. APIs also enables management at scale which can benefit customers with a large number of VxRail clusters deployed in various locations and have chosen in-house scripted solutions to manage at scale.

**Support Remote Services**—Support experience can also be a critical factor in choosing the correct HCI solution. VxRail provides single vendor support for VMware software, PowerEdge server, and VxRail software through Dell Technical Support. VxRail support includes Dell EMC Secure Remote Services for call-home and proactive two-way remote connection for remote monitoring, diagnosis, and repair throughout the entire lifecycle process to ensure maximum availability.

**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 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.

AppDefense is used to secure the applications running on the VMs. AppDefense protects the integrity of applications running on vSphere by using machine learning to understand the intended state and behavior of the application and machine in order to detect and prevent threats—VxRail running vSphere Enterprise Plus.

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, see VMware Product Security.

**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 VM. VxRail can either use an instance of vCenter that is deployed within the VxRail cluster 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
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. In addition, ESXi assigns VMs a region of usable memory and manages shared access to the physical network cards and disk controllers 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.

VMware virtual networking

A fundamental security requirement is to isolate network traffic. On VxRail, vSphere’s virtual networking capabilities provide flexible connectivity and isolation. 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 network access.

Additionally, 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 high performance, flash-optimized, HCI 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 vSAN data-at-rest-encryption
With vSAN, disks on each VxRail node are automatically organized into disk groups with a single cache Drive and one or more capacity drives. These disk groups are used to form a single vSAN Datastore, which is accessible across all the nodes in a 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 caching and capacity. The following figure illustrates the basic concepts of vSAN:

![Figure 8. The basic concepts of vSAN](image)

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 amount of usable storage will be dependent on the protection level used. 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 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.

**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 a secure infrastructure. For customers who already have a logging facility or a SIEM, VxRail easily integrates using the industry standard syslog protocol.

**VMware Cloud Foundation—including NSX**

VMware Cloud Foundation on VxRail is a Dell EMC and VMware jointly engineered integrated solution with features that simplify, streamline, and automate the operations of your entire Software-Defined Datacenter (SDDC) from Day 0 through Day 2. The new platform delivers a set of software-defined services for compute (with vSphere and vCenter), storage (with vSAN), networking (with NSX), security, and cloud management (with vRealize Suite) in both private and public environments, making it the operational hub for your hybrid cloud.

VMware Cloud Foundation on VxRail provides the simplest path to the hybrid cloud through a fully integrated hybrid cloud platform that leverages native VxRail hardware and software capabilities and other VxRail unique integrations (such as vCenter plugins and Dell EMC networking). These components work together to deliver a new turnkey hybrid cloud user experience with full-stack integration. Full-stack integration means you get both HCI infrastructure layer and cloud software stack in one complete automated lifecycle turnkey experience.

VMware NSX Data Center is the network virtualization and security platform that enables the virtual cloud network. It’s a software-defined approach to networking that extends across data centers, clouds, endpoints, and edge locations. With NSX Data Center, network functions—including switching, routing, firewalling, and load balancing—are brought closer to the application and distributed across the environment. Similar to the operational model of VMs, networks can be provisioned and managed independent of the underlying hardware.

NSX Data Center reproduces the entire network model in software, enabling any network topology—from simple to complex multilayer networks—to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX including micro-segmentation or from a broad ecosystem of third-party integrations ranging from next-generation firewalls to performance management solutions to build inherently more agile and secure environments. These services can then be extended to a number of endpoints within and across clouds. For additional information see [VMware Cloud Foundation on VxRail Architecture Guide](#).
Security capabilities are broken into 2 sections—data security and system security. Then following secure system configuration and management of the VxRail follow the principals of the Confidentiality-Integrity-Availability (CIA) triad.

VxRail provides a fully pre-configured and tested stack for all the security capabilities. These security capabilities are integrated and included with the appliance.

**Data security**

Data security follows the CIA triad in order to ensure data is only available to authorized and or specific accounts. That compliance and specifications are met. This includes both physical and user level access to data.

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

**Encryption**

Encryption protects the confidentiality of information by encoding it to make it unintelligible to unauthorized recipients. With VxRail, datastores can be encrypted using vSAN’s data-at-rest encryption (D@RE), which provides FIPS 140-2 Level 1 validated protection. 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 the full benefit of these space reduction techniques is maintained.

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, while VM encryption can be turned on and off; VM’s that get encrypted, migration with vSphere vMotion will always use encrypted vSphere vMotion. VM's that are not encrypted, can select from the encryption option of Disabled, Opportunistic, and Required when using vMotion. Opportunistic would be used by default on unencrypted VM during vMotion. The following figure summarizes the difference between VM encryption and vSAN encryption:
VxRail security capabilities

Figure 9. VM encryption vs. 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 cluster within a vCenter instance. Encrypted vMotion can be used with vSAN encryption to have both data at rest encryption and data in flight encryption. Encrypted vMotion is enforced for VMs with vSphere Encryption enabled.

Except for 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 Key Management Interoperability Protocol (KMIP) v1.1 or higher such as Dell EMC CloudLink. VMware maintains a Compatibility Guide of KMSs 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 the 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, but without authority to alter encryption settings.

**VxRail software defined networking using the optional NSX**

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

NSX with VxRail is an integrated security solution that reduces the need to deploy additional security hardware or software components. With NSX, 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 VM, as well as VDI environments. A few of the benefits of using NSX 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 HTML5 Web Client and NSX Manager plug-in.
- Consistent and automatic security controls using groups and policies. 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-deney rules to control traffic.
- Detection and blocking of spoofed VM 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 enhances the security posture of an environment and is compliant with the following certifications and standards:

- Common Criteria certification – EAL 2+
VxRail security capabilities

- ICSA Labs certified firewall
- FIPS 140-2
- Satisfaction of all NIST cybersecurity recommendations for protecting virtualized workloads

By leveraging the optional VMware NSX 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 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.

**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 limited, forcing management task completion to occur through vCenter.

Lockdown in "Normal" mode allows a select group of users to be white-listed, enabling them to manage the servers locally instead of through vCenter; this whitelist must include certain VxRail management accounts.

In strict lockdown mode, no users are allowed to manage the servers locally. Lockdown in "Strict" mode is not supported by VxRail.

**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 1.2” vCenter, iDRAC, and HCI System Software all disable the clear text HTTP interface and require the use of HTTPS, which uses TLS 1.2. 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.

**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 is 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 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.

**UEFI secure boot**

UEFI secure boot protects the operating system from corruption and root kit attacks. UEFI secure boot validates that the firmware, boot loader, and VMkernel are all digitally signed by a trusted authority. In addition, UEFI 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 the 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. With VxRail being co-engineered with VMware, we are read in early on plans for security fixes, which enables the VxRail team to quickly validate and prepare pre-qualified security patches. But not everyone is on the same side, and it becomes a race between the defenders who are working to mitigate and remediate the threats and the attackers whose goal is to exploit the vulnerabilities. VxRail being co-engineered with VMware, we are read in early on plans for security fixes, which enables VxRail team to quickly validate and prepare pre-qualified security patches.

VxRail software lifecycle management makes what could be complex and risky update operations, easy to install, and safe to implement. The 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 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 HCI System Software when updates are available. The administrator can then 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.

Not only does HCI System Software lifecycle management reduce complexity, but it also makes the infrastructure more secure by reducing the time and difficulty it takes to patch systems and remove the risk.

**VxRail with vSphere availability features**

VxRail leverages the built-in vSphere availability features including VMware High Availability (HA), VMware Distributed Resource Scheduler (DRS), and VMware 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 HA monitors running VMs in a VxRail cluster. If a VM or node fails, HA restarts on another node elsewhere in the cluster. A VM 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 spread the VM workload across all the hosts in the cluster. As VM resource demands change, DRS will migrate VM workloads, using vSphere vMotion, to other hosts within the cluster. Cyber-attacks can cause resource issues for VMs not targeted by the attack. Cyber-attacks often cause heavy resource utilization by the VM being attacked, and therefore heavy utilization of resources at the host level, which 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.

VMware stretched cluster extends the VxRail cluster from a single site to stretching the cluster across two sites for a higher level of availability. Only a single instance of a VM exists, however, fully copies of its data are maintained at both sites. Should the current site the VM is running on becomes unavailable, then 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 Appliances incorporates a starter pack for Dell EMC RecoverPoint for VM (RP4VM), 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 the virtual appliance or the internal corruption of the appliance. 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 RP4VM, 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, 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.

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

File-based backups of VxRail HCI System Software help to ensure business continuity in the rare event the VxRail VM needs to be rebuilt.

**System security**

**VxRail authentication, authorization, and accounting**

Authentication, Authorization, and Accounting (AAA) framework built in. The 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.

**Authentication**

Authentication to HCI System Software is handled by SSO through the vCenter plugin. VxRail 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) 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
VxRail security capabilities

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 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, HCI System Software, and vSphere.

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 the VxRail management plugin within vCenter. 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 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. 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.

vSphere Role Based access control supports the granular security principles of “Least Privilege” and “Separation of Responsibility,” and allows the security administrator to enhanced security by defining precise permissions based on the systems management structure of an 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. 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 on the attack to determine severity. According to the 2019 Trustwave Global Security Report, (registration required), Fifty-seven percent of the incidents investigated involved corporate and internal networks (up from 50% in 2017).
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 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 drill down to the root cause of the issue. The following figure shows the vRealize Log Insight dashboard:

![Figure 10. Realize Log Insight](image)

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 the standard syslog protocol.

**VxRail physical location security**

Physical security is an important part of any comprehensive security solution. Because VxRail 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. 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 when it is implemented, increasing the time to value of those decisions.

Compatible tools like vRealize Automation allows the automation of vSphere and vSAN. These tools can be used to automate standard day-to-day operations such as the creation of VMs or storage policies. vRealize Automation can also be used to validate that the security configuration has not drifted from its appropriate settings. If the configuration has changed, vRealize Automation is able to reconfigure the ESXi servers, vCenter, or individual VMs so that they once again meet the required security configuration. 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.

**VxRail STIG hardening package**

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 Systems Agency Security Technical Implementation Guides (DISA STIGs) give a blueprint for security hardening, 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.

Starting 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 HCI System Software as part of the installation.

Many organizations use STIGs as a baseline to harden 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 VxRail Appliance running VxRail Appliance software v4.5.x or 4.7.x comply with relevant DISA Security Technical Implementation Guidelines (STIG) requirements.

Over time, configurations can drift to less secure positions. Because of this, it’s important to not only monitor the configuration but also automate the 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 VMs 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.

**Security built into VxRail ACE Global Orchestration**

VxRail Analytical Consulting Engine (ACE) Global Orchestration complements the built-in operational simplicity with operational intelligence for the VxRail clusters. VxRail ACE delivers a combination of operational simplicity and operational intelligence with intrinsic security, enabling companies’ pursuit of IT infrastructure transformation.

VxRail ACE runs on a Dell EMC IT managed cloud platform. As a cloud-based SaaS solution, VxRail ACE has the flexibility to deliver new functionality frequently and without disruption, providing an exceptional customer experience. Its neural network for deep learning will continually improve its predictive capabilities as it ingests the wealth of metadata VxRail can collect about its clusters.

VxRail users can access VxRail ACE at [https://vxrailace.emc.com](https://vxrailace.emc.com) using their Dell EMC support credentials.

VxRail ACE collects telemetry data from VxRail nodes across the organization’s VxRail clusters and securely transmits that data to a SaaS solution managed by Dell EMC IT as shown in the following figure:
VxRail security capabilities

Figure 11. VxRail ACE high-level architecture

Dell EMC understands customers’ concerns in maintaining the security of their data. Security is intrinsic to VxRail ACE, from data collection through data transit and at rest. In addition, VxRail ACE has been securely developed using architectural controls as part of the Dell EMC standard Security Development Lifecycle. This standard defines the security-focused activities Dell EMC product teams must follow when building and releasing products in order to enable Dell EMC products to minimize the risks to our products and customer environments from security vulnerabilities.

VxRail ACE data collection

On each VxRail cluster, an Adaptive Data Collector (ADC) is running that retrieves telemetry data from the HCI System Software through VxRail hardware and software connectors. ADC does not collect any Personally Identifiable Information (PII). The telemetry data collected by the ADC is shown in the following table:

<table>
<thead>
<tr>
<th>Basic Telemetry (HW Topology: Appliances, Drive, Firmware, PSU)</th>
<th>Performance Data</th>
<th>Alarms</th>
<th>Hardware Sensor Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cluster Information&lt;br&gt; • Appliance Information</td>
<td>• Cluster (CPU, Memory, Disk)&lt;br&gt; • VM (CPU, Memory, Disk)&lt;br&gt; • vSAN (Disk, Network)</td>
<td>• vCenter&lt;br&gt; • VxRail</td>
<td>• Sensor Type&lt;br&gt; • Health State&lt;br&gt; • Name&lt;br&gt; • Current Reading</td>
</tr>
</tbody>
</table>

Telemetry data collected by the ADC is not stored locally; the data is transmitted securely over the Dell EMC Secure Remote Support (SRS) Gateway.

VxRail ACE data in transit to Dell

Only data collected by the Adaptive Data Collector (ADC) is sent to the Dell EMC backend over Dell EMC’s Secure Remote Service (SRS) Gateway. VxRail ACE subscribes for notifications of HCI system data arrival via the SRS Gateway. VxRail ACE Customers control which systems send HCI system data over the gateway. All data transmitted over the Dell EMC SRS Gateway is protected in transit by industry-standard best practices. The SRS Gateway is bidirectionally authenticated using RSA® digital certificates in...
conjunction with customer-controlled access policies and a detailed audit log. Point-to-point communication is established through the use of Advanced Encryption Standard (AES)-256 bit encryption which ensures all data is securely transported to the Dell EMC IT managed infrastructure. In addition, SRS provides for dedicated VPN and multi-factor authentication. Once the data arrives at Dell, VxRail ACE encrypts and stores the ACE data in its own Dell EMC IT managed infrastructure.

**VxRail ACE data at rest**

HCI system data received from VxRail ACE managed systems is encrypted and stored on the Dell EMC IT managed Dell infrastructure.

The Dell EMC IT infrastructure:
- Provides a secure platform that ensures each customer’s telemetry data is isolated.
- Provides High Availability, Fault Tolerance, and Disaster Recovery.
- Locates customer’s telemetry data (including backups) in the U.S.
- Indefinitely retains historical data for systems that are actively being monitored by ACE, including ACE-derived insights.
- Gives each customer access to an independent, secure portal from which each user can only see those systems in VxRail ACE that are part of that user’s site access as defined in Dell EMC MyService360.

Dell Technologies Security and Resiliency Office (SRO), led by Dell’s Chief Security Officer, is responsible for the security and protection of Dell EMC’s information technology infrastructure that hosts the VxRail ACE SaaS solution. This is accomplished via established governing security policies and procedures, and enforcement of Information Security controls, which include measures such as multi-layered firewalls, intrusion detection systems, industry-leading antivirus, and malware protection. The Dell EMC cybersecurity team is involved in running continuous vulnerability scans on the application and underlying environment. Any required remediation is handled through an ongoing vulnerability remediation program such as software upgrades, patches, or configuration changes.

All data sent to VxRail ACE is stored on infrastructure hosted in the Dell EMC data center. The Information Security Policy ensures that all Dell EMC information and resources are properly protected, information owners must ensure all resources are accounted for, and each resource has a designated custodian. All infrastructure components are located in the dedicated Dell EMC firewall-protected enclave network that is not exposed to external access. No individual direct login to the database server and database is allowed, except by the members of System Administrator and Database Administrator teams. Database application accounts are managed using standard database password authentication. Dell EMC has implemented an industry best practice Change Management process to ensure that Dell EMC infrastructure hardware is stable, controlled, and protected. Change Management provides the policies, procedures, and tools needed to govern these changes, to ensure that they undergo the appropriate reviews, approvals, and are communicated effectively to users.
VxRail security capabilities

VxRail ACE data access control

VxRail ACE data access can be divided into two categories:

- Access by customers to VxRail ACE for viewing their system data and ACE-derived insights.
- Access by internal Dell EMC IT System Administrator and Database Administrator to the VxRail ACE infrastructure that is managed by Dell EMC.

The sub-sections below describe how data access is controlled by these two categories of users.

End user access to VxRail ACE

Customers use their existing support account to login to VxRail ACE. Access to VxRail ACE data from the VxRail ACE portal requires that each end user has a valid Dell EMC support account. Authentication is handled by Dell EMC’s Single-Sign-On (SSO) infrastructure. VxRail ACE uses the Dell EMC MyService360 customer user profile for access control. The user profile is created and associated with a valid customer profile when the user registers for an account with Dell EMC. VxRail ACE provides each customer with an independent secure view of their systems and ensures that they will only be able to see their own data via VxRail ACE. Each user can only see those systems in VxRail ACE that are part of that user’s site access as per the configuration of that user in Dell EMC MyService360.

Administrative access to VxRail ACE infrastructure managed by Dell EMC IT

Dell EMC is very sensitive to the importance of protecting customers’ proprietary and confidential information. To that end, all Dell EMC employees are required to sign an employee agreement, which includes provisions that address all customer information. The obligations of this agreement extend to any machine-stored data perceived, in any manner or format, while engaged in maintenance services and remain in effect even after termination of employment with Dell EMC.

VxRail is a robust and flexible hyper-converged infrastructure that can be configured to enable organizations to satisfy compliance regulations. 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. 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. 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 full certification.

• **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.

• **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.
VxRail security capabilities

- **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 (DISA) 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 passed USGv6 interoperability testing for IPv6 in dual stack mode, as well as the higher standard for IPv6 Ready testing.

- **Trusted Platform Module**—The Trusted Computing Group defines the specification for the Trusted Platform Module (TPM). TPM 1.2 and 2.0 are optionally available with VxRail. Both are certifications with FIPS 140-2, TCG, and Common Criteria security requirements. vSphere supports TPM1.2 and TPM 2.0.

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 the categories shown in the following figure:
VxRail security solutions and partners

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
VxRail security solutions and partners

Dell EMC VxRail Appliances: Comprehensive Security by Design

White Paper

Figure 13. The Power of Dell to help you manage risk and protect your data

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.

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.

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. The following figure illustrates the Power of Dell to help you manage risk and protect your data.
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.

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 a secure IT infrastructure. VxRail provides a secure, modern infrastructure from the Core to Edge to the Cloud. 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 VxRail composite bundles may include updates to BIOS, firmware, hypervisor, vSphere, or any of the included management components that 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.
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.
The following table lists all links and references cited in this white paper:

<table>
<thead>
<tr>
<th>Asset</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Resilient Security in 14th generation of Dell EMC PowerEdge servers</td>
<td><a href="http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download">http://en.community.dell.com/techcenter/extras/m/white_papers/20444755/download</a></td>
</tr>
<tr>
<td>list of compatible key management servers</td>
<td><a href="https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&amp;details=1&amp;page=1&amp;display_interval=10&amp;sortColumn=Partner&amp;sortOrder=Asc">https://www.vmware.com/resources/compatibility/search.php?deviceCategory=kms&amp;details=1&amp;page=1&amp;display_interval=10&amp;sortColumn=Partner&amp;sortOrder=Asc</a></td>
</tr>
<tr>
<td>Asset</td>
<td>URL</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>VxRail Techbook</td>
<td><a href="https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf">https://www.emc.com/collateral/technical-documentation/h15104-VxRail-appliance-techbook.pdf</a></td>
</tr>
<tr>
<td>Security Features of the integrated Dell Remote Access Controller (iDRAC)</td>
<td><a href="http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download">http://en.community.dell.com/techcenter/extras/m/white_papers/20441744/download</a></td>
</tr>
<tr>
<td>vSAN documentation</td>
<td><a href="https://docs.vmware.com/en/VMware-vSAN/index.html">https://docs.vmware.com/en/VMware-vSAN/index.html</a></td>
</tr>
<tr>
<td>Four business transformations</td>
<td><a href="https://www.youtube.com/watch?v=TcKJ39_4Rwc">https://www.youtube.com/watch?v=TcKJ39_4Rwc</a></td>
</tr>
<tr>
<td>VMware encryption certifications</td>
<td><a href="https://www.vmware.com/security/certifications/fips.html">https://www.vmware.com/security/certifications/fips.html</a></td>
</tr>
<tr>
<td>NIST certifications for FIPs 140-2 search by Vendor for Dell EMC and VMware</td>
<td><a href="https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search">https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search</a></td>
</tr>
<tr>
<td><strong>ACE Resources</strong></td>
<td></td>
</tr>
<tr>
<td>ACE Overview video demo</td>
<td><a href="https://vxrail.is/acedemo">https://vxrail.is/acedemo</a></td>
</tr>
<tr>
<td>Smart update bundle staging video demo</td>
<td><a href="https://vxrail.is/aceupdates">https://vxrail.is/aceupdates</a></td>
</tr>
<tr>
<td><strong>YouTube - Security Resources</strong></td>
<td></td>
</tr>
<tr>
<td>Youtube - VxRail Security Overview</td>
<td><a href="https://www.youtube.com/watch?v=ZTNmYBgJv4s">https://www.youtube.com/watch?v=ZTNmYBgJv4s</a></td>
</tr>
<tr>
<td>Youtube - VxRail Security Hardening and Compliance</td>
<td><a href="https://www.youtube.com/watch?v=ZjhfCE5ng6U">https://www.youtube.com/watch?v=ZjhfCE5ng6U</a></td>
</tr>
</tbody>
</table>