VxRail Cybersecurity Solutions Overview

Challenge

Implementing a comprehensive security strategy that safeguards sensitive data from being breached and can rapidly recover data if a breach occurs is an essential priority for IT professionals. Outdated infrastructure is difficult to defend.

Solution

The Dell EMC VxRail Appliance, developed jointly with VMware, is a secure, resilient hyperconverged infrastructure system that protects vSphere®-based virtual environments. With flexible configuration options, VxRail is capable of securely hosting the most demanding workloads and datasets. Deployed with Dell Technologies products and solutions, VxRail provides an end-to-end solution able to stay a step ahead of today's evolving threat landscape.

Benefits

- Modern infrastructure engineered to defend VMware-based environments.
- Flexible configuration options to handle the most demanding workloads.
- Tightly integrated software stack reduces attack surface.
- Engineered, manufactured, deployed and maintained as a single product.
- Built-in software lifecycle management keeps the environment secure.
- Dell EMC RecoverPoint® enables rapid recovery if an attack occurs.
- Single vendor support for the end-to-end solution.

The Dell EMC VxRail™ hyperconverged infrastructure appliance provides the foundation for a resilient, adaptive cybersecurity strategy

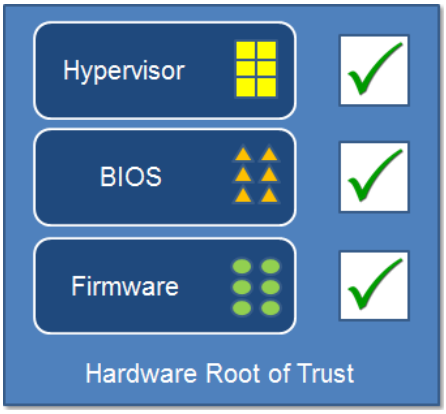
According to Risk Based Security, a security analytics company, more than 5,000 publicly-disclosed data breaches occurred in 2017, with nearly 8 billion records exposed. Governing bodies around the world are implementing sweeping regulations to force enterprises to be accountable for protecting customer data on their systems. While financial penalties can damage a company's bottom line, the notoriety of a breach can have a devastating effect on a company's brand and reputation.

Outdated infrastructure is difficult to defend, and point products from multiple vendors add complexity and increase the risk of vulnerabilities that can be exploited. Defending the business begins with secure modern infrastructure such as the Dell EMC VxRail Appliance, a hyperconverged infrastructure platform designed, built, deployed and supported to securely handle the most demanding workloads.

VxRail: Secure, resilient, adaptable infrastructure

As the only fully integrated, preconfigured, and pre-tested VMware hyperconverged infrastructure appliance family on the market, VxRail dramatically simplifies IT operations, accelerates time to market, and delivers incredible return on investment. VxRail is engineered, built, configured, and maintained following Dell EMC's stringent industry-leading Secure Development Lifecycle process. VxRail is a fully integrated, preconfigured and pretested hyperconverged family of appliances delivered and supported as a single product by Dell EMC.

VxRail is built on the latest generation of Dell EMC PowerEdge™ servers and Intel® Xeon® Scalable Processors with embedded hardware and system-level security features. As shown in the figure below, cryptographically signed and verified firmware ensures the server executes only the intended version of firmware, BIOS and hypervisor while preventing the undetected introduction of malware.



What makes up a VxRail Appliance?

Jointly engineered with VMware, VxRail is a fully integrated, preconfigured, and pretested hyperconverged family of appliances, delivered as a single product and supported by Dell EMC. VxRail offers configuration choices to meet any use case.

Components that make up a VxRail system include:

- Latest generation of Dell EMC PowerEdge Servers.
- vSphere ESXi hypervisor preinstalled on each node.
- VMware vCenter Server™ interface provides day-to-day management of the virtual infrastructure.
- VMware vSAN® software-defined storage provides secure and resilient storage.
- VMware virtual networking isolates network traffic.
- VxRail Manager provides lifecycle management and serviceability for clusters.
- VMware vRealize Log Insight™ provides ongoing notifications about the state of the virtual environment and appliance hardware. vRealize Log Insight easily integrates into an existing log management facility or an end-to-end security information and event management (SIEM) solution.

VxRail protects sensitive data

Denying attackers access to sensitive information while ensuring appropriate, authorized access is a fundamental requirement for a secure environment. VxRail offers encryption to protect the confidentially of data in use, in motion and at rest. vSAN encryption protects the entire datastore. All virtual machines (VMs) leverage vSAN encryption while still achieving the space-saving benefits of deduplication and compression. VM encryption provides the flexibility to encrypt on a per-VM basis, allowing a single cluster to have both encrypted and non-encrypted VMs. VM encryption follows the VM wherever it is hosted and fully protects data as it is transported over the network during a vMotion migration. In addition, VxRail supports encrypted vMotion where VMs are encrypted when they move between hosts. This includes vMotion migrations within a VxRail as well as vMotion migrations to or from a VxRail.

Other than vMotion encryption, where key management is handled internally, VxRail uses key management services compatible with the KMIP 1.1 standard. Internal encryption is handled by a common set of modules that are FIPS 140-2 validated.

VxRail ensures a secure configuration

VMware vSphere has a “secure by default” intent whereby system configurations are set for secure bias by default. Depending on the risk profile of the business, the system configuration can be further hardened. The United States Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) are used by both the public and private sectors for guidance on how to securely configure computer systems. Dell EMC has developed a VxRail STIG that may be used as a security blueprint. Using the Dell EMC VxRail STIG compliance scripts with automation tools, VxRail can be quickly and easily configured to a hardened state. The STIG can also be used to monitor the secure state of the system and, if necessary, revert the configuration back to a known secure state.

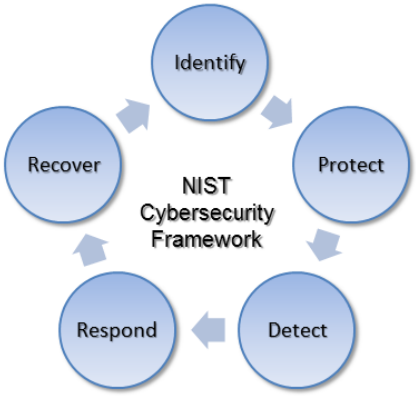
VxRail lifecycle management reduces complexity

Vendors frequently release software updates to address known security vulnerabilities. One of the most effective actions an organization can take to maintain a secure infrastructure is to keep their software patchescurrent. The VxRail team engineers, tests, and releases updates to all system software components as a bundle. A software bundle can include updates to BIOS, firmware, hypervisor, vSphere or any of the included management components.

When vulnerabilities are detected, fixes are quickly developed to mitigate the threat and then extensively tested on the VxRail platform before being released to customers. Systems administrators are notified of the update and can download the bundle directly from VxRail Manager. Using an automated procedure, administrators apply the update while the system remains online serving the business. Not only does VxRail Manager lifecycle management reduce complexity, it makes the infrastructure more secure by reducing the time and risk normally associated with patching a system.

Integrated Dell EMC RecoverPoint enables rapid system recovery

Strong security defenses are critical, but a robust and trusted recovery plan is equally important. Backup and replication are the cornerstones of recovery after a breach. All VxRail Appliances include an initial set of licenses for Dell EMC RecoverPoint for VM (RP4VM), which provides best-in-class local and remote replication and granular recovery. If a virtual machine is compromised, or data is damaged or ransomed, the VM and dataset can be quickly rolled back to the point-in-time prior to the attack, allowing the business to quickly recover.



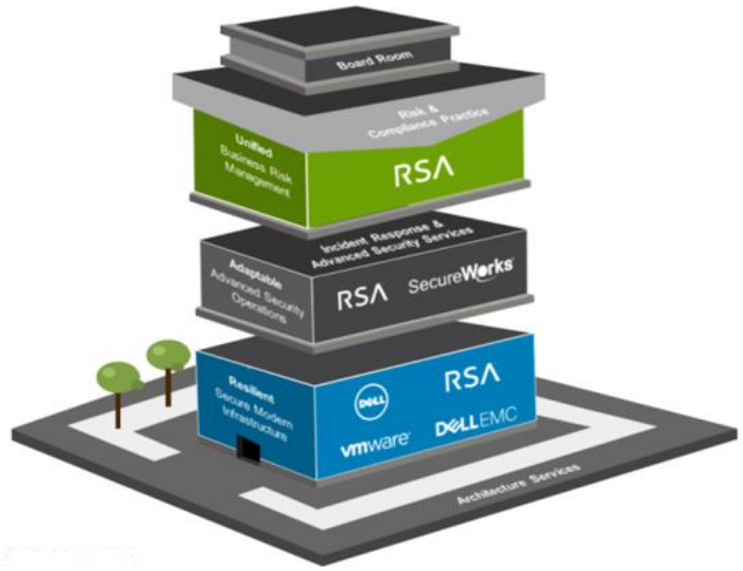
VxRail aligns with NIST cybersecurity framework

Cybersecurity is a broad and diverse topic. Security frameworks provide an effective way for people with different levels of security expertise to discuss cybersecurity. The NIST Cybersecurity Framework (NIST CSF) is organized into five core functions (shown in the figure to the left) that an organization must address to implement an effective cybersecurity strategy. Many organizations use the NIST framework to assess and improve their organization's ability to prevent, detect and respond to cyberattacks.

For more information on how VxRail aligns with the NIST CSF, review the *VxRail Features Supporting NIST Cyber Security Framework* technical note.

Only Dell Technologies has the products and services to master the security challenges of today and tomorrow

The figure to the right shows the Dell Technologies approach to IT and security transformation. Protecting an organization requires a layered defense with multiple levels of security. A secure, adaptive and resilient hyperconverged infrastructure provides the foundation. Layered on top of the infrastructure are advanced security operations that adapt and defend against ever-evolving threats. RSA incident response software and SecureWorks advanced services provide instantaneous visibility and understanding of what is going on across physical and virtual networks. Threat intelligence and advanced analytics incorporate real-time threat-feeds and analysis to help identify threats and make faster, more effective decisions. Rapid response and remediation leverage automated action and response decision support for faster containment across the entire attack surface.



Keeping your virtualization environment secure

- ✓ Start with VxRail, a secure modern infrastructure.
- ✓ Use encryption to protect data in use, in motion, and at rest.
- ✓ Apply appropriate secure configuration hardening.
- ✓ Keep system patched and updated.
- ✓ Deploy Dell Technologies security operations.

Summary

VxRail provides a secure, resilient, scalable infrastructure ideal for keeping VMware-based virtualization environment secure. VxRail is engineered, built, configured and maintained following Dell EMC's industry-leading Secure Development Lifecycle process. VxRail protects sensitive information by encrypting data in use, in motion and at rest. The system configuration has a "secure by default" intent and Dell EMC provides a STIG as a blueprint for further hardening. VxRail Manager automated software lifecycle management makes it easy to keep the system software up-to-date. By applying software bundles that have been extensively tested with the full VxRail software stack, the complexity and risk often associated with software updates is eliminated. While VxRail provides the foundation for security transformation, keeping VMware-based virtualization environments secure also requires advanced security operations. Only Dell Technologies has the breadth and depth of products and services to master the cybersecurity challenges of today and tomorrow.

Learn more about Dell EMC converged infrastructure.

Contact a Dell EMC Expert.
1-866-438-3622