

5 steps to protect your virtualization environment with VxRail Appliance

Security begins with a foundation of trust built on top of a secure platform. If you cannot trust the platform, you cannot trust anything upstream. The Dell EMC VxRail Appliance™ delivers a secure, modern infrastructure resilient from the ground up that protects the platform from power-on through the stack of hypervisor, VMs, OS and applications. VxRail surrounds data with security that moves with the data and automatically enforces least-privileged application access.

Step

1

START WITH VXRAIL, A SECURE MODERN INFRASTRUCTURE

The Dell EMC VxRail Appliance, developed jointly with VMware, is a secure, resilient and adaptable hyper-converged infrastructure system. With flexible configuration options, it is capable of securely hosting the most demanding workloads and datasets. VxRail has the adaptability to defend against current and future threats.

Step

2

USE ENCRYPTION TO PROTECT DATA IN USE, IN MOTION AND AT REST

Denying attackers access to sensitive information while ensuring appropriate, authorized access is a fundamental requirement of a secure environment. Through VMware vSphere®, VxRail offers encryption to protect the confidentiality of data in use, in motion and at rest.

Step

3

APPLY APPROPRIATE SECURE CONFIGURATION HARDENING

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. Using the Dell EMC VxRail Security Technical Implementation Guides (STIG) compliance scripts with automation tools, VxRail can be quickly and easily configured to a hardened state.

Step

4

KEEP SYSTEMS PATCHED AND UPDATED

One of the most effective actions an organization can take to keep its infrastructure secure is to keep their software patches current. The VxRail team engineers, tests and releases updates to all system software components as a bundle. When vulnerabilities are discovered, 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 the VxRail Manager interface. 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.

Step

5

DEPLOY DELL TECHNOLOGIES SECURITY OPERATIONS

Protecting an organization requires a layered defense with multiple levels of security. A secure, adaptive and resilient hyper-converged 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 visibility and understanding of what is going on in real-time across physical and virtual networks. Threat intelligence and advanced analytics incorporate real-time threat-feeds and analysis to help identify threats and make faster, more effective decisions. Rapid response and remediation leverage automated action and response decision support for faster containment across the entire attack surface.

[Learn more](#) about the Dell EMC VxRail Appliance. Contact a Dell EMC Expert at 1-866-438-3622.