When customers are looking at technologies to support their implementation of a NIST Cyber Security Framework they should understand how the feature sets of the product can support both their peoples and process planning. Dell EMC VxRail Appliances have numerous features that align to the NIST framework (image below), and this paper will provide evidence to that point.

National Institute of Standards and Technology, Cybersecurity Framework

https://www.nist.gov/cyberframework
Features and their security contributions

- **VxRail Hypervisor Manager:**
  Provides tight integration between the VMWare VSAN and vSphere Hypervisor that simplifies use

- **VxRail Policy Blueprints:**
  Pre-define the types of Virtual Machines configuration to include which technologies and access users can deploy

- **vRealize Health Checks:**
  Checks available resources and active queries on the vRealize Log Insight virtual appliance, and view current statistics about the operation of vRealize Log Insight

- **vRealize Log Insights:**
  Delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility. It provides deep operational visibility and faster troubleshooting across physical, virtual and cloud environments

- **Performance Monitoring for vCenter:**
  Support new entities, metrics and events such as datastore- and virtual machine–specific alarms. These alarms can trigger new automated workflows to remedy and pre-empt problems

- **FIPS 140-2 D@RE:**
  Provides at rest encryption for data that can protect against data exposure through physical media control loss

- **DISA STIG:**
  The system has been scanned using DISA level STIG standards for the core OS. A STIG level of security can be activated ensuring the highest level of system configuration for the system to decrease cyber-attack targets

- **Optional – NSX Inline Monitoring & Firewall:**
  Private support tunnel for Dell EMC remote support communications. Requires Secure Service Credentials, utilizing RSA technology

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. It provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes.

The NIST CSF is designed with the intent that individual businesses and other organizations use an assessment of the business risks they face to guide their use of the framework in a cost-effective way.

The framework is divided into three parts, "Core", "Profile" and "Tiers". The "Framework Core" contains an array of activities, outcomes and references which detail approaches to aspects of cyber security. The "Framework Implementation Tiers" are used by an organization to clarify for itself and its partners how it views cybersecurity risk and the degree of sophistication of its management approach. VxRail technology features can be used to support an organization planning for their people and processes to simplify framework implementation.

**Identify:**
The Identify tier is focused on developing organizational understanding to manage cybersecurity risk for systems, assets, data, and capabilities. VxRail has several technologies to support the Identify tier. VxRail can contribute to a customer’s asset management goals through granular data access and administrative management.

VxRail Policy Blueprints provides the capability to provide rules and restrictions for VM configuration and access. The vRealize Log Insights logging and dashboards can provide an extensive understanding of the environment to contribute Risk Assessment and Management.

An administrators Asset Management approach, to include details on access control and auditing capabilities should be regularly reviewed and updates should fall under the Governance process to ensure that changes align with the overall cybersecurity framework goals.

The approach for asset management, to include logging and auditing should influence the Risk Assessment. This data would drive adjustments and implementation of the expansive VxRail security and data protection technologies that include FIPS 140-2, DISA STIG, and optional NSX Inline Monitoring and Firewall.

The Identify Function should develop the organizational understanding to manage cybersecurity risk.
Protect:
Upon completion of the Identify tier a customer can use **VxRail Policy Blueprints**, **FIPS 140-2**, **DISA STIG features**, and **NSX Inline Monitoring and Firewall** to ensure data is utilized by personnel with appropriate requirements and credentials.

Maintenance processes are supported by the extensive capability to review performance, configuration, and performance logging and configurations provided by the Syslog Support for OS and Audit activities. The data can be reviewed and analyzed to identify existing issues as well as predict growth or identify future risks.

The Information Protection Process and Procedures can utilize the extensive Protective Technologies of VxRail for logging, audit (**vRealize Health Checks, Log Insights, Performance Monitoring for vCenter**), to support the people and processes for the Protect tier.

Detect:
The Detect tier is focused on developing and implementing the appropriate activities to take action regarding a detected cybersecurity event. The goal is to have processes defined prior to an event so that the response is measured and consistent with established policies and pre-defined outcomes.

Real time monitoring, alert, logging support, and audit capabilities (**vRealize Health Checks, Log Insights, Performance Monitoring for vCenter, and NSX Inline Monitoring & Firewall**) can be used to provide real time event information and compare historical data for anomalies in expected reporting and events.

Implementing DISA STIG Compliance will disable unnecessary services and ports for a highly secure deployment cutting down on the “noise” within the logging to ensure it is easier to identify and analyze for system anomalies.

If alerts or anomalies are reported the administrator should investigate VxRail Hypervisor, and Performance Monitoring for vCenter, and can contact Dell EMC to review logs and alerts to assist with the Detection Process to mitigate concerns.
Respond:
The Respond tier is focused on developing and implementing the appropriate activities to take action regarding a detected cybersecurity event. These plans should be pre-established prior to an event to ensure consistent response.

All of the work done in the Identify and Protect Tiers should now support a customer’s Respond activities. Reviewing VxRail Hypervisor and reviewing the VM snap settings, and the state of the replication, high availability configuration and backups should influence the Response Planning.

The planning data can be pulled into the Analysis phase with the addition of the data from the audit, logging, and monitoring data to identify needed changes to protect the environment and data.

Based on the analysis threat Mitigation is executed to deflect risk to unauthorized data access or loss. These practices can then be analyzed to assess whether they should be permanent changes to drive improvements in the overall protection profile.

Recover:
The Recover tier is focused on implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. If solid policies, processes, and practices were implemented in the Identify and Protect phases of the framework then data recovery should be easy to execute with the lack of data deletion capabilities that were enforced by the VxRail Policy Blueprints, protection of VMs from malicious user deletion.

VxRail Hypervisor can be utilized to check backups and snaps and can be used to recover compromised data or systems as necessary.
Dell EMC VxRail Appliances offer extreme configuration flexibility to choose the performance, capacity, and graphics capability needed to meet your HCI workload requirements. Dell EMC VxRail Appliances built on the new PowerEdge 14th generation servers powered by Intel® Xeon® Scalable processors offer configure-to-order platforms that deliver data services, resiliency, and QoS, enabling faster, better, and simplified delivery of virtual desktops, business-critical applications, remote office infrastructure, and more.

- **E Series** – Everywhere from data center core to edge deployments, the combination of density, drive groups, and balance of resources in a low profile 1U form factor enables it to be deployed for a wide range of use cases.
- **V Series** – VDI-optimized graphics ready appliances with support for up to three graphics accelerators for specialized use cases such as high-end 2D/3D visualization. Each appliance has one node per 2U chassis. Available in all-flash or hybrid configurations.
- **P Series** – Performance intensive appliances optimized for heavy workloads such as databases. Each appliance has one node per 2U chassis. Available in all-flash or hybrid configurations.
- **S Series** – Storage dense appliances for demanding applications such as virtualized Microsoft SharePoint, Microsoft Exchange, big data, and analytics. Each appliance has one node per 2U chassis. Available in hybrid configurations only.
- **G Series** – General-purpose appliances for broad hyper-converged use cases. Up to four nodes fit in a single 2U chassis. Available in all-flash or hybrid configurations. (Note: Currently available with Intel® Xeon® 2600 series processors in a non-PowerEdge platform.)