Whitepaper

Protecting and Securing Telecom Networks with Red Hat® OpenShift® and Dell EMC PowerProtect Data Manager

Protecting and Securing Telecom Networks with Red Hat® OpenShift® and Dell EMC PowerProtect Data Manager

Table of contents

Telecom Operators are moving to cloud native architectures

It has become evident that the road to 5G will be paved with clouds. Around the world, telecommunications operators are moving to cloud-native network architectures that support network functions and microservices running in containers on Kubernetes. In a traditional telecommunications architecture, services are delivered through network functions. With the advent of 4G, many of these functions moved from standalone appliances where the hardware and software were coupled together to decoupled virtualized network functions (VNFs) that could run on virtual machines. With 5G, the paradigm again shifts, this time from VNFs to microservices where the VNF software is essentially decoupled into smaller components stored in containers. The advantage of a container-based software approach is better portability, scalability, and agility. These containers are orchestrated into services using Kubernetes, which organizes the containers into logical clusters.

The shift to cloud-native networks has myriad benefits for operators. It can increase agility, reduce both CapEx and OpEx costs, simplify network management, and bring a host of new technologies to bear on 5G services including artificial intelligence (AI) and automation. This increased agility enables operators to deliver new services at the edge, to both consumers and enterprises, that drive revenue growth. AI and increased automation will provide insights and efficiencies that improve customer satisfaction and streamline operations.

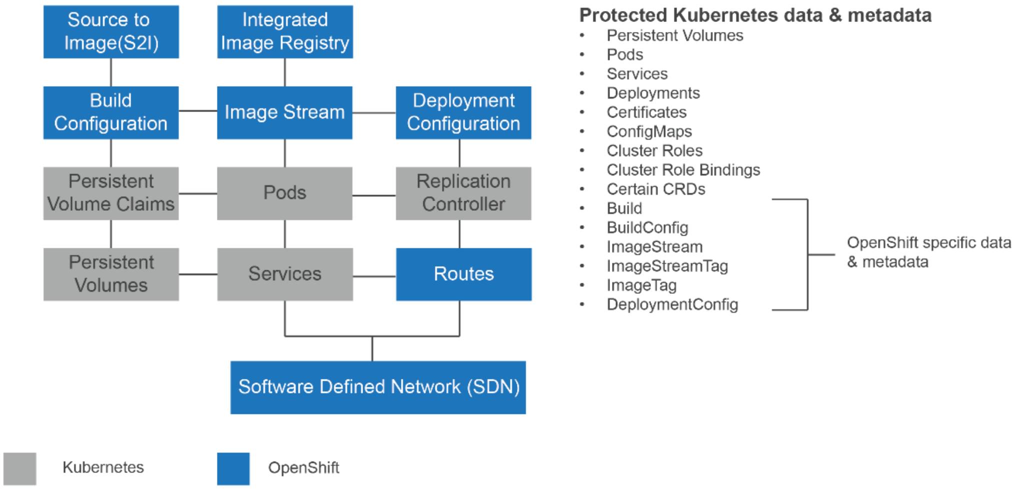
Red Hat OpenShift is an industry leading platform for delivery of container-based applications on Kubernetes. Red Hat has seen strong adoption among mobile operators due to its commitment to open standards and the quality of its professional services and customer support. Dell Technologies has partnered with Red Hat to create a reference architecture for communications service providers. This reference architecture provides a validated foundation for deploying a telco-grade, cloud-native, 5G network that features Red Hat OpenShift Container Platform on telco-optimized hardware and software from Dell Technologies.

Protecting data in a cloud native world

In this new cloud native world, data is becoming increasingly important and the requirements for managing and protecting it grow. As enterprises increasingly run business critical applications on operator networks, these enterprises will expect their data to always be protected, secure and available. In addition, the data from operations used to maintain and optimize network performance, enhance customer experience, and identify new ways of engaging with customers will become the fuel that drives competitive advantage. Like all network architectures, cloud-native networks carry risks of data loss that can impact operations from range of events such human error, machine error, natural disaster, sabotage, or cyber attack. This is especially true as the network topologies move to open, disaggregated ecosystems that stitch together network functions in containers running from the core to the far edge of the network.   Having a comprehensive data protection and management strategy becomes essential to ensuring operations and delivering services.

Securing databases and applications in an OpenShift environment

Protecting a telecom network based on a cloud native architecture means not only protecting the data generated by applications, but also the meta data associated with the platform and infrastructure running those applications.   Red Hat OpenShift is a container application platform that adds several additional components on top of the standard Kubernetes distribution. To fully restore OpenShift namespaces, data, and metadata for these additional components such as Build, BuildConfig, ImageStream, ImageStreamTag, ImageTag, DeploymentConfig must be backed up as well. These additional components support Source to Image and Image to deployment workflow that takes an existing source code repository and converts it to associated container or Docker images. Fortunately, Dell Technologies utilizes the OpenShift plugin that allows these components to be backed up and restored, extending the benefits of Dell EMC PowerProtect Data Manager to OpenShift environments.



Red Hat OpenShift NameSpace

PowerProtect Data Manager utilizes a specially designed boost plugin that allows it write to Dell EMC PowerProtect physical and virtual appliances located on-premises or in the public cloud.   During the discovery process, PowerProtect Data Manager will detect if a cluster is an OpenShift cluster and automatically install the OpenShift plugin. During backups and restores, the OpenShift plugin will be leveraged to protect the associated OpenShift components. This process is transparent to the user in terms of policy creation and during restores.

Power Protect Data Manager is a centralized, highly available software solution that provides consistent and reliable backup and restore services for the OpenShift platform and its workloads.   It automatically discovers and protects databases, virtual machines, file systems and Kubernetes containers while a common policy engine automates compliance and governance across workloads. It also provides application consistent protection for databases like MySQL, Oracle, SAP, Cassandra, MongoDB, and PostgreSQL.

PowerProtect Data Manager empowers application owners with self-service restore processes while maintaining central governance. DevOps and admin teams can quickly create point time copies for test and dev, cluster migration, data analysis and more.   They can also assign protection policies from a published list and ensure application consistent protection for databases from customizable templates. Data retention locks provide immutable copies to support regulatory, compliance and cyber recovery processes.

PowerProtect Data Manager significantly reduces network congestion through inline dedupe and compression achieving data reduction rates up to 65X with Dell EMC PowerProtect DD Series Appliances. It also includes software defined data movers enabling it to run multiple concurrent backup streams to create a highly scalable data protection solution for OpenShift environments.

PowerProtect Data Manager is now part of the Dell Technologies Red Hat OpenShift Reference Architecture for Telecom. This reference architecture provides operators with an accelerated path for deploying a cloud native network based on Red Hat OpenShift that includes a powerful policy-based data protection solution to secure the networks most valuable asset – data.

Cyber recovery with Dell EMC PowerProtect Cyber Recovery

Cyber threats are growing across every industry and telecommunications is no exception. In July 2020, Telecom Argentina had roughly 18,000 call center computers infected by a ransomware attack. The hackers caused extensive damage to the company’s network after they managed to gain control over an internal domain admin from which they spread their ransomware payload. The hackers demanded over $7.5 million dollars in ransom to unlock encrypted files[1].[i]

This is but one example of the cyber threats mobile operators face every day.   As operators deploy cloud-native networks based on open standards and industry standard hardware, they must have a cyber resiliency strategy and well-tested plans to protect and recover critical data, systems and operations from these threats.

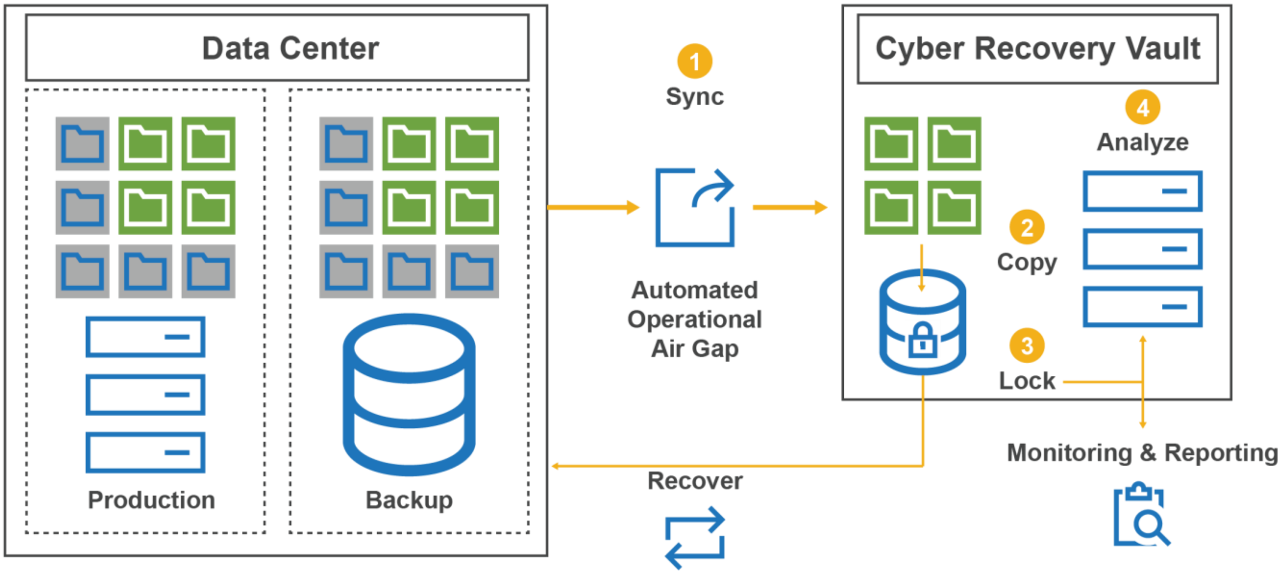
Real-time cyber protection solutions are never 100% effective. Therefore, cyber recovery processes should be an integral part of any cyber resiliency strategy. Protecting a copy of critical data, in an isolated manner, is the best-known way to provide recovery from attacks. Cyber security experts and leaders now recommend that organizations evaluate an offline and air-gapped “data vault” that contains point in time copies of the critical data to meet these requirements. Dell EMC PowerProtect Cyber Recovery, which is built upon Dell EMC PowerProtect Data Manager, provides an air-gapped data vault to protect critical data in OpenShift environments.

PowerProtect Cyber Recovery’s data vault provides a physical and logical separation from the main network. In the event of a ransomware attack or other network breach, a copy of all data, including the container information needed for service recovery, is preserved and available for recovery using standard data recovery processes.

The data vault process consists of four basic steps:

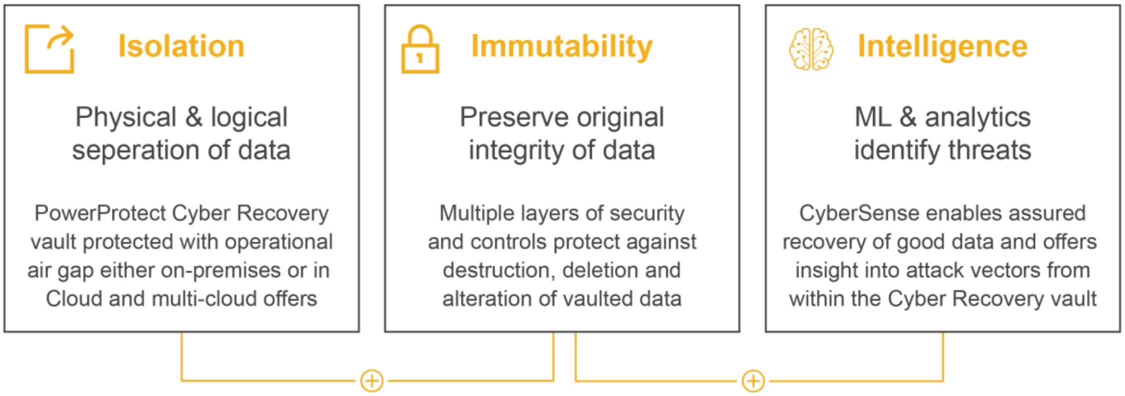
1. The management server unlocks the air-gap and synchronizes critical data into the data vault’s target storage. The air gap is then re-locked.
2. A copy of that data is made with a configurable retention policy
3. The data is retention locked to further protect it from accidental or intentional deletion
4. CyberSense analyzes for anomalies and remediation of corrupted files.

Recovering data from the vault in the event of a cyberattack can be performed using PowerProtect Cyber Recovery



Cyber Recovery Process

In Dell's experience, a secure "data vault" requires the 3 I's: Isolation, Immutability and Intelligence – both individually and collectively working in an integrated and seamless fashion in a very proscribed manner.



Isolation

Physical & logical seperation of data

PowerProtect Cyber Recovery vault protected with operational air gap either on-premises or in Cloud and multi-cloud offers

Immutability

Preserve original integrity of data

Multiple layers of security and controls protect against destruction, deletion and alteration of vaulted data

Intelligence

ML & analytics identify threats

CyberSense enables assured recovery of good data and offers insight into attack vectors from within the Cyber Recovery vault

Requirements for a Secure Data Vault

Isolation is critical. The vault is ideally operated in a physically restricted area, such as a cage or locked room, that helps to guard against an insider threat. When the air gap is a "locked" state – no data can flow – there is no access to any part of the solution.

Immutability is next. Using PowerProtect DD's Compliance Mode Retention Lock capability, data is prevented from deletion or change for a set time period. The lock cannot be overridden, even by an administrator with full privileges.

Intelligence for PowerProtect Cyber Recovery is based on the analytics engine – CyberSense. CyberSense scans critical data in the vault including unstructured files and databases. It then analyzes the data checking for corruption, file entropy, mass deletions/creations and uses machine learning algorithms to determine if a cyber attack occurred. When an anomaly or attack signature is detected, CyberSense forensic tools identify which files have potentially been corrupted, the user account associated with the attack, and the specific malware or executable file involved in the attack.

In addition to PowerProtect Cyber Recovery, Dell provides advisory and implementation services led by cyber recovery experts. These services are designed to help telecommunications operators create a cyber recovery strategy and processes based on industry best practices and in-depth knowledge. The goal of Dell's cyber recovery services is to identify which critical information needs to be recovered, map out a recovery process, and make improvements over time.

Conclusion

Moving to a cloud-native architecture is a daunting, but a necessary step for telecommunications operators. Fortunately, many enterprises around the world have already taken that step with leading technology partners such as Dell Technologies and Red Hat to guide them. By building their cloud-native network of the future on proven, industry-leading solutions from Red Hat and Dell, operators can accelerate the deployment of 5G services and reduce the risk of network migration.

Adopting a cloud-native architecture also means re-thinking security and resiliency for a disaggregated, container-based, and Kubernetes-orchestrated network. Dell Technologies is uniquely poised to help operators address this challenge through its data protection and Cyber Recovery solutions and services that have been integrated and validated with Red Hat's OpenShift container platform. The Dell-Red Hat joint solution delivers a complete cloud-native platform that includes the data protection, threat analysis, and disaster recovery that telecom operators require to deliver high availability and exceptional service agility.

To learn more about Dell EMC PowerProtect visit: http://delltechnologies.com/dataprotection

To learn more about Dell EMC PowerProtect Cyber Recovery visit: http://delltechnologies.com/cyberrecovery [ii]

[i] [1] Ransomware gang demands $7.5 million from Argentinian ISP, ZDnNet.com, https://www.zdnet.com/article/ransomware-gang-demands-7-5-million-from-argentinian-isp