



in

f



PowerFlex and PowerProtect: Keeping Your IT Kingdom Free of Ransomware

Wed, 13 Jul 2022 13:05:58 -0000 | Read Time: 0 minutes

Tony Foster

“To be, or not to be? That is the question.” Sadly, the answer for many organizations is “to be” the victim of ransomware. In 2020, the Internet Crime Complaint Center (IC3), a department of the FBI, received “2,474 complaints identified as ransomware with adjusted losses of over \$29.1 million” according to their annual report (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

These perspectives make it appear that no one is immune to ransomware.

However, if your organization is attacked, wouldn't you prefer to avoid both the attention and paying a ransom for your data?

The Dell PowerFlex Solutions Engineering team developed a white paper to help make this dream come true for PowerFlex customers. They worked jointly with the Dell PowerProtect team to create a design that illustrates how to integrate Dell PowerProtect Cyber Recovery with PowerFlex. See Ransomware Protection: Secure Your Data on Dell PowerFlex with Dell PowerProtect Cyber Recovery (<https://infohub.delltechnologies.com/t/ransomware-protection-secure-your-data-on-dell-powerflex-with-dell-powerprotect-cyber-recovery-1/>).

The white paper shows how to use the Cyber Recovery solution with PowerFlex to thwart ransomware and other malicious attacks, protecting your kingdom from would-be attackers. This protection is accomplished by creating an air-gapped vault that can be used with other data protection strategies to mitigate the actions of bad actors. This configuration is shown in the following architectural diagram:

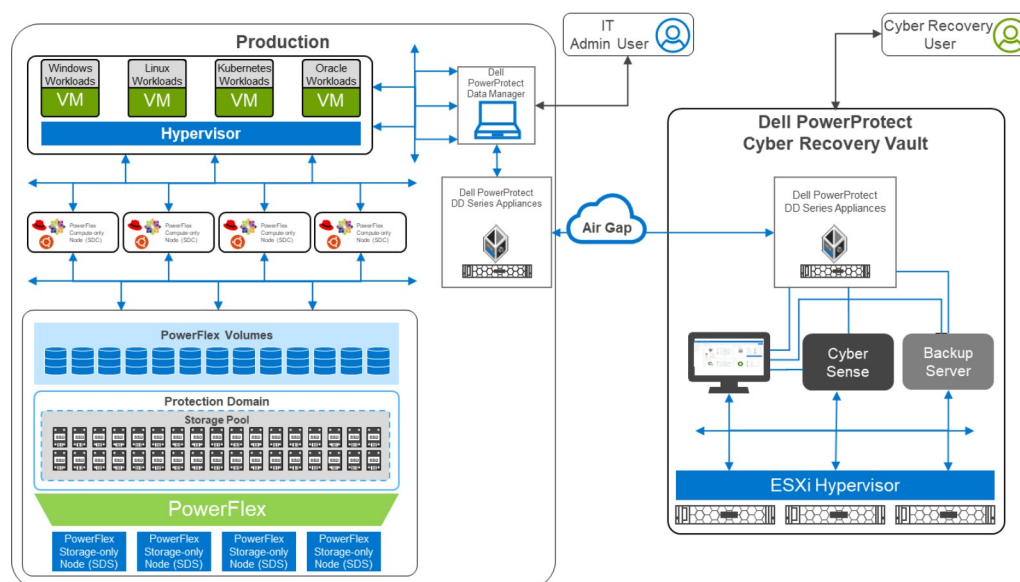


Figure 1: Architectural diagram

Air gaps and keeping the kingdom secure

The white paper describes a two-layer PowerFlex design in which the storage and compute environment are separate. The left side of the diagram shows the production environment. On the right side of the diagram, notice that there is a

tampering, such as encryption of volumes or a large number of deletions.

The logical air gap between the two environments is only opened to replicate data from the production environment to the Cyber Recovery vault. Also, the connection between the two environments is only activated from the Cyber Recovery vault. I like to think of this scenario as a moat surrounding a castle with a drawbridge. The only way to cross the moat is over the drawbridge. The drawbridge is controlled from the castle—a secure location that is hard to breach. Likewise, the air gap makes it very difficult for intruders.

Separation of powers

Notice that there are two different users shown in the diagram: an Admin User and a Cyber Recovery User. This difference is important because many attacks can originate within the organization either knowingly or unknowingly, such as a spear phishing attack that targets IT. The division of powers and responsibilities makes it more difficult for a bad actor to compromise both users and get the keys to the kingdom. Therefore, the bad actor has a nearly impossible challenge disrupting both the production environment and the Cyber Recovery environment.

Protecting the kingdom

Let's take a deeper look at the logical architecture used in the white paper. The design uses a pair of PowerProtect DD systems in which the data resides for both the production and vault sites. Replication between the two PowerProtect DD systems occurs over the logically air-gapped connection. Think of this replication of data as materials moving across the drawbridge to the castle. Material can arrive at the castle only when the gate house lowers the drawbridge.

The Cyber Recovery software is responsible for the synchronization of data and locking specified data copies. This software acts like the guards at the gate of the castle: they raise and lower the drawbridge and only allow so many carts into the castle at one time.

A backup server runs the Cyber Recovery software. The backup server supports various options to meet specific needs. Think of the backup server as the troops in a castle: there are the guards at the gate, archers on the walls, and all the other resources and activities that keep the castle safe. The type of troops varies

is responsible for detecting signs of corruption caused by ransomware and similar threats. It uses machine learning (ML) to analyze the backup copies stored in the vault PowerProtect DD to look for signs of corruption. CyberSense detects corruption with a confidence level of up to 99.5 percent. Think of CyberSense as the trusted advisor to the castle: alerting the appropriate teams when an attack is imminent and allowing the castle to defend against attacks.

Putting it all together

In the following animation, we see a high-level overview of how the environment operates under normal conditions, during a ransomware attack, and during recovery. It shows content being replicated into the Cyber Recovery vault from the PowerFlex environment. We then see a bad actor attempt to compromise the VMs in the PowerFlex environment. CyberSense detects the attack and notifies the Cyber Recovery administrators. The administrators can then work with the production team to secure and restore the environment, thwarting the bad actor and the attempt to hold the organization hostage.

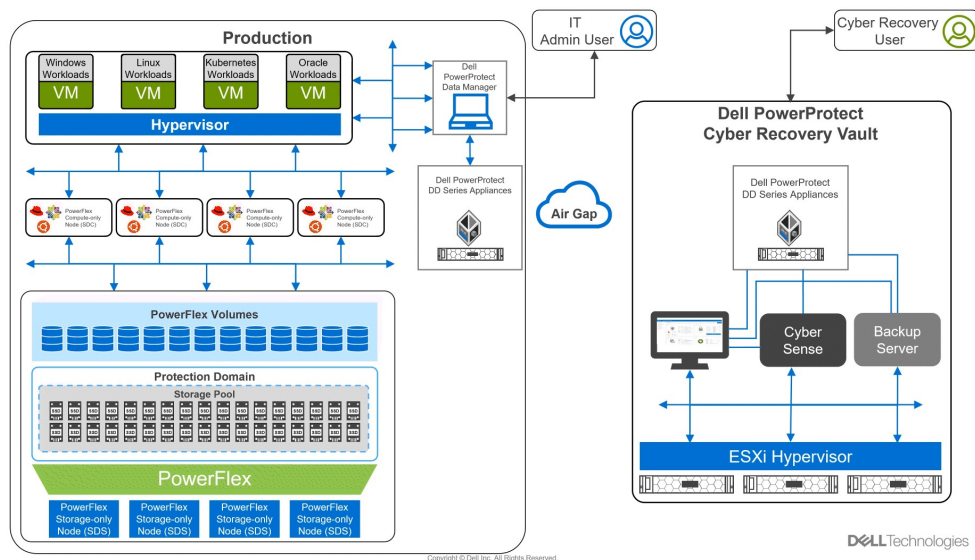


Figure 2: Animation of a ransomware attack and recovery

Beyond describing the architecture of this solution, the white paper shows how to deploy and configure both environments. Readers can take the next step towards building protection from a cyberattack.

The white paper is an excellent resource to learn more about protecting your

Twitter: @wonder_nerd (https://twitter.com/wonder_nerd)

LinkedIn (<https://linkedin.com/in/wondernerd/>)

Tags: Data Domain PowerFlex PowerProtect Cyber Recovery

Related Blog Posts



(/p/part-2-powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)

data protection PowerProtect PowerProtect Data Manager Cyber Recovery CyberSense

Part 2 – PowerProtect Cyber Recovery – Abilities and Improvements in the Cloud

(/p/part-2-powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)



Eli Persin

Mon, 24 Oct 2022 18:43:01 -0000 | Read Time: 0 minutes

(/p/part-2-powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)

In my previous blog (<https://infohub.delltechnologies.com/p/powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/>) I talked about the new abilities on the cloud for the PowerProtect Cyber Recovery 19.11 release, which also covered Cyber Recovery on Microsoft




(/p/powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)

cloud PowerProtect Cyber Recovery

PowerProtect Cyber Recovery – Abilities and Improvements in the Cloud

(/p/powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)

 Eli Persin

Mon, 20 Jun 2022 19:01:06 -0000 | Read Time: 0 minutes

(/p/powerprotect-cyber-recovery-abilities-and-improvements-in-the-cloud/)

As part of organizations' cloud journey, their presence in the cloud is increasing and they are running their development and production environment, or some of it, in the cloud.

Although running in the cloud has its own benefits, the need for cyber recovery abilities doesn't

logo

© 2023 Dell Inc. (<https://www.dell.com/learn/us/en/uscorp1/site-terms-of-use-copyright>)

[Privacy](https://www.dell.com/learn/us/en/uscorp1/policies-privacy) (<https://www.dell.com/learn/us/en/uscorp1/policies-privacy>)

[Terms Of Use](https://www.dell.com/learn/us/en/uscorp1/site-terms-of-use) (<https://www.dell.com/learn/us/en/uscorp1/site-terms-of-use>)

[Legal](https://www.dellemc.com/en-us/customer-services/product-warranty-and-service-descriptions.htm) (<https://www.dellemc.com/en-us/customer-services/product-warranty-and-service-descriptions.htm>)

[Anti-Slavery and Human Trafficking](https://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/dell-california-trafficking.pdf) (<https://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/dell-california-trafficking.pdf>)