Dell Wants to Make Enterprise Data More Resilient

A PUBLICATION FOR CLIENTS OF J.GOLD ASSOCIATES

"...With Dell's approach in creating a data protection appliance and enhancing its APEX offerings with a similar facility, it's providing a much needed capability that many companies have yet to implement. Yet the cost avoidance of a single data loss or accelerated recovery from a cyberattack can easily pay for the product, and potentially many times over...."

Most organizations have a very serious problem when it comes to data resiliency and preventing business disruptions due to data loss. In a recent Dell Technologies GDPI report, the average cost of a data loss was over $1M, which our research shows to be a very low estimate given the potential to reputational damage and business operations disruption such an event could cause an enterprise. Further, 63% of respondents were not confident that they could recover critical data after a cyberattack, while 67% said they were not confident that their existing data protection measures were sufficient to protect them from malware threats and ransonware attacks, even as 48% said they have had a cyberattack in the past 12 months that prevented them from using their data.

None of these statistics should be surprising given the high exposure attacks that have taken place over the past few years. What is surprising is that so few enterprises have confidence in their own data security measures. Given this troubling trend, Dell wants to create a compelling data protection capability for organizations that's easily deployed and robust, but also affordable. As part of their APEX family of products, Dell Data Protection provides a multi-cloud (public and private) approach, including into and from the cloud backup, disaster recovery, long term data retention and cyberattack recovery, while supporting modern workloads (e.g., containers, Kubernetes, SaaS, etc.). Indeed, Dell claims that it already protects 14 Exabytes of public cloud data for more than 1700 customers.

Dell is offering the PowerProtect Data Manager Appliance for data protection and resiliency that removes much of the burden that companies have in deploying such services. Dell claims it can be deployed in under 30 minutes, offers 12TB - 96TB of storage, has VMware integrated and is cloud ready and cyber recovery ready. While this initial device is aimed at the mid-tier, we expect larger systems to be available shortly that can handle more expansive enterprise needs. Dell is also announcing a Cyber Recovery Vault that will run in Google Cloud (it already provides such capability in AWS and Azure), which can be acquired through the normal cloud marketplace that enables customers to install features needed for their deployments as part of their existing cloud agreement.

Although we expect most of the installations for Dell PowerProtect's 1300 customers are on-prem, the popularity of moving workloads to the cloud is a growing capability that Dell can exploit. Indeed, with Dell's leading APEX technologies as a service offerings, this is a logical fit for the data storage

services that are critical to enterprise resiliency and recovery to counter the increasing numbers of attacks. One of the major stumbling blocks for many companies that haven't fully deployed data protection capabilities is the complexity of building out this capability, often requiring specialized expertise and products from multiple vendors to support multiple systems/solutions. And even in the cloud where most hyperscalers offer a data protection service, they are not great at providing a multi-cloud capability that is becoming a prevalent use case in many enterprises. Bringing this flexible consumption capability with cross-cloud capability to customers is a key strength of the Dell offering. And Dell is so confident in its approach that it offers a $10M Cyber Recovery guarantee.

But moving customers to the new products may not be as straight forward as we'd like to see. Dell is offering migration tools that can move policies and agents to the new environment. This is useful for previous generation products, but their focus is on existing older Dell solutions. Creating migration tools for other vendors' products and/or public cloud solutions is a future item for them. That's not necessarily a bad approach, as there are plenty of older technology Dell customers that can be migrated. But it is somewhat limiting in the needs of enterprises wishing to simplify and consolidate their approach.

Data resiliency after a cyberattck is a major value added capability that companies who have been attacked can benefit from financially in nearly eliminating downtime that could be weeks or months and cause a great deal of lost revenues and/or operations shut downs, not to mention the ability to forgo any ransomware payments to get the data recovered. It's difficult for companies to discuss the successes they have had with preventing ransomware, as many affected organizations do not want to make their challenges public. But Dell did provide one example of how their systems helped. A public school district in CA was attacked by ransomware twice - once before they had Dell protection and once after. Before implementing the Dell protection tech, it took weeks and months to come recover all their systems. After they implemented Dell cyber recovery capability, they were able to bring the systems back up in hours after the attack.

Bottom Line: With Dell's approach in creating a data protection appliance and enhancing its APEX offerings with a similar facility, it's providing a much needed capability that many companies have yet to implement. Yet the cost avoidance of a single data loss or accelerated recovery from a cyberattack can easily pay for the product, and potentially many times over. Enterprises that don't already have such data resiliency capabilities in place should look at deploying a product like Dell is offering in order to proactively prevent data disasters. Failure to do so will open organizations to costly and operationally disastrous situations that could otherwise be easily avoided.

"…Enterprises that don't already have such data resiliency capabilities in place should look at deploying a product like Dell is offering in order to proactively prevent data disasters. Failure to do so will open organizations to costly and operationally disastrous situations that could otherwise be easily avoided...."

J.Gold Associates, LLC.
6 Valentine Road
Northborough, MA 01532 USA

Phone:
+1-508-393-5294

Web:
www.jgoldassociates.com

Email:
info@jgoldassociates.com

Research, Analysis, Strategy, Insight