IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Dell Technologies Introduces AI Workload Safeguarding

May 30, 2024

By: Phil Goodwin

IDC's Quick Take

Seemingly every IT infrastructure supplier is hyping their AI solutions, but a few suppliers seem to have thought through the data and workload safeguarding implications. During the recent Dell Technologies World 2024 event, Dell announced its data protection solution for these unique workloads that appears to be comprehensive and giving the company an early-mover advantage.

Event Highlights

Dell Technologies World held in Las Vegas, Nevada, May 20–23, 2024, contained plenty of AI-related content. Dell announced enhancements to its Dell AI Factory, including new servers and AI orchestration software. While not garnering as much attention, the company's announcement regarding AI data and workload protection is a significant advancement in this area that will be essential in the AI era.

IDC's Point of View

In numerous IT infrastructure trade shows over recent months, there has been no shortage of AI announcements. Few, however, seem to have thought through the data and workload protection requirements. Some have defaulted to back up AI data alone as their strategy, but we find this to be insufficient. Moreover, our research indicates that a few IT organizations have given sufficient to AI system protection.

Protecting AI workloads involves much more than just protecting data. Considerations include:

- **Workload state** – Similar to containers, state matters in AI workloads, particularly learning modules (LMs). Indeed, many AI workloads are container based. Because the LM is accepting data potentially from various data feeds, restoring data to a prior point will miss subsequent data from the feeds unless that feeding data is also captured.
- **System protection** – Protecting the AI model itself is equally important to protecting the data. Models can become corrupted due to error or malicious intent, requiring the model to be restored to a prior state.
- **Compliance** – Because LMs are built from various data feeds, two compliance issues arise. First, PII, HIPAA, and other confidential data must be protected from disclosure, including in backup copies where the data must be masked or encrypted. Second, organizations may be compelled to prove chain of custody for copyrighted material was not included in the LM. Backed up systems and data may be critical in this effort.
- **Malicious data injection** – Cyber-attackers may seek to inject erroneous data into LM such that they yield incorrect results and demand a ransom for the code to remove such data. Granular data recovery may be required to identify and remove malicious data. It also requires that cyber-recovery steps regarding clean room recovery and air-gap protections be implemented.

To address the four use cases, Dell has announced its reference design for AI data protection. This design is based on the Dell Scalable Architecture for retrieval augmented generation (RAG) with NVIDIA microservices and is part of the Dell AI Factory. It can be implemented using Dell's portfolio of data protection software and purpose-built backup appliances.

AI implementation and models are evolving so rapidly that it is very difficult to predict precise workload protection requirements 12-36 months from now. Thus it is possible that some of Dell's moves today will need a course correction in the future. However, we believe that as an early mover in AI protection as part of the larger Dell AI Factory, Dell is well positioned to navigate these changes. With a combination of services and technology, Dell can proactively guide customers to address issues they have not fully considered before suffering undesirable consequences.

Subscriptions Covered:
Cloud Data Logistics and Protection