Organisations turn to Zero Trust to modernise cybersecurity programmes

Issued by Dell Technologies South Africa

10 Jul 2023

Organisations are turning to Zero Trust to modernise their cybersecurity programmes and keep pace with an evolving attack landscape. But determining where to start, the capabilities to prioritise and the actions needed to progress towards maturity can be complicated.

Doug Woolley, general manager at Dell Technologies South Africa

Doug Woolley, general manager, Dell Technologies South Africa, said: "Security and IT leaders need help planning their strategy and implementing the tools to support it. To address this requirement, Dell Technologies has introduced Project Fort Zero to provide an end-to-end Zero Trust security solution for global organisations to protect against cyberattacks. It delivers a repeatable blueprint for an end-to-end solution that is based on a validated reference architecture recognised around the world – that of the US Department of Defence."

Project Fort Zero builds on the momentum of Dell's Zero Trust Centre of Excellence and partner ecosystem to accelerate Zero Trust adoption. Leading an ecosystem of more than 30 leading technology companies, Dell will deliver a validated, advanced maturity Zero Trust solution within the next 12 months.

"Zero Trust is designed for decentralised environments, but integrating it across hundreds of point products from dozens of vendors is complex – making it out of reach for most organisations," Woolley said. "We're helping South African organisations solve today's security challenges by easing integration and accelerating adoption of Zero Trust."

The fully configured Project Fort Zero solution will lower the barrier to Zero Trust adoption. Dell will take on the technology integration and orchestration that typically falls to individual organisations across several vendors. In doing so, the estimated time for advanced Zero Trust adoption is reduced through a private cloud. As a result, the end-to-end solution will help public and private sector organisations adapt and respond to cybersecurity risks while offering the highest level of protection.

Project Fort Zero serves a variety of use cases including:

- **In on-premises data centres** for organisations where data security and compliance are paramount.
- **In remote or regional locations** like retail stores where secure, real-time analysis of customer data can deliver a competitive advantage.
- **In the field** where a temporary implementation is needed for operational continuity in places with intermittent connectivity such as airplanes and vehicles.

Along with Project Fort Zero, Dell is expanding its security portfolio with Product Success Accelerator (PSX) for Backup, a new service to help organisations protect and recover data in the event of disruption.

PSX for Backup simplifies the implementation and maintenance of backup environments to enable data recovery. PSX for Backup follows the recent release of PSX for Cyber Recovery, which implements and helps operationalise an isolated cyber recovery vault. The isolated cyber recovery vault is intended to be a finality control that delivers assured

recoverability after a cyber attack by ensuring that suspicious data copies (of backups) are identified in time. Organisations leverage cyber recovery vault from Dell Technologies based on some of the most stringent requirements from the Sheltered Harbor Alliance (an American non-profit that was created by the US Federal Reserve and more than 30 participant banks, to deal with best practices related to cyber security and recoverability). Dell's isolated cyber recovery vault is endorsed by the Sheltered Harbor Alliance, and South African entities can benefit from this critical data recovery control, in order to meet their survival time objective.

Organisations can choose from three levels of backup or cyber recovery based on their needs:

- **Ready** includes planning workshops, configuration of a validated backup or vault environment, a success plan, a runbook and outcome-based skills training.
- **Optimise** adds quarterly assessments, improvement recommendations and assisted restore test simulations.
- **Operate** adds ongoing operational assistance to meet the solution's performance objectives. Highly skilled experts monitor and investigate alerts, initiate corrective actions and help with restore tasks at the customer's direction.