DELL Technologies

DERIVE TECHNOLOGIES

Solution Brief

Protecting DNA Sequencing Data From Cyber Attacks

PowerScale Cyber Protection Helps Keep Next-Generation Sequencing Data Safe

Helping Keep Data Protected

- Dell PowerScale is a trusted platform in next-gernation sequencing environments
- PowerScale has built in data security features that help protect data
- Superna, a trusted Dell Technologies partner can help protect data from ransomware attacks
- Superna Eyeglass® Ransomware Defender leverages PowerScale's built in snapshot, API's and replication technology to protect the data
- Superna Eyeglass® Ransomware Defender assists before, during and after a cyber-attack providing assistance throughout an incident
- Superna's Eyeglass® Ransomware Defender protects data in place and offers investment protection with integrated Airgap automation features
- Enable a disaster recovery site and/or the AirGap cluster to be located off-prem or in the cloud.

Genomic Data Comes Under Attack

Hospitals, research facilities, pharmaceutical companies and laboratories have all invested in the use of next-generation sequencing (NGS) as a method of genomic analysis to accelerate discoveries and advance personalized patient care. A few of the challenges that arise with NGS is the need for a high-performance compute environment that can keep up with the workflow and reliable and performant data storage for the massive of amounts of data being generated and analyzed. However, a new challenge is now on the horizon for these institutions with the ongoing battle against cyber criminals, keeping this data safe from a cyber attack.

In June 2022, the U.S. Food and Drug Administration (FDA) issued a warning to healthcare institutions and laboratories of a potential cyber threat to DNA sequencing software that could target personal patient data. Luckily, software patches and updates were sent out at a rapid pace to help close this vulnerability, but the threat of an attack still exists as they do in all industries[1]. In healthcare specifically, phishing, ransomware, and cyberfraud have been on the rise with over 28% of cyber attacks being ransomware[2]. Compaines and care facilities that deal with patient data need to develop strategies and leverage technoloy to keep their data protected and operations up and running.

Dell PowerScale has long been trusted as the data storage platform for NGS environments, but it can also help keep your data protected from cyber attacks.

Secure Next-Generation Sequencing with PowerScale

Dell PowerScale is a scale-out, network attached storage system that provides Life Sciences organizations with a simple and proven solution. PowerScale solutions provide secure ultra-high storage capacity and processing performance for all scales of genomic data.

Behind PowerScale is Dell PowerScale OneFS operating system that offers many features and functionalities that are imperative to successful healthcare institutions. PowerScale with OneFS offers native security features built directly into the platform. PowerScale supports data at rest encryption (D@RE) with self-encrypting drives, snapshots with SnapshotIQ and data replication with SyncIQ. These features alone offer institutions piece-of-mind when it comes to data security, but for ransomware, protection can be taken one step further.

Derive Technologies is a Minority-Owned Business Enterprise (MBE) and a brand-agnostic full-service IT integrator aligned with best-of-breed technology to optimize and empower your IT environment.

Contact Us

www.derivetech.com
(212) 263-1111
info@derivetech.com
40 Wall Street, 20th Floor, New York, NY 10005

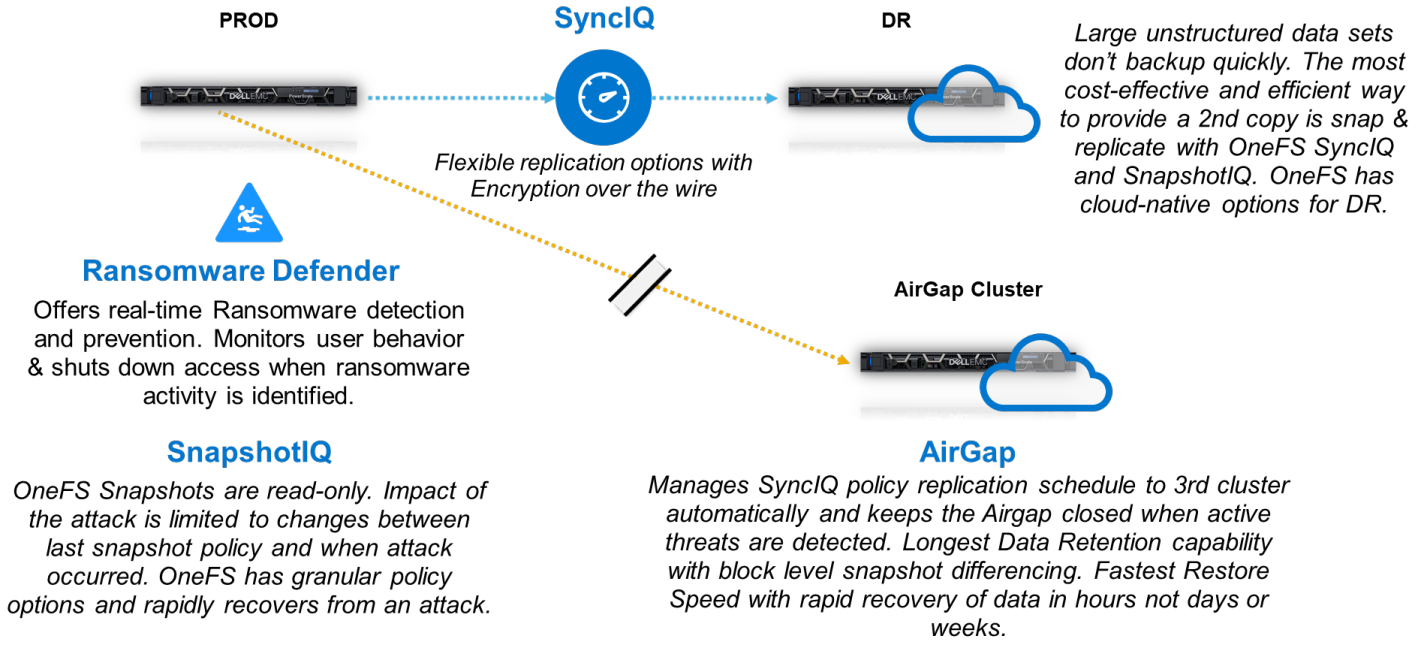
Superna Eyeglass® Ransomware Defender

Superna Eyeglass® Ransomware Defender is a highly scalable, real-time event processing solution that employs user behavior analytics to detect and halt a ransomware attack. By monitoring user file system accesses, Ransomware Defender detects changes to users' normal data access patterns; when administrator-defined thresholds are met, Ransomware Defender can take defensive action to prevent major damage and minimize the recovery time. If Ransomware Defender detects ransomware attack behavior it initiates multiple defensive actions, including locking users from file shares—either in real-time or delayed. There are also timed Auto Lockout rules such that action is taken even if an administrator is not available, as well automatic response escalation if multiple infections are detected in parallel. Deployment is simplified with a Learning mode that can automatically configure itself based on work load monitoring of any environment.

Ransomware Defender integrates AirGap Cyber Vault capabilities with the ability to suspend data copy operations automatically when the source data is under threat. This offers the industry's fastest rapid recover mode eliminating days and weeks of restoring data from the vault devices that would be experienced by typical backup solutions. Superna's Rapid Recovery allows the offline data to be usable in < 2 hours regardless of the size of the data set protected. For more information on this offering from Superna is available here.

How It All Works

The graphic below highlights a reference architecture for a Ransomware Defender deployment with PowerScale for NGS Data.



[1] Baxter, Amy. "FDA issues a cybersecurity warning: DNA sequencing software is vulnerable to attacks." HealthExec, 03 June, 2022, https://healthexec.com/topics/health-it/cybersecurity/fda-warns-dna-software-cybersecurity-exploitation?utm_source=newsletter&utm_medium=he_health_it

[2] IDC White Paper, sponsored by Dell Technologies, Establishing Uncompromising Data Availability for Healthcare Organizations, doc #US47447321, February 2021