DELL Technologies

DERIVE TECHNOLOGIES

Solution Brief

Protecting Your Patient's Medical Images

Superna Eyeglass® Ransomware Defender Helps Keep Medical Images Safe from Cyber Criminals

Keeping Patient Data Safe

- Dell EMC PowerScale is a trusted platform in healthcare for the storage and archiving of medical images
- PowerScale has built in data security features that help protect patient 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
- Faction Services on Dell EMC PowerScale enable the disaster recovery site and/or the AirGap cluster to be located off-prem or in the cloud.

Patient Information is Under Attack

Healthcare is undergoing a data explosion. According to IDC, healthcare data will soon reach the 4ZB level and will exceed 10ZB by 2025. Even though healthcare institutions manage less than the industry average, they must retain 25% longer[1]. This means that all patient information including images and scans in the PACS or VNA must be stored and protected from cyber criminals.

Recently, the healthcare industry has come under attack as criminals have found unique ways to target healthcare providers with phishing, cyberfraud, or ransomware attacks that put the entire institution and its data at risk. These types of attacks have been on the rise since 2020 with 28% of these attacks being filed as ransomware[2]. However, a recent IDC survey suggests that only 60% of healthcare organizations felt as though they were prepared to handle the increase in data and the security requirements around it[1]. With more and more medical images being managed by PACS, such as whole slide images and bed-side ultrasounds, it's never been more important to keep this data protected.

Cyber attacks lead to downtime, damaged reputations, and a drop in quality of care delivered.

Medical Imaging Lives on PowerScale

PACS or VNA environments need unstructured data storage that offers performance, scalability, and protection in an easy to manage platform. PowerScale is scale-out network attached storage (NAS) that functions as a single file system across clusters. This allows for data to be accessible across the file system. Behind PowerScale is Dell EMC PowerScale OneFS operating system that offers many features and functionalities that are imperative to successful healthcare institutions. You can read more about PowerScale for Medical Imaging here.

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 healthcare institutions piece-of-mind when it comes to data protection, but for ransomware, you need to protect data beyond this.

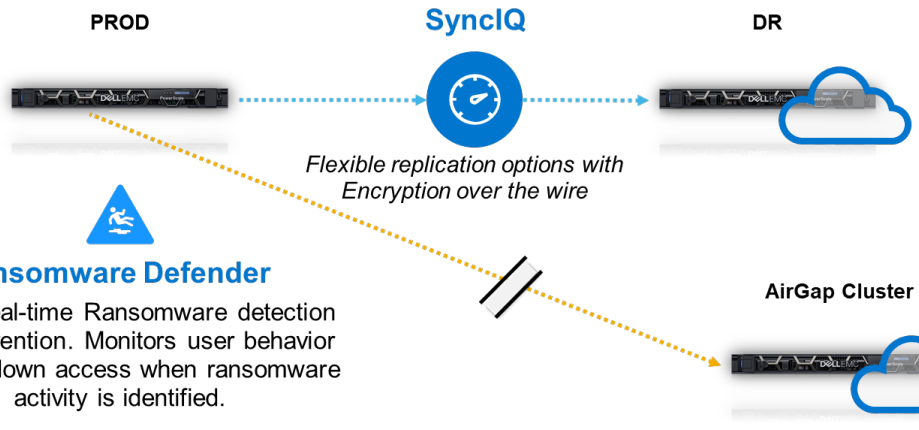
Superna Eyeglass® Ransomware Defender

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 medical imaging. With Faction Services on Dell EMC PowerScale, the DR site and/or the AirGap cluster can be in the cloud.



Large unstructured data sets don't backup quickly. The most cost-effective and efficient way to provide a 2nd copy is snap & replicate with OneFS SyncIQ and SnapshotIQ. OneFS has cloud-native options for DR.

SnapshotIQ

OneFS Snapshots are read-only. Impact of the attack is limited to changes between last snapshot policy and when attack occurred. OneFS has granular policy options and rapidly recovers from an attack.

AirGap

Manages SyncIQ policy replication schedule to 3rd cluster automatically and keeps the Airgap closed when active threats are detected. Longest Data Retention capability with block level snapshot differencing. Fastest Restore Speed with rapid recovery of data in hours not days or weeks.

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

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

[2] Davis, Jessica. "Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware." HealthITSecurity, HealthITSecurity, 25 Feb. 2021, healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware.