# RANSOMWARE PROTECTION FROM SUPERNA & DELL EMC

## Ransomware protection for Isilon users

### ESSENTIALS

- Dell EMC Isilon provides a robust suite of features to ensure data protection and regulatory compliance.
- Superna enhances these capabilities with Eyeglass and Ransomware Defender
- Ransomware Defender is an add-on product to Superna Eyeglass® and provides an affordable, easy and powerful method to protect from ransomware attacks
- Superna can detect suspicious behavior, alert data administrators and automatic defensive action locks out the affected user from accessing all Isilon data
- Superna's planned integration with Isilon SnapshotIQ™ can offer proactive restore point as close to ground zero of an attack, with an automated snapshot feature. This will minimize the impact and accelerate the recovery process.

### RANSOMWARE DEFENDER TO DETECT AND PREVENT

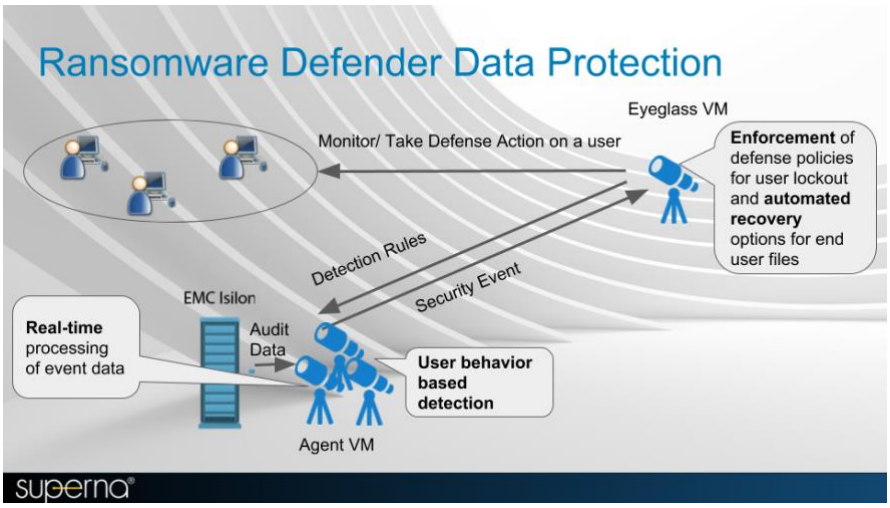
The increasing number of high profile and extremely wide spread ransomware attacks has elevated protection from this new threat to the highest executive level of most businesses. CEOs, CIOs and CSOs understand that a successful attack on their business could cost them an extremely large sum of money to just regain access to their data—and that's not to mention all of the other costs that could potentially put their entire business at risk.

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.

Superna Ransomware Defender for Isilon provides your business with numerous important benefits, including:

- Measurable return on investment—potentially millions in revenue considering the high cost per minute of unplanned downtime
- Scalability—Ransomware Defender is built on big data technologies that operate at scale using the compute and storage node concept. Integration with Isilon Access Zones and HDFS features enables user behavior analytics data to be stored on Isilon.
- Enterprise Security Administration—Role Based Access Control feature allows Eyeglass administrators to assign a Ransomware role using Isilon Authentication providers and Active Directory groups to manage and monitor Ransomware Defender security settings and incidents separately from DR monitoring.




## ISILON SOLUTIONS FOR RANSOMWARE ATTACK RECOVERY

Isilon has a number of features that work with Superna products to help protect against ransomware attacks. In addition to the auditing feature that Superna utilizes, Isilon has File Blocking capability which prevents unwanted or illegal content from being placed on the cluster in the first place. Even more important is Isilon SnapShotIQ, which maintains a "clean" copy of your data—ideally at a remote site.

The process is straightforward:

- Create Snapshot Copy of the data at the primary site
- Enable Eyeglass File System protection job to detect new Snapshots on SyncIQ protected paths.
- Superna Eyeglass will auto detect existing or new Snapshot schedules and replicate them to the secondary site with no administrator actions required.
- Multiple recovery points are now available at the primary site and secondary site with no administrator actions required.
- Managed and monitored from a single pane of glass, SyncIQ and Snapshots are monitored to ensure they are fully in sync at both sites at all times.

Superna Eyeglass® Ransomware Defender also identifies the files that tripped the threat detector and the previous 1 hour of files accessed by the user. This helps build a profile of the exact files that require remediation and recovery from the attack. To be prepared for a ransomware attack, make sure client machine Anti-virus scanning is enabled and that regular backups are being created. Also establish and enable well-designed snapshot policies and snapshot retention policies to proved multiple recovery points should an attack occur. A planned feature in Ransomware defender will create a Snapshot at the SMB Share entry point of the attack as a secondary action to provide the best possible recovery point as close to the initial attack. This also ensures secondary user infections benefit from this Snapshot recover on the same SMB share.

If an attack does occur the obvious first step is to stop the attack. Superna Eyeglass® Ransomware Defender can execute commands to stop the attack in progress on all managed clusters, not just the cluster the user infection was initially detected. Next, the auditing features of Ransomware Defender isolate where the attacks are coming from (user IP address, and AD login credentials) and exactly which files were affected and when. If necessary, restore the active data sets back to a pre-attack state from the saved Snapshots.

## SUMMARY

Dell EMC Isilon and Superna Eyeglass® Ransomware Defender help keep your data protected from insider threats and ransomware. Ransomware Defender is available as

an add-on to Superna's Eyeglass®—trusted and widely used file system synchronization technology available for Dell EMC Isilon systems.

## CONTACT US

To learn more, contact your local representative or authorized reseller.