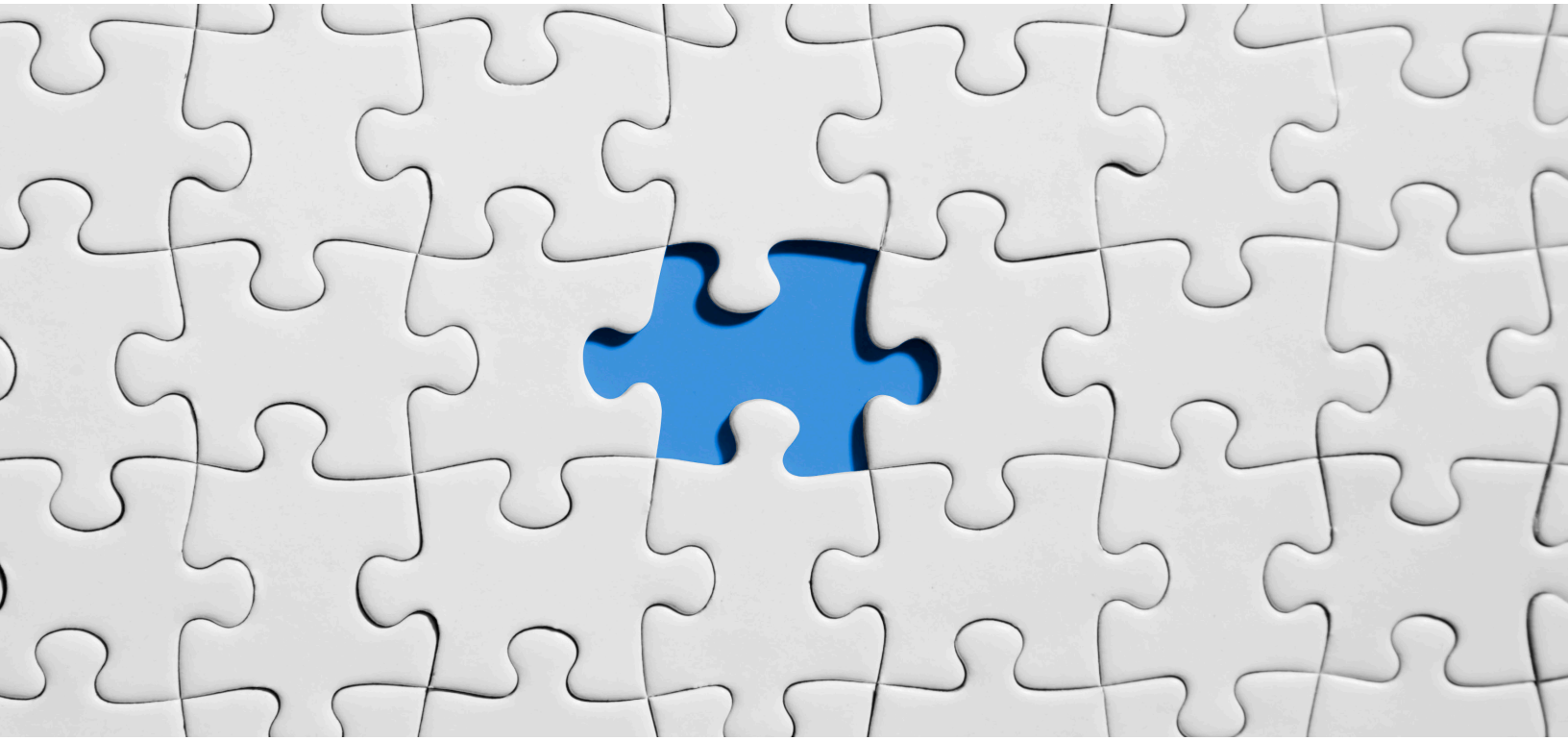
DELL Technologies

DELL EMC POWERSCALE WITH SUPERNA FOR HEALTHCARE



Sai Ganesh

Sales Engineer Analyst

Dell Technologies

Sai.ganesh@dell.com

Akshay U

Associate Sales Engineer Analyst

Dell Technologies

Akshay_u@Dell.com

Nidhi Shree

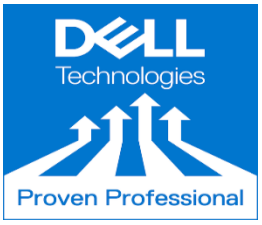
Associate Sales Engineer Analyst

Dell Technologies

Nidhishreen.shreen@dell.com

Knowledge Sharing Article

DELL Technologies Proven Professional



The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

Table of Contents

Abstract

Those who want to stay at the forefront of progress in technology must adapt and modernize. Both consumers and businesses are embracing emerging technologies. Regardless of the vertical, data drives today's industries. Healthcare is one of those important, competitive sectors that continuously require creativity and improvement in its results, efficiency and usability.

Due to the COVID-19 pandemic, the healthcare sector worldwide has experienced a dramatic shift to deal with new challenges, broadening the scope of technology-driven healthcare solutions significantly. Technologies such as AI/ML, AR/VR, Telemedicine, Internet of Medical Things (IoMT), Blockchain, etc., have become significant tools to help healthcare providers and organizations operate more effectively.

As organizations become increasingly dependent on data, the modern threat of cyberattacks, and the importance of data security, availability and integrity protection demand modern and proven technologies and techniques to secure sensitive mission-critical operations. Cyber Threat is defined as the possibility of a malicious attempt to damage or disrupt a computer network or system. This definition is incomplete without including the attempt to access files and infiltrate or steal data. Some of the most common types of cyberattacks include Ransomware, Malware, Phishing, Denial-of-Service (DOS) attack, and social engineered Trojans to name a few. As a result, IT security/Cybersecurity has become an integral part of the digital strategy of organizations.

Ransomware is a type of malware that threatens to publish or block access to data or a system, more commonly by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, these ransoms usually come with a deadline. If the victim does not pay in time the data that has been encrypted is gone forever. In the USA, ransomware attackers target healthcare more than any other industry sector, recognizing that by taking hostage critical applications and patient data hostage that can put lives at risk, health care institutions are likelier to quickly pay a ransom.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and U.S. Department of Health and Human Services (HHS) have credible information of increased and imminent ransomware attacks against healthcare providers. CISA, FBI, and HHS have released AA20-302A Ransomware Activity Targeting the Healthcare and Public Health Sector that details both the threat and practices that healthcare organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats.

Data center security refers to the physical practices and virtual technologies used to protect a data center from external threats and attacks. Because data centers hold sensitive or proprietary information, such as customer data or intellectual property, sites must be both digitally and physically secured. Security can be divided into physical and software security. Physical security encompasses a wide range of processes and strategies used to prevent outside interference. Software or virtual security prevents cybercriminals from entering the network by bypassing the firewall, cracking passwords, or through other loopholes.

Dell EMC PowerScale provides healthcare organizations an easy-to-manage, unified storage system that can span multiple operating platforms and locations. It can scale quickly to manage growth without sacrificing performance or data protection, unlocking a customer’s Data Capital. We will look into Dell EMC PowerScale’s layered Cyber Security approach for data protection which includes:

- Employing data protection best practices
- Data Hardening and PowerScale protection features
- Dell EMC Advanced Protection concepts such as Isolated Recovery, etc.

Dell EMC PowerScale and Superna Eyeglass Suite together offer a complete solution for managing and protecting data at scale covering an organization's current and future data management challenges. This article helps in understanding the anatomy of ransomware attacks and explores how Superna offerings such as Ransomware Defender and Eyeglass Easy Auditor complement Dell EMC PowerScale solutions available today to defend against such attacks.

Introduction

Cybersecurity in healthcare is a growing problem. Hacking and IT security breaches have gradually increased over the past three years, and many healthcare organizations have failed to protect their data from cyber-attacks. The proliferation of IoT devices in the healthcare industry has led to healthcare providers securing more connected medical devices than ever before. Cybercriminals are now developing more sophisticated and complex techniques to attack the healthcare sector.

Every healthcare organization handles and stores patient's personally identifiable information (PII) and protected health information (PHI) in one or more health information systems. They are also expected to store this data for a specific period due to governance policies. IoT-connected devices starting from the complex laboratory and surgical equipment to the hospital's medical billing software which deals with the patient's insurance and financial information are all open to attack once the organization's network security perimeter is breached. Protecting a patient's PII and PHI is the prime area of focus for healthcare organizations.

The global pandemic places healthcare systems under constant strain. Healthcare facilities around the world have also been hit by a wave of cyberattacks, including ransomware attacks. Below are some of the common types of cyberattacks.

Types of Cyberattacks

- **Denial-of-service attack**
  Distributed Denial of service (DDoS) attack is an attempt made by the hacker to block access to a server or a website that is connected to the Internet. A DOS attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth, making the system incapable of responding to any query.
- **Phishing**
  Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, etc. by impersonating oneself as a reputable source, usually through email.
- **Insider threat**
  An insider threat is a security risk to an organization that comes from within the business itself. It may originate with current or former employees, usually by compromising the internal network with viruses, Trojan horses, malware, etc.
- **Trojan horses**
  A Trojan horse is a program designed to perform legitimate tasks in the frontend, while also performing unknown or unwanted tasks in the backend. It can also let many viruses and worms install onto the network devices and compromise the system.
- **Malware**
  Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.
- **Ransomware**
  Ransomware is a type of malware that threatens to publish or block access to data or a system, more commonly by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, these ransoms usually come with a deadline. If the victim does not pay in time the data

that has been encrypted is gone forever. Since every device and activity is connected and controlled by IoT, ransomware blocks access to these devices and databases. This can paralyze hospital activity, i.e. patients cannot be admitted nor discharged, and most importantly the hospital system has no access to patient data. Ransomware attackers target healthcare more than any other industry sector because the attackers hold the critical application and patient data hostage which can put lives at risk. It is likely that healthcare institutions would rather pay the ransom than compromise their patients. Ransomware attacks have seen a sharp rise this year and hospitals have been particularly vulnerable since the start of COVID-19.

Common types of Ransomware

Ransomware attacks date back to 1989 when the “Aids Info Disk” or “PC Cyborg Trojan” was used to extort money from recipients of the malware. Emsisoft, a New Zealand-based cybersecurity firm, stated in its latest report that the healthcare industry, government, federal and education sector have been a target of at least 2,354 ransomware attacks in 2020. The CISA, FBI, HHS have credible information of increased and imminent ransomware attacks against healthcare providers. These agencies have released AA20-302A Ransomware Activity Targeting the Healthcare and Public Health Sector that details both the threat and practices that healthcare organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats. Below are some of the common types of Ransomware targeted towards the healthcare sector:

- **Ryuk**
  Ryuk ransomware wreaked havoc throughout 2020, reportedly responsible for more than a third of all ransomware attacks in 2020. Used in attacks targeting companies, hospitals, and government municipalities, Ryuk is used where the attackers make sure that business-critical files are encrypted so they can ask for large ransom amounts. Ryuk uses AES-256 to encrypt files and an RSA public key to encrypt the AES key. It then attempts to delete all backup files, preventing the victim from recovering encrypted files without the decryption key.

  Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider was one of the recent victims of Ryuk. It had to shut down its health care facility systems across the US after the attack. They had no access to anything computer-based including old labs and PACS radiology system. During the cyberattack, files were being renamed to include the “ .ryk ” extension and the impacted computers' screens changed to display a ransom note reading "Shadow of the Universe,"

- **WannaCry**
  The WannaCry ransomware attack was a global cyberattack (2017) by the WannaCry ransomware cryptoworm, which targeted Windows machines through a Microsoft exploit known as EternalBlue. The Windows machines were encrypted, and a ransom was demanded in Bitcoin cryptocurrency. The ransomware hit over 125,000 organizations in over 150 countries. According to a research report from Armis, WannaCry continues to be an active threat to 40% of healthcare organizations.

NHS trusts were left vulnerable in a major ransomware attack in May 2017. More than a third of trusts in England were blocked by the WannaCry ransomware, according to the National Audit Office (NAO). At least 6,900 NHS appointments were cancelled due to the attack. The malware encrypted data on infected computers and demanded a ransom roughly equivalent to £230 ($300).

- **Egregor**
  Egregor is one of the most rapidly growing ransomware families. The FBI has issued a Private Industry Alert about the growing threat of Egregor ransomware attacks. Egregor ransomware is a ransomware-as-a-service operation that was first identified in September 2020. The attackers behind the operation recruit affiliates to distribute their ransomware and give them a portion of any ransoms they generate.

  GBMC Healthcare in Maryland was attacked by Egregor in early December 2020. The malware infected its IT systems, forcing many GBMC systems offline.

- **SamSam**
  After getting hit by the SamSam ransomware in March 2018, Atlanta, Georgia, spent more than $5 million rebuilding its computer network, including nearly $3 million hiring emergency consultants and crisis managers.

Ransomware Defense Best Practices

- **Be aware of cyber-attacks affecting your industry**
  Threat intelligence is the practice of gathering, analyzing, and utilizing data from previous cyber-attacks to gain knowledge on prevention and mitigation tactics. Threat intelligence sharing enables organizations to understand attack patterns and prevent similar attacks from occurring. Below are two examples of automated threat intelligence feeds recommended by the Public Health Council:
  - **CISA's Automated Indicator Sharing**
    This automated indicator sharing (AIS) system enables real-time exchange of information regarding evolving cyber threats between the federal government and private sector organizations.
  - **Health Information Sharing and Analysis Center**
    The Health Information Sharing and Analysis Center (H-ISAC) is a global, non-profit organization offering healthcare organizations a free cyber threat intelligence sharing platform for H-ISAC community members. H-ISAC provides automated threat intelligence sharing from numerous internal and external sources.

- **Discover the vulnerabilities in your organization**
  When you know the cyber risks that could impact your organization, you need to figure out how vulnerable your organization is to those threats. Cyber Protection and Privacy Laws differ depending on the type of organization. To protect PHI, the healthcare industry follows security compliance regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Below are a few examples of cyber defense assessments.

- **Vulnerability assessment**
  - Understanding your vulnerabilities is a vital first step to identifying the gaps in your security protection.
- **Security risk assessment**
  - Have a third-party expert perform an annual security risk assessment that meets HIPAA requirements.
- **Penetration testing**
  - Install and configure anti-malware defenses in your environment correctly and ensure that the software is up to date.

- **Secure potential attack vectors to improve your security**
  Once a weakness is found, it is important to fix the vulnerability and incorporate cyber defense measures to prevent potential attacks. There are many cybersecurity products that can reduce the risk of a cyber-attack; below are a few:
  - **Backup and Disaster Recovery**
    Backup copies enable data to be restored from an earlier point in time to help the business recover from an attack.
  - **Endpoint Detection and Response**
    Organizations should invest in a strong endpoint detection and response (EDR) platform to secure their end devices.
  - **Mobile Device Management**
    Mobile Device Management (MDM) solutions enable security teams to lock down USB ports on remote laptops, preventing data to be moved to an external drive and beyond the security bubble.
  - **Provide Employee Cybersecurity Training**
    Conduct regular security awareness training and emphasize vulnerabilities, such as phishing schemes, the importance of strong password policies, etc.

Dell EMC PowerScale for Healthcare

Healthcare organizations are challenged by the volume and types of sensitive, secure patient information exponentially increasing every year. They strive to manage explosive data growth, but also meet the increasing demands for Connected Health initiatives. To adapt to or mitigate disruption, there will be dramatic shifts in business and patient care delivery. It is meeting these challenges that make Dell EMC PowerScale solutions critical. Dell EMC PowerScale provides healthcare organizations an easy-to-manage, unified storage system.

Dell EMC PowerScale provides support for the most demanding workloads. Its ability to scale-out performance and capacity by adding CPU or storage to achieve the desired effect makes it a leader in file storage. It offers many great features that make it a leader in scale-out file storage, including:

- **Single file system** – Having a single file system and one namespace avoids added complexity to the environment and enables policies to be across the entire data footprint.

- **Simplicity and Ease of use** – PowerScale is simple and easy to manage for storage admins but also offers a great experience to users that is transparent, even when leveraging the cloud to back up data.
- **Global availability and protection** – Achieved by leveraging CloudPools or through asynchronous replication to a secondary PowerScale cluster.
- **Linear scalability** – Unlike scale-up NAS built on legacy technology, PowerScale allows you to scale performance and capacity independently or both at the same time. For many workloads as growth occurs on different storage platforms, there is a substantial performance hit. PowerScale can balance these two aspects of your storage.
- **Unmatched storage efficiency** – With both utilization rates that exceed 80% as well as the ability to automate tiering to lower-cost infrastructure, PowerScale delivers the efficiency to keep up with growing environments and tight budgets.
- **Automated Policy-Based Tiering** – Delivers the ability to simplify management no matter how large your data becomes. This breaks the challenging relationship of data proliferation and resourcing constraints by allowing IT Operations teams to stretch and cover growing data footprints effortlessly.

To fully address this emerging IT agenda for cloud and Big Data the Dell Technologies Healthcare team continues to develop a robust partner ecosystem to help support infrastructure that provides the highest levels of performance, availability, security, and automation required for around the clock patient care delivery. We have a strong set of healthcare partners that we work with daily from testing, validation, and solution certification perspective that help ensure time to solution value when you purchase infrastructure from Dell Technologies and our partners.

We are also working with a variety of solution partners, systems integrators, and cloud partners that know healthcare to help move forward your initiatives for healthcare hybrid cloud and Big Data Analytics that incorporates security of PHI.

Dell EMC PowerScale Layered Cybersecurity for data protection

With Dell EMC Powerscale one can take immediate action to improve your cybersecurity status by following the layered approach which includes:

- **Employing data protection best practices**
    - An N+1 architecture will layer your defenses to protect against a broader base of attacks.
- **Data Hardening and PowerScale Protection Features**
    - Use the DPS Hardening Guides or deploy Professional Services to perform hardening.
    - Set up Snapshots and SyncIQ for data recovery.
    - Enable encryption of data in flight and at rest.
    - Deploy Superna Easy Auditor.
    - Turn on retention lock in your key production filers and backup targets. Even a short retention period will protect against devastating attacks.
- **Use Advanced Protection Services**
    - The Isolated Recovery Solution is a powerful solution to protect against today's most devastating attacks and enable a very fast recovery.

- Use Dell Technologies Service Offerings to advise your organization on a holistic security implementation, to implement the necessary infrastructure, and to validate that everything is working as designed.

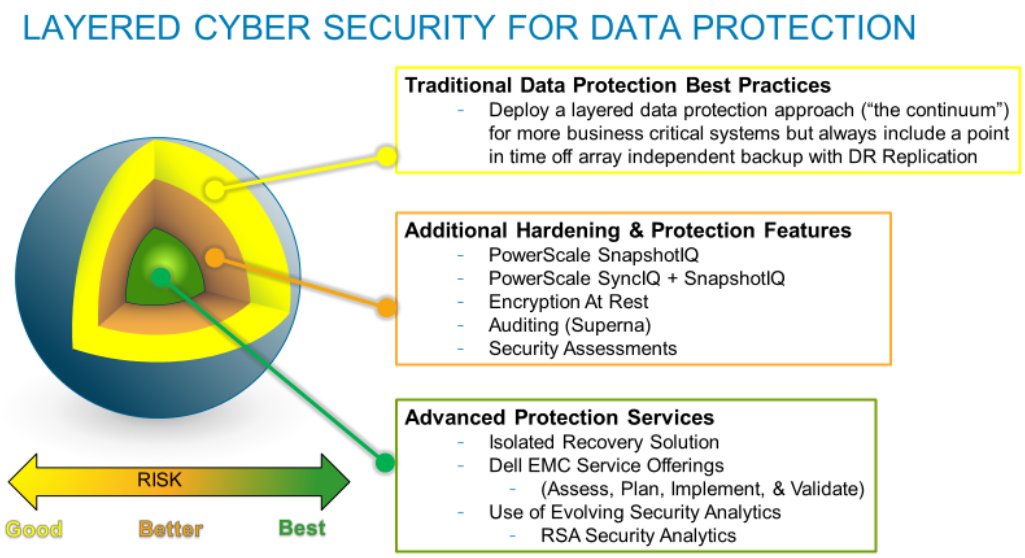


Image Source: https://inside.dell.com/docs/DOC-267634

Superna Eyeglass Products for Dell EMC PowerScale

Superna delivers disaster recovery orchestration, security, root cause analytics, and configuration management solutions for Dell EMC PowerScale. Listed are the various Superna solutions:

- **Superna DR Automation Module**
  - Offers automated failover and cluster DR monitoring.
- **Superna Ransomware Defender**
  - Offers real-time threat detection, prevention and recovery.
- **Superna Golden Copy**
  - Ransomware/Malware Isolated copy of data on another storage device "**Virtual AirGap**".
  - Offers File to Object S3 copy PowerScale data with **Superna AirGap** and Security. Creating a master copy of a data set in S3 compatible storage.
- **Superna Easy Auditor**
  - Offers real-time and historical file auditing with real-time monitor and policy-based triggers.
- **Superna Performance Auditor**
  - Offers real-time performance using audit data to summarize top users, paths, subnets, and nodes.
- **Superna Eyeglass Search & Recover**
  - Offers full text index, incremental indexing, file system analytics.
- **Superna Cluster Storage Monitor**

- Offers automated Quota creation with AD integration, Quota reporting, Quota chargeback billing, and File unlock portal for helpdesks.

Superna Ransomware Defender

Superna Ransomware Defender minimizes the cost and impact of ransomware by protecting data from attacks originating inside the network. The solution uses per-user behavior analytics to detect abnormal file access behavior to protect the file system. The Ransomware Defender module uses automatic snapshots, identifies compromised files, and denies infected users' accounts from attacking data by locking the users out. Listed are its functions:

- Stops Ransomware real-time across all managed clusters using user behavior-based detection. Provides automatic Escalated response if there are multiple infections.
- Security Guard feature – Simulated Ransomware attack validates that response actions to an attack are functioning as expected with alerts to administrators to ensure all security components are ready and tested daily.
- Detects user path, file, shares IP address where the attack originated, and captures last hour of user activity before the attack.
- Administrator alerts, logs suspicious log on activity, and timed Auto lockout rules if administrator not available to review a security incident.

Dell EMC PowerScale + Ransomware Defender Architecture

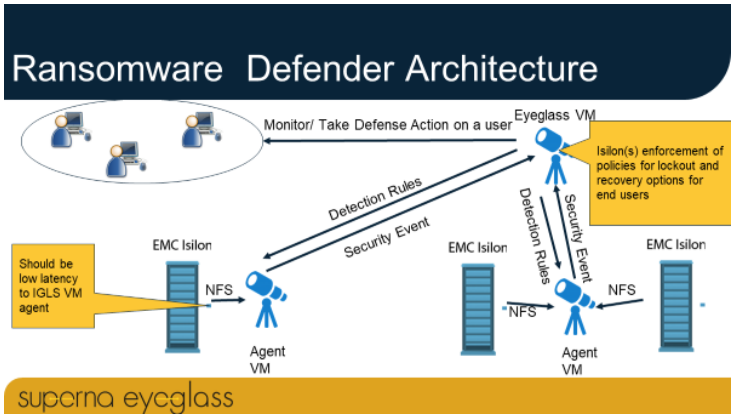


Image Source: https://inside.dell.com/docs/DOC-427470

- Ransomware Defender integrates with Dell EMC PowerScale file auditing feature. The solution offers a fully active 3 VM cluster appliance on VMware that can parallel process audit events while surviving a single node failure. Integrated CEE processing reduces the cost of external servers using Docker containers.
- Integrated with Eyeglass DR edition to simplify failover of Ransomware monitoring from production to Disaster Recovery.

Superna Easy Auditor

Superna Easy Auditor simplifies and lowers the cost of file access security reporting and introduces real-time audit features. It enables pro-active protection of data with automated responses that protect data before it is compromised. Reporting and searching audit is possible with interactive UI or scheduled reports for longer running queries.

- Enables easy automated auditing of PowerScale clusters.
- Automated reports check HIPAA compliance from a data access and Cluster configuration view.
- Next-generation Audit platform uses PowerScale HADOOP HDFS on PowerScale to store and leverage the nodes to analyze audit log data.
    - Legacy platforms use relational database architecture and require fast FC storage to perform queries with higher cost in storage and server infrastructure
- Leverages the power of Scale-out NAS to reduce the cost to store analyze audit data with reduced compute VM's (no hardware appliance needed).

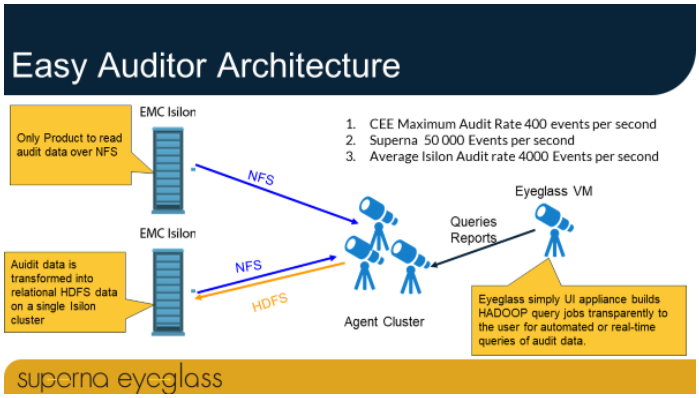


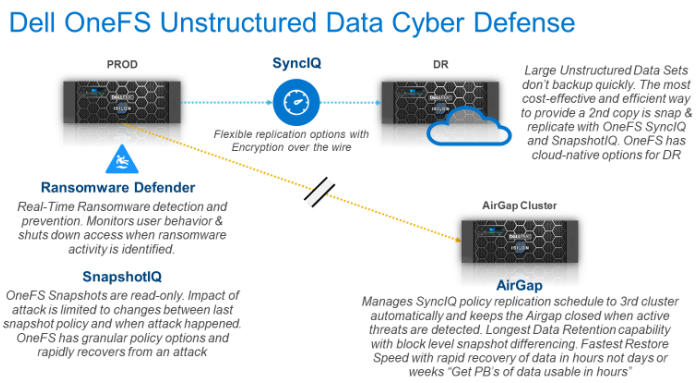
Image Source: https://inside.dell.com/docs/DOC-427470

Dell EMC PowerScale Cyber Defense Solution Offerings

The best way to protect unstructured content is to quickly detect and shut down infected accounts. More capacity infected equals longer Recovery Time Objective (RTO). The following solution offerings are arranged in the order of Good, Better, and Best based on the level of protection an organization is looking for along with Dell EMC PowerScale:

- **Good**
    - OneFS Read-Only Snapshots
    - DR cluster with SyncIQ Encrypted replication and snapshots
- **Better = Good + Superna Ransomware Defender**
    - Superna Ransomware Defender monitors user behavior to detect attacks faster than typical methods
        - Alert or act on attacks
        - Expedite the recovery process and determine infected files
- **Best = Better + Superna AirGap**
    - Superna AirGap Software to 3rd cluster
        - Keeps the Airgap closed when active threats are detected

- Provides a usable copy of data (Recovery Point Objective [RPO] in hours instead of days) regardless of infection status on Production and DR



Conclusion

The necessity to secure patient data is more important than ever and ransomware attacks cannot be allowed obstruct delivery of treatment to patients where every minute counts. It is important for the healthcare organization to first understand the characteristics, causes, and indicators of ransomware attacks and then be proactive in taking preventative measures. When it comes to healthcare, data held ransom can mean lives are put at risk. Building the cyber resilience of a hospital is vital and it is a shared responsibility of both the users and manufacturers. Users undergo regular security training and manufacturers should equip their products with the appropriate cybersecurity measures. It is important to understand that cyber-attacks are unavoidable because malicious hackers are always finding new ways to exploit vulnerabilities. Strong password policies along with MFA can significantly improve security. By combining technical controls with employee training, organizations will stay steps ahead of cyber-criminals. Most cybercriminals are looking for easy prey.

This article discussed a variety of threats faced by healthcare organizations, the current status, and the best practices that can help healthcare organizations defend themselves against ransomware. We also discussed how Dell EMC PowerScale's layered cybersecurity approach along with Superna offerings such as Superna Ransomware Defender, Superna Easy Audit, and Superna Gold Copy Virtual AirGap can offer simplified and automated solutions to health care customers to ensure business continuity and protection against ransomware. It is hoped that this article will provide readers with the importance of cybersecurity measures to move towards a future of highly scalable, easily managed, and well-protected storage solutions.

DISCLAIMER: *The information provided in this whitepaper does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this whitepaper are for general educational and research purposes only. Readers should contact their attorney for any legal questions if you were a victim of ransomware or a Cyber-attack.*

References

- Types of Cyberattack
  - Cyberattack – Wikipedia (https://en.wikipedia.org/wiki/Cyberattack)
  - Cisco - Cyber Attack - What Are Common Cyberthreats? (https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~how-cyber-attacks-work)
- Types of Ransomware
  - What are the different types of ransomware? (https://www.kaspersky.co.in/resource-center/threats/ransomware-examples)
  - The Most Common Types of Ransomware Strains (https://www.datto.com/blog/common-types-of-ransomware)
- Healthcare cyberattacks
  - HIPAA Journal - Healthcare Cybersecurity (https://www.hipaajournal.com/category/healthcare-cybersecurity/#:~:text=In%202020%2C%20healthcare%20data%20breaches,also%20a%20record%2Dbreaking%20year)
  - 560 Healthcare Providers Fell Victim to Ransomware Attacks in 2020 (https://healthitsecurity.com/news/560-healthcare-providers-fell-victim-to-ransomware-attacks-in-2020)
  - Eric Kedrosky - Global Ransomware and Cyberattacks on Healthcare Spike during Pandemic (https://securityboulevard.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/)
- Healtcare Cybersecurity
  - Top 3 Cyber Security Practices to Prevent Cyber Attacks in Healthcare (https://www.provendatarecovery.com/blog/top-cyber-security-practices-prevent-attacks-healthcare/)
  - https://www.securitymagazine.com/articles/93770-healthcare-cybersecurity-strategy-start-at-the-end
  - Salem T. Argaw - Cybersecurity of Hospitals (https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7)
- Ransomware Defense Strategies
  - Ben Webster - Mitigating Healthcare Ransomware Attacks (https://www.infosecurity-magazine.com/blogs/healthcare-ransomware-attacks/)
  - Arundhati Parmar - Ransomware in healthcare: The inevitable truth (https://medcitynews.com/2020/10/ransomware-in-healthcare-the-inevitable-truth/?rf=1)
- Dell EMC PowerScale Healthcare solutions
  - https://inside.dell.com/docs/DOC-51047
- Superna
  - https://www.supernaeyeglass.com/products
  - https://b4cd9a40-2c00-4627-9775-166ed45c610e.filesusr.com/ugd/933f05_f5960ebae0904d6aa21656ba9ff8f3f5.pdf

- Ransomware Case Study
    - Ryuk UHS - https://techcrunch.com/2020/09/28/universal-health-services-ransomware/
    - WannaCry NHS - https://www.bbc.com/news/technology-41753022
    - Egregor GBMC - https://healthitsecurity.com/news/ransomware-attack-on-marylands-gbmc-health-spurs-ehr-downtime
    - SamSam Atlanta - https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/