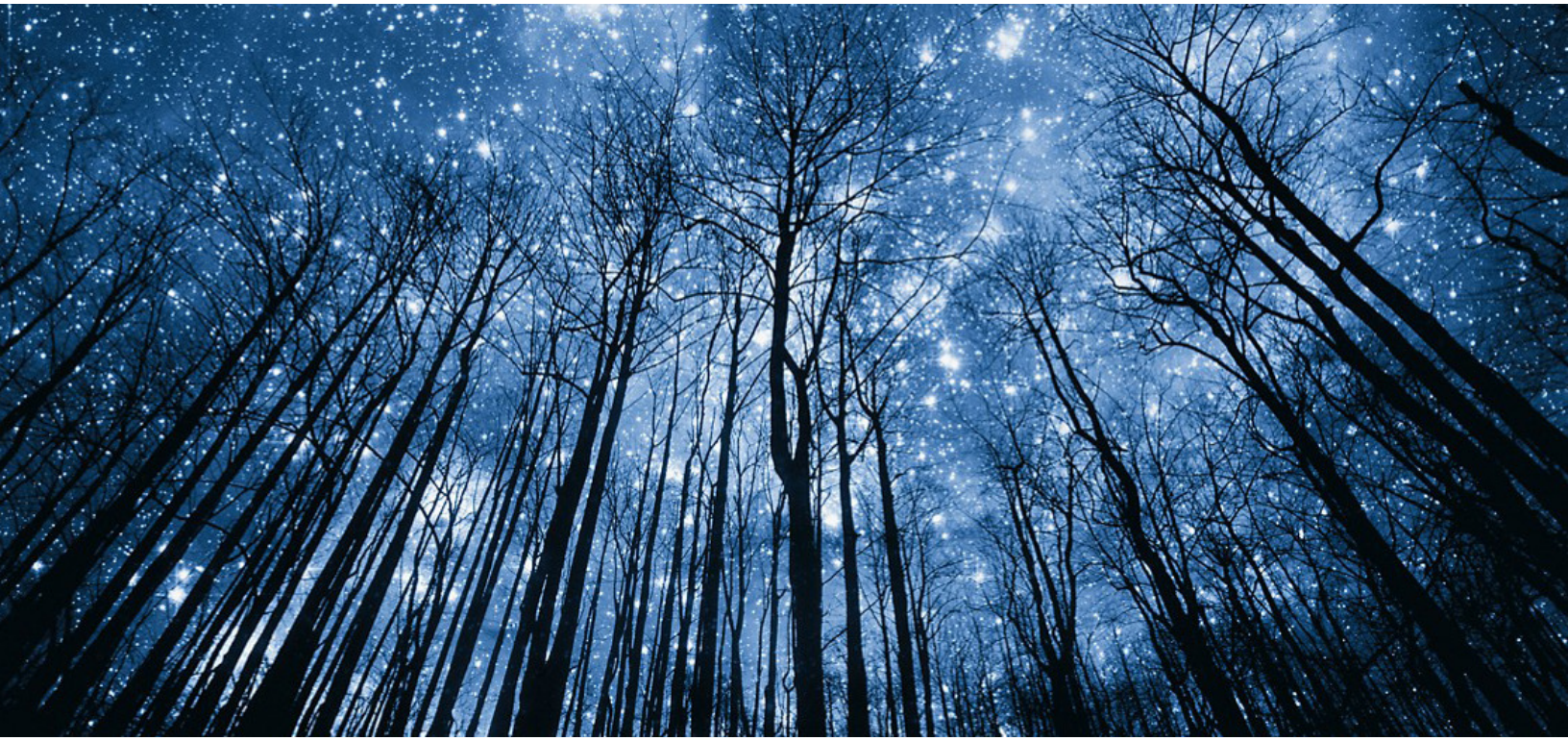
DELL Technologies

POWERSCALE CYBERSECURITY – SUPERNA AIRGAP GUIDE



Lenin Ponnappa
Inside Product Specialist

Shwetha L
Inside Product Specialist
Dell Technologies
Shwetha.lokesh@dell.com

Prateek Bhat
Inside Product Specialist
Dell Technologies
Prateek.bhat@dell.com

Proven Professional

Knowledge Sharing Article

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

Today, there is rapid growth in technology. New technologies are emerging day by day and are changing the environment. But due to these advancements in technology It has become a challenge to safeguard our critical information. Cybersecurity is integral to technology. As per research, it is said that a cyber-attack takes place every 11 seconds over the globe which attributes to average cost of one attack for $13M and still growing. Under such critical circumstances, Cyber Security has become a pillar of any Technological firm in modern day. One of the biggest challenges any organization deals with nowadays with all the digital data explosion and usage of the internet is maintaining the integrity of information and securing it.

Why is it so important to secure data? Well, cyber attackers all over the globe are waiting to steal and manipulate the information that can be inferred from data and use it to cause harm or destruction. The data has various levels of sensitivity ranging from personal information to critical business-related industry information. Whenever we think about cyber-security, the pioneer topic that hits our mind is cyber-attacks. Organizations, Business Firms, Government bodies are all striving hard to take preventive measures against cyber-crimes. Besides all these actions being practiced, cyber security is still a primary concern for many.

There are Various types of cyber-attacks that might have a long-term or short-term effect on the system or data. These attacks are getting sophisticated day by day and tools or strategies to terminate such attacks are really the need of moment. There are various types of cyber-attacks like Malware, Phishing, Man in the Middle attacks (MitM), Denial of Service (DOS) Attack, SQL injections, Zero-day Exploit, Password attack, Cross-site Scripting, Rootkits, Internet of Things (IoT) Attacks and many more attacks. The whole complexity of attacks is increasing with new attacks emerging day by day. Many attacks happen over the Network by probing the defenses and exploiting the vulnerabilities. Attacker will scan the network by certain tools and build an attack plan against the target.

Ransomware is one such attack, which brings serious threat to the data integrity and development of any organization. Ransomware attacks came into existence as early as 1989. In 30 years, it became one of the most dangerous attacks that organizations can face. Ransomware attacks have gained global traction, with the motive of gaining monetary benefits through illegal activities. It is a growing threat to the data of businesses and because of the copious amounts of money to be made, new variants appear frequently. It can lead to the loss of sensitive information, the interruption of normal operations, and reputational damage to a business.

Superna Airgap is one such technology which pioneers in providing a modelled layer of protection against such ransomware attacks. Superna Airgap which is integrated with the Superna Ransomware Defender which follows NIST Key Framework having the attributes of identifying, protecting, detecting, responding, and recovering to the attack, is one-of-a-kind solutions to prevent any ransomware attacks. The Superna Airgap is the data repository of last resort. This is the place where you go when the regular defenses have failed.

In this paper we will discuss,

- Overview of Ransomware attacks and their effects.
- The cybersecurity strategy of Dell Technologies partnering with Superna to mitigate and terminate such attacks.
- How different is the cyber resiliency with Dell Data Protection solutions with respect to Dell Unstructured Data Solutions?

One of the features of Superna Multi Vector Defense is a type of security monitoring detection vector focused on a particular layer of the application stack like the syslog, email log, etc. We will dive deep into this topic in this paper. We will also focus on challenges faced by cyber security with the latest technologies.

This paper will be useful for,

- Technologists, Engineers, Leaders, stakeholders, who need to know what strategy Dell Technologies have for cyber-security in space of Unstructured data solutions, especially file based.
- How Dell Technologies and Superna create one of a kind technical solution for Cyber-security with minimal management jargons.
- Technical enthusiasts who want to know what Superna Ransomware defender and Airgap are, what are the options, and other technical aspects.
- Technical team and customers to differentiate between the Dell Data Protection and Unstructured Data Solutions Cyber Resiliency Portfolio.

Cybersecurity and Resiliency Introduction

Cybersecurity can be defined as the process or science of protecting systems, networks, and the data that these systems contain from malicious attacks, which might cause huge losses to organization and data confidentiality and integrity problem to customer data. To disrupt the Cybersecurity of an organization, the attacker or the agent tries different methods and practices. These practices are called Cyberattacks. Usually, the aim of cyberattacks are to access, change, or destroy important and sensitive information of a firm and in return seek money from stakeholders, users and employees or even interrupt day-to-day business processes.

Any organization that decides to build protection Cyber-attacks or corruptions needs to keep in mind the right approach to implement this, that is, to have multiple layers of protection widely dispersed across the edge, core, cloud and most prominently in the storge systems. So, this is not just an exercise of keeping the systems secure, it is a true strategy of keeping the whole organization, its data and all the sensitive customer information safe from any attacks that may be induced in future or may already have been induced as such. In any organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks.

Implementing effective cyber resiliency and its strategies is particularly challenging in the new-age technological era because there are multi-millions of connected devices, applications and data that are laid out in every phase and lifecycle of the development and deployment. People, and attackers are becoming more innovative and achieving new ways to disrupt the cyber resiliency of the organizations.

Why is Cybercrime Increasing?

Data is the new Oil, Data is the new diamond, Data is the new wealth. The costliest and fastest-growing type of cybercrime is data and information theft. As per research, it is said that a cyber-attack takes place every 11 seconds over the globe which attributes to average cost of one attack for $13M and still growing. Under such critical circumstances, Cyber Security has become a pillar of any Technological firm in modern day. The growing accessibility of identification information to the web via various services, tools, and systems is driving this trend ahead. According to the report of Accenture, 71% of all attacks are financially motivated and involve small business in 43% of all cases and overall business of $5.2 Trillion is at risk because of these threats, which is massive!

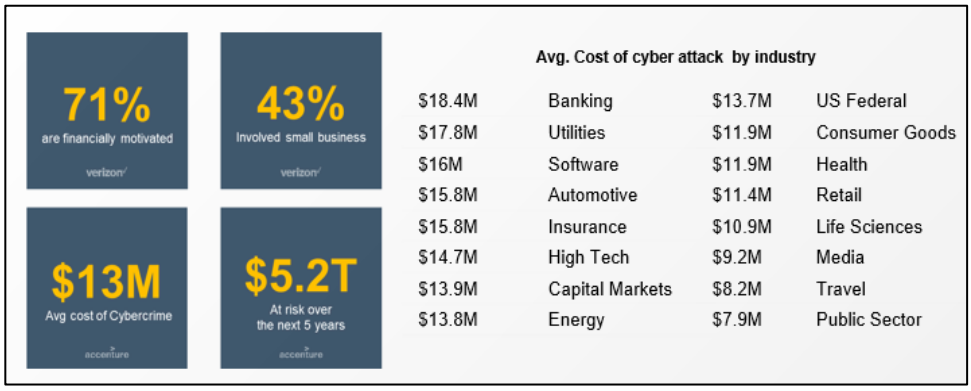


Figure: Some of the statistics from Accenture and Cybersecurity Venture reports
Image Source: https://inside.dell.com/docs/DOC-516693

But it is now no longer the best target. Industrial controls that control energy grids and different infrastructure may be disrupted or destroyed. And identification robbery is not always the best goal, cyber-assaults can also additionally compromise facts integrity (wreck or trade facts) to reproduce mistrust in an agency or government. Cybercriminals are getting greater sophisticated, converting what they target, how they influence agencies and their techniques of assault for distinctive protection systems. Social engineering stays the absolute best shape of cyber-assault with ransomware, phishing, and adware being the very best shape of entry. According to the Ninth Annual Cost of Cybercrime Study from Accenture and the Ponemon Institute, the common fee of cybercrime for an agency has expanded through $1.4 million over the past years to $13.0 million and the common wide variety of facts breaches rose through eleven percentage to 145%. Data breaches can contain monetary statistics like credit score card numbers or financial institution account details, covered fitness statistics (PHI), for my part identifiable statistics (PII), alternate secrets, highbrow property, and different goals of commercial espionage. Other phrases for facts breaches encompass unintended statistical disclosure, facts leak, cloud leak, statistics leakage, or facts spill. Other elements riding the increase in cybercrime encompass:

- The disbursed nature of the Internet
- The cap potential for cybercriminals to assault goals outdoor their jurisdiction makes policing extraordinarily difficult
- Increasing profitability and simplicity of trade at the darkish web
- The extensive use of connected devices and the Internet of Things (IOT).

Importance of Cybersecurity

Fundamentally, our society is extra technologically reliant than ever earlier than and there may be no signal that this fashion will slow. Data leaks that would bring about identification robbery are publicly published on social media accounts. Sensitive data like social protection numbers, credit score card data and financial institution account info are saved in cloud garage offerings like Dropbox or Google Drive.

Whether you are an individual, small business or large multinational, you rely on computer systems daily. Pair this with the rise in cloud services, poor cloud service security, smartphones, and the Internet of Things (IoT) and we have a myriad of potential security vulnerabilities that did not exist a few decades ago. We need to be educated on the comparison between cybersecurity and information security, although the skillsets are the same.

The depend on reality is whether you are an individual, small enterprise or huge multinational, you depend upon laptop structures day to day. Pair this with the upward push in cloud services, bad cloud carrier safety, smartphones, and the Internet of Things (IoT) and we've a myriad of capacity safety vulnerabilities that failed to exist some a long

time ago. We want to be knowledgeable at the assessment of cybersecurity and statistics safety, although the skillsets are the same. Governments round the arena are bringing greater interest to cybercrimes. General Data Protection Regulation (GDPR) is an extraordinary example. It has multiplied the reputational harm of statistics breaches through forcing all companies that perform withinside the EU to:

• Communicate statistics breaches

• Appoint a statistics safety officer

• Require person consent to method statistics

• Anonymize statistics for privacy

The fashion closer to public disclosure is not confined to Europe. While there are not any countrywide legal guidelines overseeing statistics breach disclosure withinside the United States, there are statistics breach legal guidelines in all 50 states. Commonalities include:

• The requirement to inform the ones that influence as quickly as possible

• Let the authorities realize as quickly as possible

• Pay a few forms of fine.

They pushed well known forums just like the National Institute of Standards and Technology (NIST) to launch frameworks to assist companies apprehend their safety risks, enhance cybersecurity measures, and save you cyber-attacks.

Common Threats and Concerns in Cybersecurity

Cybersecurity threats are of a broad variety based on what they affect and how they affect the systems or data. All threats have different methods, and malicious attackers have different methods of attack. Here we have briefly noted some of the important threats that affect the systems normally.

Phishing

Phishing is a social engineering attack that is used to obtain personal information from users, such as login passwords and financial information. Here the attacker possesses as a trustworthy party and somehow makes a victim open specific mail, message, or link. In the backend recipient is misled into opening a malicious link, which can lead to malware installation, system freeze as part of a ransomware attack, or the revealing of sensitive data.

Malware

Malware is an active attack which involves a sort of software that is created with the goal of causing harm or gaining unauthorized access to a computer. This may change the data / harm the data when active in the system. Cyber thieves utilize it to harvest data that they may exploit to gain financial advantage over their victims. This information includes everything from financial information to health-care records to passwords and emails.

Ransomware

This is an active attack, which is persistent in the new age and affects the system and organization both financially and technically. The attackers, here, induce malware or malicious software into the system, that contains Encryption

algorithms which encrypt the data and keep that as hostage. Only specialized decryption tools can be used to decrypt this. Its purpose is to extort money by preventing access to data or the computer system until a ransom is paid. However, Paying the ransom is not the surety of files being retrieved to system or the organization. It keeps the victim's personal information hostage and prevents access to the system.
Example: Referring the Fig, Ryuk is one of the most active ransomwares and the biggest players among other ransomwares. It is a type of crypto ransomware that blocks access to a file, system, or device by using encryption until the ransom is paid.

Man in the Middle attack (MitM)

A Man in the Middle (MitM) attack occurs when an attacker establishes a position between the sender and receiver of electronic/digital messages and intercepts them, possibly altering them in transit. The sender and receiver believe they are communicating directly with each other. An example of a MitM attack is in the military to confuse the enemy.

Trojans

Trojans, named after the Greek mythological Trojan Horse, are a form of malware that disguises itself as something else before releasing destructive code within the target system. They are deceitful programs that pretend to do one thing but do something adverse. They not only hamper data confidentiality but also affect the system's data integrity and availability.

Denial of Service (DDoS)

Multiple infected computer systems attack a target and cause a denial of service for users of the targeted resource in a distributed denial of service (DDoS) attack. Target can be different resources of the computational system like network, server, storage, or other web-based applications. The rush of incoming messages, connection requests, and malformed packets causes the target system to slow down, crash, and shut down, denying service to genuine users and systems.

Data Breaches

Important/private/confidential data is exposed to an unauthorized individual when there is a data breach. A little flaw can lead to a big data leak if it is not addressed properly. Without authorization, data from a data breach is seen and/or spread. A data breach may affect anybody, from individuals to large corporations and governments. More significantly, if someone is not protected, they can endanger others.

Ransomware Attacks and Types

Ransomware is a sort of malicious software (malware) that threatens to post, or blocks entry to server or a laptop system, normally through encrypting it, till the sufferer can pay a ransom price to the attacker. In many cases, the ransom calls come with a deadline. Ransomware assaults are not unusual these days. Major businesses in North America and Europe alike have fallen sufferer to it. Cybercriminals will assault any consumer, or any enterprise and sufferers come from all industries. Several authorities' agencies, together with the FBI, propose in opposition to paying the ransom to preserve from encouraging the ransomware cycle, as does the No More Ransom Project. Furthermore, 1/2 of the sufferers who pay the ransom are probably to be afflicted by repeat ransomware assaults, if it is not always wiped clean from the system.

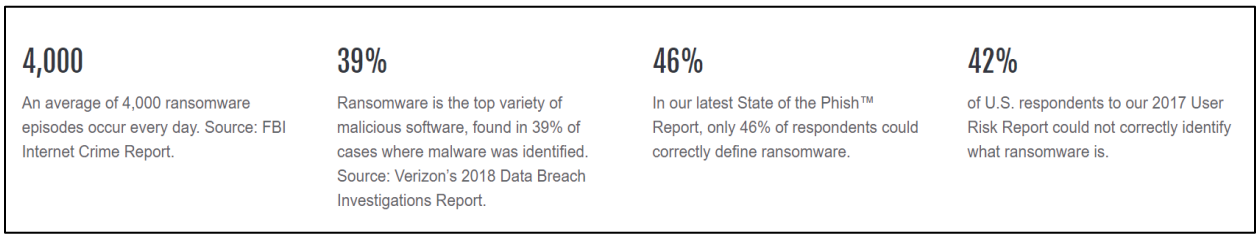


Figure: Some of the statistics related to Ransomware attacks
Image source: https://www.proofpoint.com/us/threat-reference/ransomware

These are some of the Ransomware types:

WannaCry – A worldwide cyberattack in May 2017. It was created by WannaCry ransomware cryptoworm. The main victims of this ransomware attack were the MS Windows OS and demanding ransom payments in Bitcoins

Ryuk – This ransomware had compromised the Healthcare, Government, Manufacturing, Technology and Academia organizations in 2019. They had the highest ransom demand at USD $12.5M.

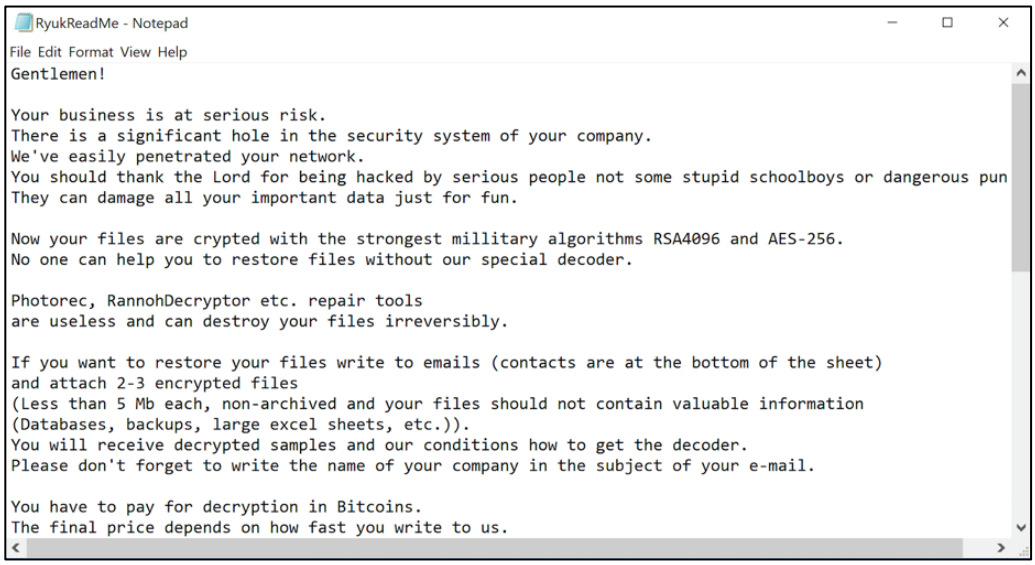


Figure: An actual ransomware attack notes which was sent to one of the firms by Ryuk.
Image Source: https://inside.dell.com/docs/DOC-516693

Egregor – It earned its destructive reputation after the group successfully breached Barnes & Noble and then breached the video game developers Crytek and Ubisoft in 2020.

Samsam – This ransomware is a custom infection used in targeted attacks, often deployed using a wide range of exploits or brute-force tactics. The attacks were made on targets via vulnerable JBoss host servers during a previous wave of Samsam attacks in 2016 and 2017.

PowerScale Cyber Defense Strategy

Generally, there are 7 security layers for any ideal cyber security solution considered, namely:

The Human Layer – Where in the Data Center / Place where the data is to be stored is monitored and secured by human beings, that is, the security guards may be belonging to private security agencies or government bodies.

Perimeter Security – These may also include the CCTV cameras and other practical set up done to secure the data center overall. They go hand in hand with the Human Layer of Security.

Network Security – Network Security may include the antivirus to monitor the network, Network access control, Setting up a Network security policy, etc.

Endpoint Security – Endpoint security provides security teams the visibility, they need to uncover incidents that would otherwise remain invisible. This is important because it provides a graphical view of how the attacker gained access to the system and what they did once they were inside.

Application Security – Providing security at the application level is the main aim of application security. Some of the features are application logging, Privilege grant, authentication, access privileges etc.

Data Security deals with securing the Data or information stored in the system. Backups, Data Sanitization and Erasure are some of the examples. Some of the systems may be encrypted from a hardware perspective, some may be from a software perspective.

Mission Critical asset Security – This type of security practice protects the organization's mission critical assets. Some of the essential information is stored in this layer of architecture. These are such data which run the core of the business of that organization

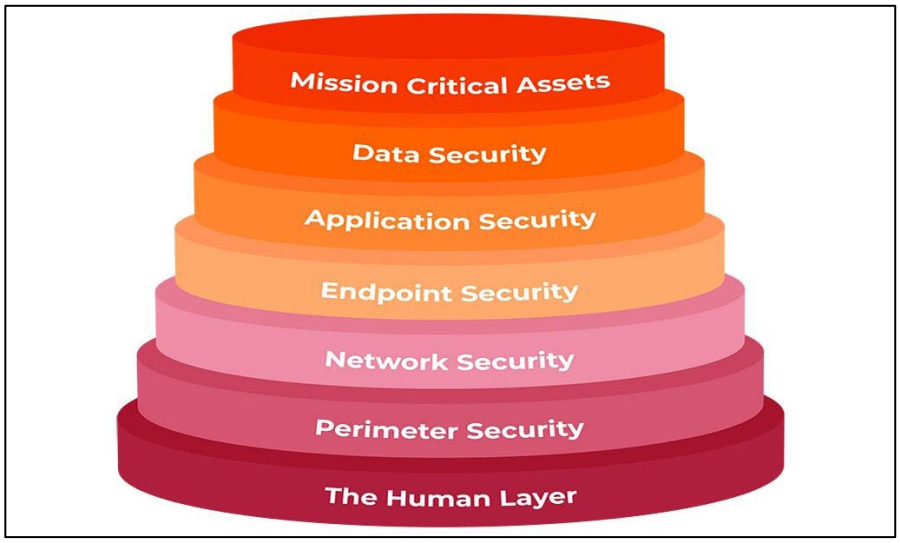


Figure: Different layers of cyber defense strategy commonly used in industry
Image Source: https://www.dotnek.com/Files/Blog/30330/What-are-the-7-layers-of-security.jpg

According to the trend in Industry, we can visualize that most of the IT security investments are made at the Network and Application Layers, However, under critical situations like Ransomware attack or Malware Injection, some of these security layers may not provide a complete security to the entire system. In such cases, the system is subject to vulnerability. This can be mitigated by providing proper security strategies at more inner layers such as data layer and Mission critical assets layer as well. This will ensure that the data which the system contains is not hampered, even though if it gets affected somehow, the security strategy in this layer gives freedom to re-organize the data that is affected from such attacks.

The above-mentioned strategy is the exact one that is followed by PowerScale as well, when we consider Cyber Resiliency. PowerScale Cyber Solution not only aims to fortify the data layer, but if any ransomware attacks the system and reaches the data layer as well, the strategy aims to provide adequate failover capabilities in such scenario as well.

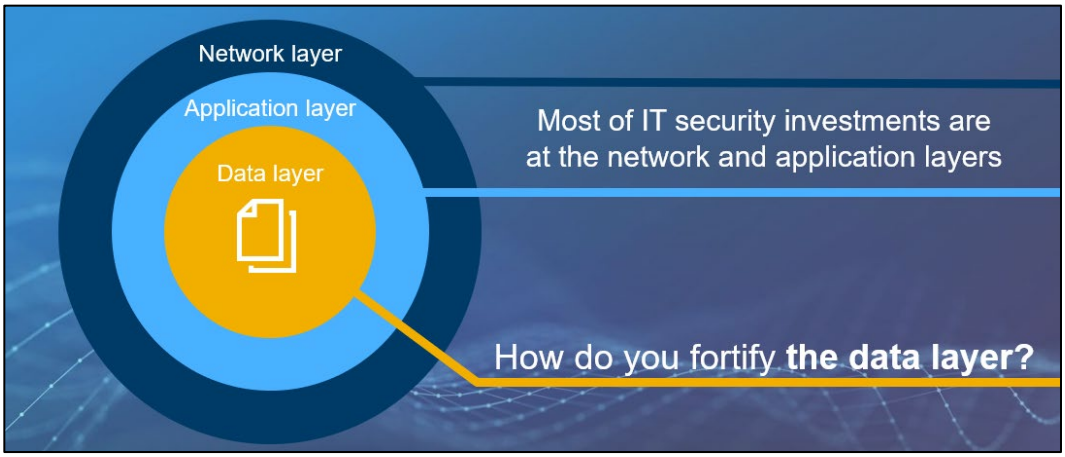


Figure: Dell Technologies along with Superna aim to provide defense at Network, application, and data layers.
Image Source: https://inside.dell.com/docs/DOC-516693

Dell Technologies PowerScale extends its tremendous partnership with Superna, in order to provide Cyber Resiliency for the unstructured data portfolio. Superna technologists along with Dell architects have designed and implemented this technology. Now we will investigate what Superna is and what are some of the important technologies they work on. By understanding this, we can visualize how Dell Technologies works with Superna intensively to design the Cyber Resiliency Strategy.

What is Superna?

Superna is a strategic partner of Dell Technologies in designing Cyber Resilience Strategy, especially around the Unstructured data solutions through its wide variety of software capabilities and offerings. Superna aims to deliver DR orchestration, security, root cause analytics and configuration management solutions for file storage systems.

Customers can utilize the wide variety of Superna Eyeglass® portfolio to reduce the unplanned downtime, protect and secure business critical data, enable continuous operations, and simplify administration of Scale Out NAS all under a single bundled solution with easy maintenance.

Some of the Superna Technologies include:

- **Superna DR Automation Module:** Offers automated failover and cluster DR monitoring.
- **Superna Ransomware Defender: Isolated** data copy is stored on "Virtual Airgap," hence providing shield against Ransomware and Malware, also offers File to Object S3 copy PowerScale data with Superna AirGap and Security. Creates master copy of a data set in S3 compatible storage called vault.
- **Superna Ransomware defender for AWS S3:** Real time behavioral analysis of S3 bucket access to identify malicious activity and Simulated attack feature to self-test detection and provide health status with automated test feature called Security Guard
- **Superna Cyber Scanner:** Understands file types and offers content aware analysis of file information checking for corruption, encryption or file modifications that render the ineffective data.

- **Superna Easy Auditor:** This offers file auditing capabilities both historically and real-time and enables policy-based triggers.
- **Superna Eyeglass Search and recover:** Offers full text index, incremental indexing, file system analytics.
- **Data Marshal (Coming Soon):** Cloud object storage enabled archive platform that automates moving stale data to object storage.
- **Superna Golden Copy:** An archive/backup and recall platform simplify moving files to object storage for long term retention or 3rd copies.
- **Superna Eyeglass AnyCopy:** enables high performance data movement workflows between clusters leveraging Isilon/PowerScale SyncIQ.
- **Superna Performance Auditor:** Offers real-time performance using audit data to summarize top users, paths, subnets, and nodes.
- **Cluster Storage Monitor:** automates the management of storage reporting, and quota administration. The additional(add-on) manages one or more clusters and offers chargeback reporting, searching, and reporting of all quota types.
- **Superna AirGap:** Fully Automated Cyber Vault for daily reporting on synced data with summary reports, and per sync job object list of successful or failed syncs

PowerScale Cyber Resiliency Implementation using Superna

Superna Airgap along with the Superna Ransomware Defender which follows NIST Key Framework having the attributes of identifying, protecting, detecting, responding, and recovering to the attack, is one-of-a-kind solutions to prevent any ransomware attacks. The NIST (National Institute of Standards and Technology) Framework for the Cyber Resiliency briefly states that a good strategy should contain these key principles:

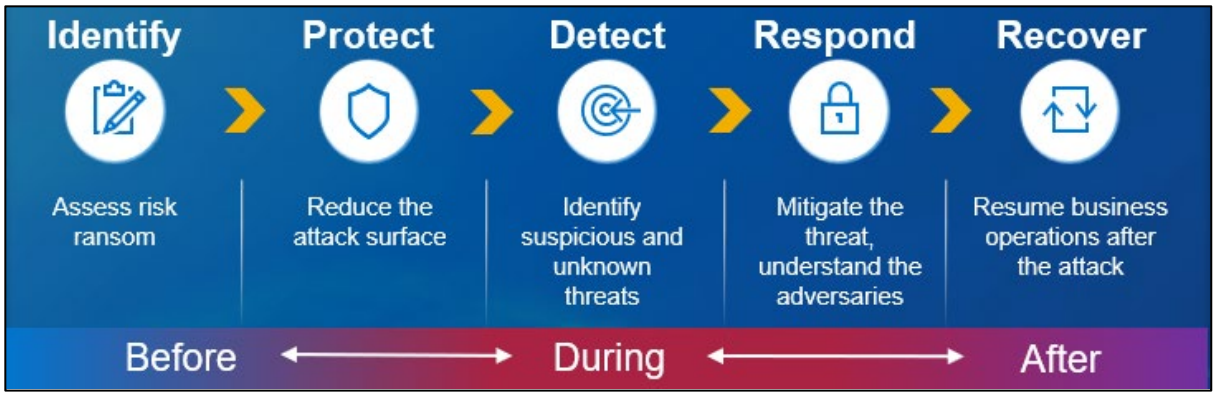


Figure: PowerScale Cyber Resiliency implementation using Superna
Source: Created by authors

Identify – Try to Identify the threat and prevent Ransom attack. Let the system be aware of different attacks that might affect in future according to the latest trends. In this step you will also identify your current security profile and your target security profile. A gap-analysis helps to explain to shareholders why specific steps are required to mitigate critical risks for the organization.

Protect – Try to reduce the attack surface and protect the systems by applying the minimal surface exposure strategy. This is also to protect the organization against the known bad before an attack is executed.

1. Applying all the core protection features available on the OneFS platform

- Access Control: This is where the core data protection functions are being executed. We change the access permissions based on recent access. IF a user did not access or modify certain data for more than a year, does he still need write access?
- Immutability: It is also about having immutable snapshots, replica versions, etc. Is there data that needs to be protected with immutability: by defining the data as WORM, you can also update your backup strategy towards an archiving strategy.
- Encryption: It is also about encrypting data in transport, encrypting data at rest.
- Anti-virus: Integrating with anti-virus/anti-malware protection that does content inspection.
- Dell Security Advisories (DSA): And do not forget our Dell Security Advisories where we inform our customers about fixes to common vulnerabilities and exposures.

2. Data isolation and onsite/offsite discussion

Data isolation is about having a last resort copy of business-critical data. This is achieved using the Airgap functionality to isolate the cyber vault copy of the data. This copy is logically separated from the production copy of the data. Data syncing happens only intermittently by closing the airgap after making sure there are no known issues.

Detect – If at all, an attack / intrusion happens detect and identify the threat and try to mitigate that through different methodologies. Real time access auditing helps detect different patterns in what data is being accessed by who and through which network path and alerts and automatic response can be set up to stop suspicious activity. Ransomware Defender also offers a "learning mode" that can be used to train the system to a particular workload or subset of data to detect unusual behavior. Examples of unusual patterns include:

- a user accessing data from an IP path that he/she does not normally use.
- File read operations happening at scale.
- Mass encryption of data happening across many files (something Ransomware attackers would do to hold the data to a ransom).
- Mass deletion of files.

Respond – Understand what the loss might be, what magnitude it might affect and its adversaries thoroughly, and try to mitigate the threat. Depending on the unusual activity detected there are a few actions IT teams can take:

- Deny read access and stop encryption as appropriate
- Terminate replication to Cyber vault
- Delete or quarantine virus infected files
- Initiate root-cause-analysis (RCA) to find the underlying cause of the unusual activity

Recover – Implies, recovering after the threat / attack has affected the system and resume the as is business operation accordingly. The key enabler of the air gapped cybervault is the network isolation and therefore the cyber vault PowerScale cluster can be on prem. However, in the event of an attack, IT teams may want to failover to a fully operational infrastructure (compute + network + storage) that gives a clean slate to operate from. Thanks to the Superna DR Edition such failover can happen without elaborate runbooks. DR readiness is constantly monitored, and IT

teams are notified of any issues with syncing data and configurations. This is of huge value to IT teams who are always grappling with the challenge of synchronizing all the data and configuration between the primary and failover infrastructure.

The technology works in such a way that the data is protected before, during and after the attack, to make sur that even if the attack happens on the system, no data of that organization is at stake. If the data is locked and held as hostage, the solution easily enables the firm to failover to a different site that is maintained as a vault, away from the network connectivity. However, The Ransomware Defender Solution from Superna also provides the capability to intelligently detect the attack and mitigate it as soon as something is detected in the system.

This implies that the Technology involved in reducing the risk follows the NIST standard framework. How is this implied in PowerScale and Superna Ransomware Defender and Airgap? Well, this is done through 3 different measures named as: Isolate, Detect, Recover

- Isolate: This process involves isolating the Vault or Air Gapped cluster from the networked layer
- Detect: This process involves Real-time threat detection at the data layer, if there are Mass deletions and encryption that is spotted effectively
- Recover: This is a stage where the attack is already induced. Yet, Data can be recovered in few minutes or hours, due to the deployment of single click failover airgap.

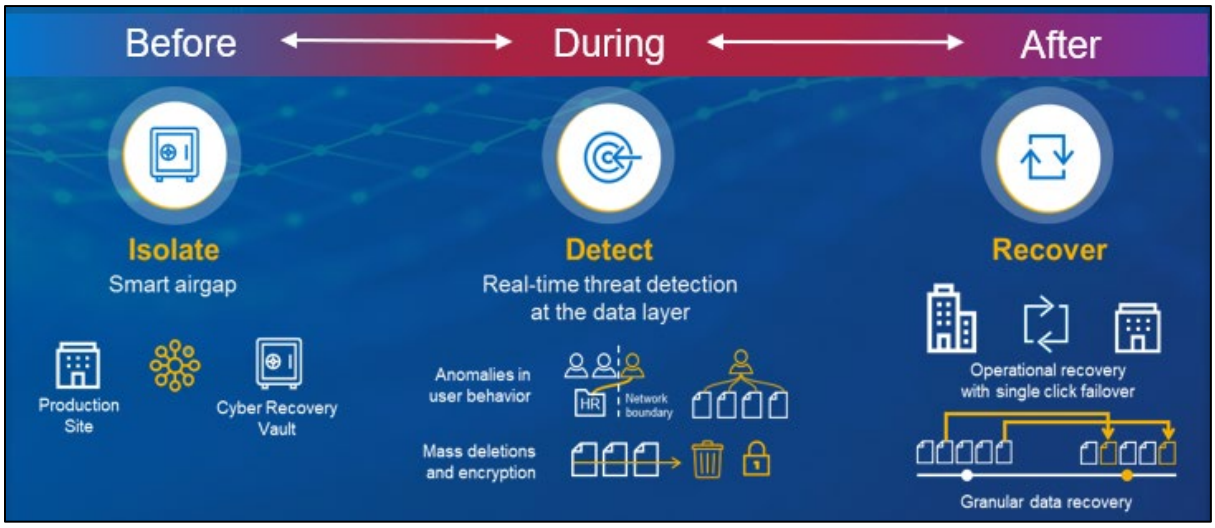


Figure: PowerScale Cyber Resiliency implementation using Superna
Image Source: Created by authors

Superna Ransomware Defender and Smart AirGap with PowerScale Functionality

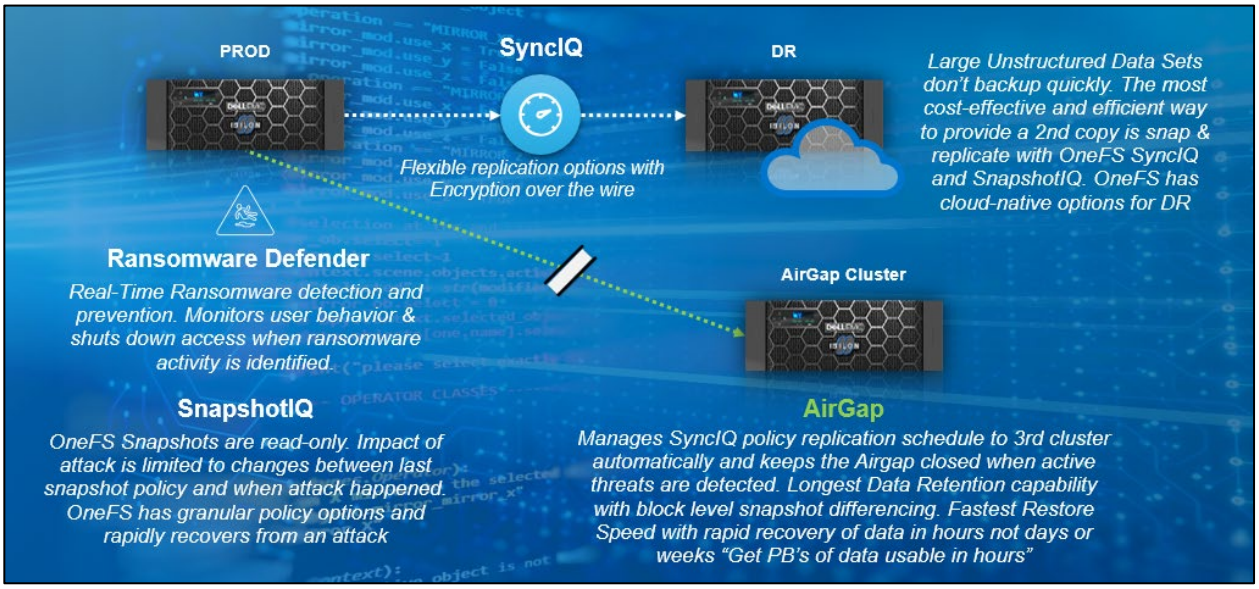


Figure: DellEMC PowerScale and Superna Airgap illustration
Image Source: https://inside.dell.com/docs/DOC-516693

Superna Ransomware Defender integrates AirGap Cyber Vault abilities with the capacity to droop statistics reproduction operations routinely while the supply statistics is beneath threat. Superna's Rapid Recovery lets offline statistics be usable irrespective of the scale of the statistics set protected. The Rapid recuperation additionally restores SMB and NFS percentage definitions. The version is to set up a third cluster with the functionality to reduce the relationship among them while there may be a ransomware attack. This lets the statistics within the vault (AirGap Cluster) to be unhurt and secure for similar use.

The best way to protect unstructured data is detection and shutting down the infected accounts. More capacity infected equals longer Recovery Time Objective (RTO). These solutions are arranged format of good, better, and best solutions based on the type and level of protection an organization can get with Dell EMC PowerScale and Superna:

- **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
    - Airgap is closed – if threats detected

Ransomware Defender is a storage layer protection solution for file and object data that monitors user behavior and protects data in real time with user file system lockouts, snapshots, file, and object tracking and infected host IP tracking, along with fully integrated Cyber vault automation for offline data management.

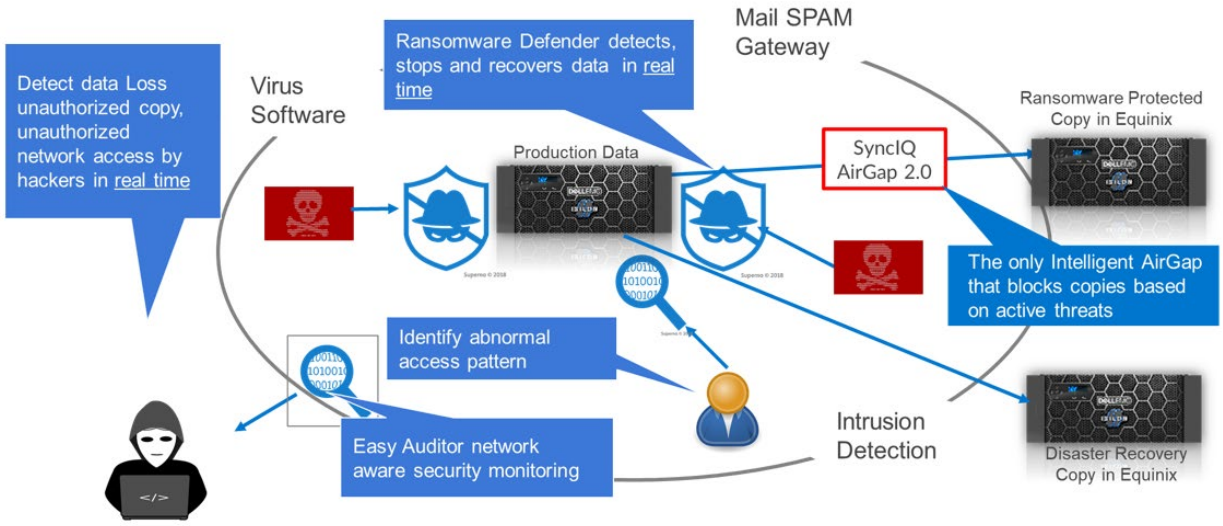


Figure: Ransomware Defender with Airgap
Image source: https://inside.dell.com/docs/DOC-516693

How UDS Cyber Resiliency differs from DPS (Data Protection Solutions)?

Due to the various changes in the technology as well as portfolio background, UDS and DPS Cyber Resiliency Strategies are different in the Dell Technologies Portfolio. It is especially important to know what scenario we need to be positioning what products. Rather, the situation of the customer must be analyzed and prioritized here.

So, once requirements are analyzed, the right portfolio must be mapped to the challenge.

The flowchart designed below provides the key to which portfolio needs to be positioned in what scenario.

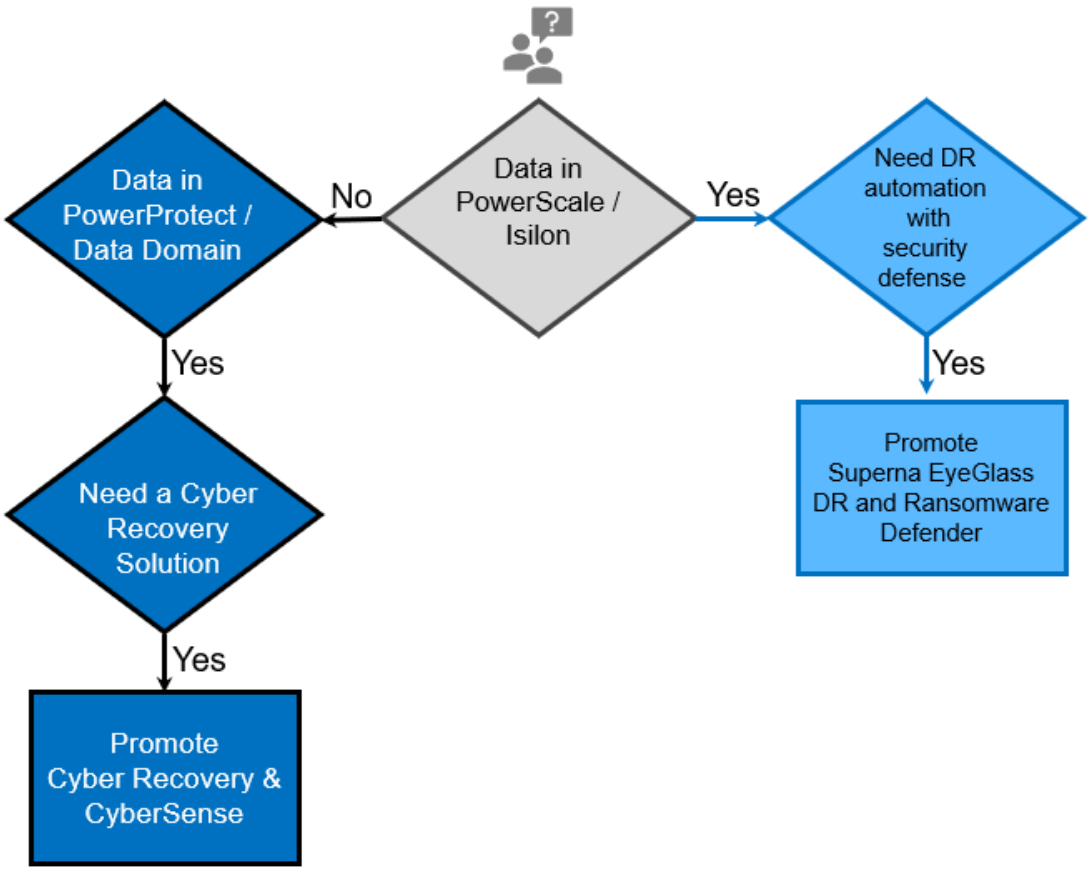


Fig: Flowchart for positioning Power Protect Cyber Recovery vs PowerScale Superna
Image source: https://inside.dell.com/docs/DOC-516693

To provide more clarity and distinction between the features of these methodologies, a table has been represented. The following table provides a complete picture of where to position Dell EMC PowerProtect Cyber Recovery + CyberSense vs Dell EMC PowerScale with Superna EyeGlass DR + Ransomware Defender. It also depicts the target platform that these technologies intend to work with and some of the key differences in those.

Product	**Dell EMC PowerProtect Cyber Recovery + CyberSense**	**Dell EMC PowerScale with Superna EyeGlass DR + Ransomware Defender**
Target Platform	Dell EMC PowerProtect / Data Domain appliances	Dell EMC PowerScale & Isilon scaled-out NAS clusters
Works with	Backup software writing data to PowerProtect/ Data Domain appliances such as PowerProtect Data Manager, NetWorker, Avamar	PowerScale & Isilon clusters only with SyncIQ data replication of production file data to a different PowerScale / Isilon cluster

Positioning:	Cyber Recovery provides resilience to data backed up in PowerProtect appliances for protection against ransomware and cybercrime events. CyberSense is an AI/ML tool which provides daily validation of the data in the vault and post attack identifies known good copies and which files to recover to get back up.	Data protection and security for PowerScale & Isilon production environments Superna EyeGlass DR provides Disaster Recovery orchestration and automation for PowerScale & Isilon Ransomware Defender detects and halts malware attacks using events/activity-based analytics
Opportunities:	For PowerProtect / Data Domain appliances customers looking for protection from ransomware & cybercrime events, lead with PowerProtect Cyber Recovery. For Cyber Recovery customers looking to have the intelligence to detect anomaly or ransomware inside vault, then lead with CyberSense.	For PowerScale & Isilon customers looking for automated disaster recovery with operational efficiency, lead with EyeGlass DR Promote Superna Ransomware Defender for PowerScale & Isilon customers looking for real-time ransomware detection to stop malware attacks and to extend security protection with air gap capability to isolate a third copy of data separate from production or DR environment
Prerequisites:	Backup and replication targets are PowerProtect /Data Domain appliances. Cyber Recovery secured vault required for the CyberSense software to perform anomaly detection.	PowerScale SyncIQ data replication is prerequisite for Superna EyeGlass DR EyeGlass DR is required for Ransomware Defender module

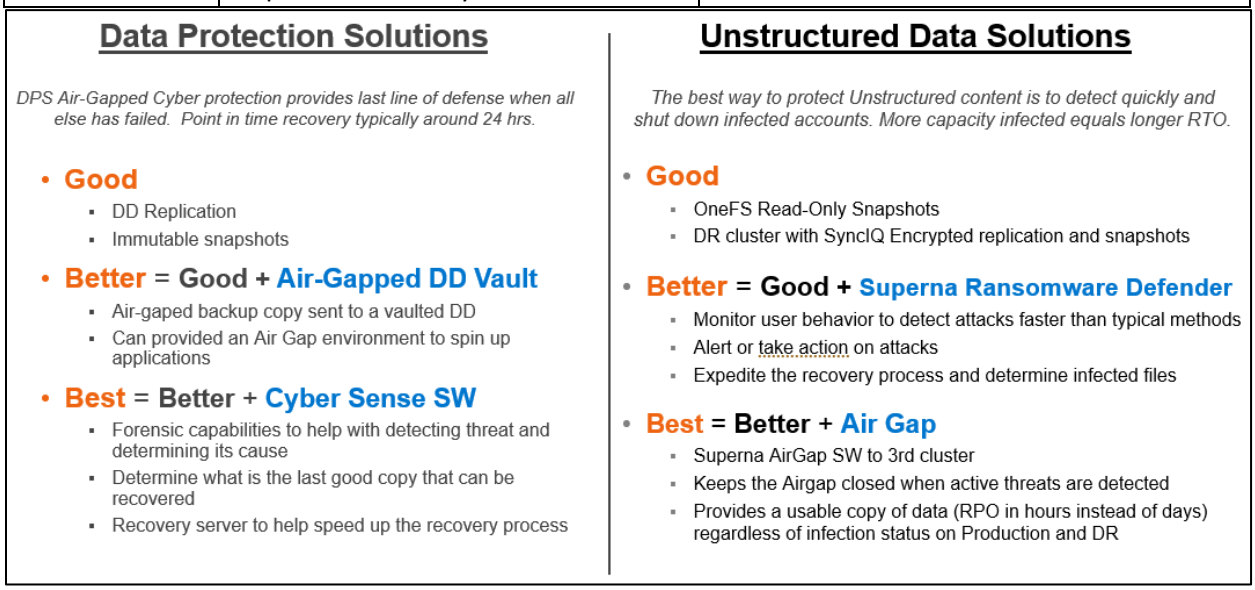


Fig: DellEMC PowerScale and Superna Airgap illustration
Src: https://inside.dell.com/docs/DOC-516693

Benefits of PowerScale and Superna Cyber Defense Strategy

Some of the key benefits of PowerScale and Superna Cyber Defense Strategy are:

- **Capability of Recovering 1PB of data in few hours** – takes days or even weeks to recover data.
- **Immutability with worm lock** - Data immutability makes sure attackers cannot alter or delete data
- **AI powered threat detection** - Monitoring production data and alerting of suspicious activity puts IT a step ahead of attackers
- **Scalable to multiple clusters** - Single pane of glass for threat detection and data isolation to protect multiple PowerScale clusters

Conclusion

The rapid threat landscape requires an updated threat response system that removes humans from the response and allows rapid multi-vector detection responses regardless of where the threat originated in the infrastructure. Ransomware is one such attack, which brings serious threat to the data integrity and development of any organization. Ransomware attacks started in 1989. Since then, it has been one of the most dangerous attacks on data. Hence, these attacks have gained global traction, with the motive of gaining monetary benefits through illegal activities. It is a growing threat to the data of businesses and because of the copious amounts of money to be made, new variants appear frequently. It can lead to the loss of sensitive information, the interruption of normal operations, and reputational damage to a business.

Superna products such as the Ransomware Defender, Easy Auditor and the Smart Airgap API for Dell PowerScale provide the ability to integrate security with intelligent, proactive data protection to keep pace with the evolving sophistication and speed of today's cyber-attacks.

This article covers the various types of threats and the importance of cyber security to tackle attacks. The paper also includes the ransomware attacks and the types. Then, we also discussed DELL EMC Powerscale's integration with Superna's ransomware defender to overcome the ransomware and cyber threats.

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

- Ryuk ransomware - https://www.trendmicro.com/en_in/what-is/ransomware/ryuk-ransomware.html
- Egregor ransomware - https://www.upguard.com/blog/what-is-egregor-ransomware

- Samsam Ransomware – https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/
- Denial of Service: https://www.coursehero.com/tutors-problems/Networking/33000022-A-DDoS-attack-occurs-when-a-a-single-machine-carries-out-a-DoS/
- Cybersecurity - https://www.comptia.org/content/articles/what-is-cybersecurity
- End point security - https://purplesec.us/network-security-types/#EDR
- UDS Cyber Protection & Recovery BDM Deck: https://www.delltechnologies.com/asset/en-us/products/storage/selling-competitive/h18808-cp-uds-cyber-protection-recovery-bdm-deck.pptx
- DPS+UDS Unified Positioning BDM Deck: https://www.delltechnologies.com/asset/en-us/products/security/selling-competitive/dell-technologies-cyber-resiliency-solutions.pptx
- PowerProtect & CyberSense vs. PowerScale & Superna: https://dell.sharepoint.com/sites/StorageCentral/SitePages/Position.aspx
- PowerScale Cyber Security: https://inside.dell.com/docs/DOC-516693
- Whitepaper: https://www.delltechnologies.com/asset/en-us/products/storage/technical-support/h19052-wp-multi-vector-defense-for-powerscale.pdf

Learn more at www.dell.com/certification