DELL Technologies

Whitepaper

Enhance Your Cyber Resilient Strategy with Dell Data Protection Solutions

A Cyber Resilient Strategy With Dell Data Protection Solutions

Abstract
At the core of any business or organization, there is an enormous reliance on data to serve customers, drive insights, develop products, grow revenue and much more. Cyber threats from external sources along with the increase of insider bad actors, make it more important than ever to ensure that the organization's data is protected and recoverable. To counter threats, organizations need to assess their risk and deploy a "cyber resilient" strategy appropriate to their needs.

December 2022

Table of Contents

Introduction 3

Dell Data Protection Perspective on Cyber Resilience 4

Incident Response 7

Protecting Other Data and Services 8

Conclusion 8

Introduction

Ransomware and data destruction attacks continue to create high levels of risk for digital driven businesses – which today is almost every business. Attacks can target organizations in any industry, any geography and of any size. To counter the threat, organizations need to assess their risk and deploy a "cyber resilient" strategy appropriate to their needs.

What is Cyber Resilience

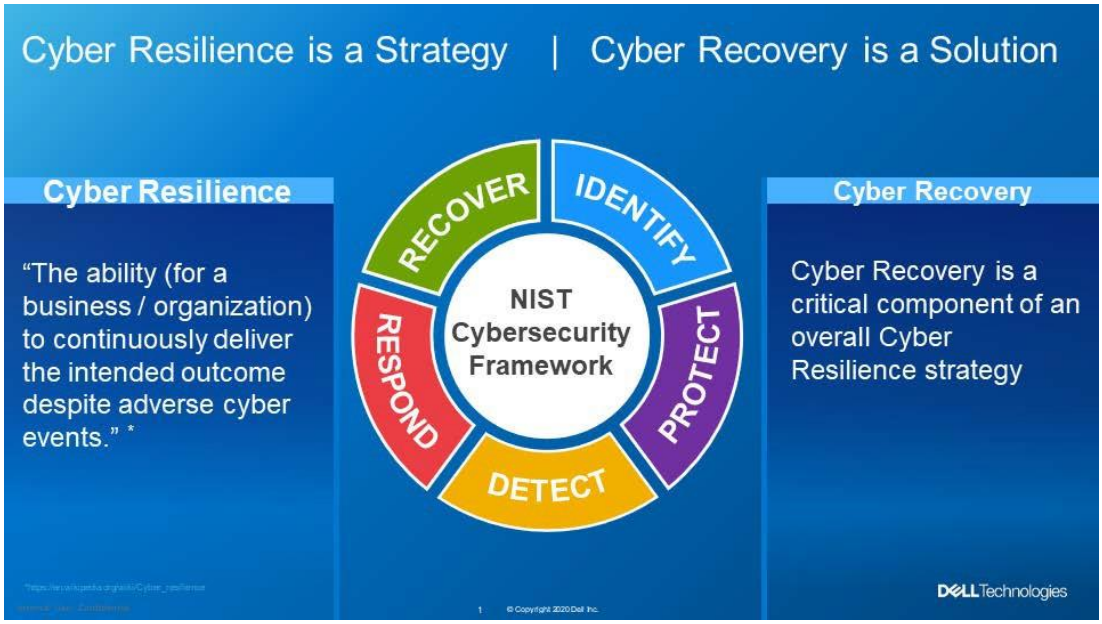
Cyber resilience is the ability to withstand, adapt to and recover from adverse cyber events. It is a strategy that includes cybersecurity capabilities such as cyber recovery but focuses more on business outcomes and requirements than on individual cyber products or controls.

A cyber resilient organization is able to withstand day-to-day cyberattacks; have resilient processes that can continue operations in the face of those attacks; and when necessary, recover those systems in a timely, efficient and secure manner.

How "Data Protection" Fits with Cybersecurity and Cyber Enhance Resilience

At Dell, data protection means safeguarding business-important information from corruption or loss and is a key component of a cyber resilience strategy. Traditionally, data protection consists of backup and disaster recovery techniques designed to enable a business to continue functioning after a physical disaster (floods, fires, power outages) or human error.

A good cyber resilience strategy starts with leveraging existing investments in data protection. Backups deliver a strong starting foundation for organizations needing to restore data that has been encrypted, corrupted or deleted in a cyberattack. But the backup infrastructure is often under attack, too. A good cyber resilience strategy must include measures against those attacks and perhaps even more sophisticated attacks.

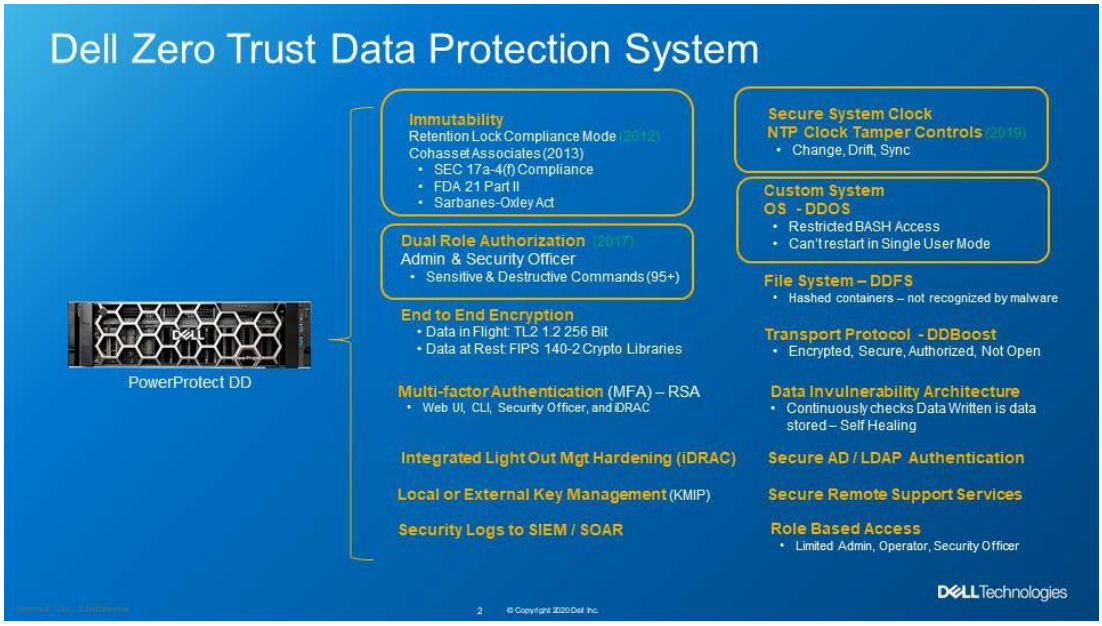


Dell Data Protection Perspective on Cyber Resilience

A full cyber resilience and cybersecurity strategy is beyond the scope of this paper. Instead, this paper focuses on using both existing and available data protection capabilities to substantially enhance your organization's resilience posture and mature its recovery capabilities.

Immediately Enhance Resilience

Bad actors frequently target the backup infrastructure so that it is not available for use in recovery operations, which would reduce their ability to obtain a ransom. That's why Dell Data Protection Solutions such as PowerProtect DD, PowerProtect Data Manager, Avamar, Networker and other solutions include built-in capabilities to substantially harden the backup environment. Dell PowerProtect DD systems provide an excellent building block for these capabilities:



An organization seeking to quickly improve its cyber resilience should immediately evaluate the following capabilities which are built into Dell Data Protection Solutions:

- **Enable retention lock.** PowerProtect DD retention lock helps protect data from being changed or deleted during a specified locking period. The Governance mode balances operations with security by enabling an administrator to override the lock. In Compliance mode, which is recommended for security purposes, there is no such override. In addition, built-in capabilities can further protect against attacks that attempt to prematurely expire the locking capability. Support for retention lock is built into Networker, Avamar (with the most recent version) and PowerProtect Data Manager, along with backup software from some third parties.
- **Protect Against Destructive Commands.** Enabling retention lock in compliance mode also enables other secure features. For example, certain destructive commands such as resetting the file system can no longer be run. Other sensitive but less destructive commands can still be run, but require authorization from a second role – the security officer - to authorize

- **Use DDBoost.** A common point of ransomware attacks is a CIFS or NFS share that is used by the backup data mover to write data to a storage target. DDBoost eliminates this mount point and also provides operational efficiencies.
- **Leverage deduplication.** The superior deduplication properties built into PowerProtect DD substantially reduce the amount of storage necessary to maintain backups, reduce the number of components that must be managed, and can cut network traffic by 99%. While these benefits are normally viewed as cost-reducing or efficiency concerns, they also deliver a massive security benefit. There are fewer components to protect, fewer switches and ports to configure, monitor and maintain, and less network traffic that must be monitored.
- **Anomaly Detection.** Organizations should also deploy the built-in capabilities of Data Protection Advisor immediately to detect and report on anomalous behavior in the backup environment. A separate paper (title / link?) provides details on how to quickly deploy this capability. Note that this capability is designed to be complimentary to CyberSense analytics used in the PowerProtect Cyber Recovery solution. Anomaly detection is designed to detect activites in the production backup environment that are not standard and could represent threat actor activity. In contrast, CyberSense in the PowerProtect Cyber Recovery vault are designed to help with efficiency and safety during recovery.

Deploy Capabilities Supporting Zero Trust Principles

All Dell Data Protection Solutions include capabilities that can be used as part of any overarching Zero Trust and/or strong cybersecurity strategy, such as:

- **Role based access controls.** Proper definition of roles can help to implement the principle of least privilege, which allows user to only perform functions necessary to their roles.
- **Persistent logging functionality.** Logs can be fed to the Security and Incident Event Management (SIEM) system, provide auditing trails and help with forensic reviews and investigations.
- **Encryption of data at rest and in flight.** Encrypting data is a well established control to protect the confidentiality of information.
- **Multi-factor authentication.** Many organizations are implementing multi-factor authentication as a protection against bad actors stealing or identifying used or previously compromised credentials.
- **Local and external key management.** Key management helps to insure that encryption keys can be rotated to protect against compromise, while also making the management of those keys safe and efficient.retention lock configuration on the PowerProtect DD itself.
- **Change the retention duration.** Although this would not have an impact on data previously stored and retention locked, it would impact policies run after the change. An increase in retention could cause storage to reach capacity while a decrease could allow early deletion of data sets.

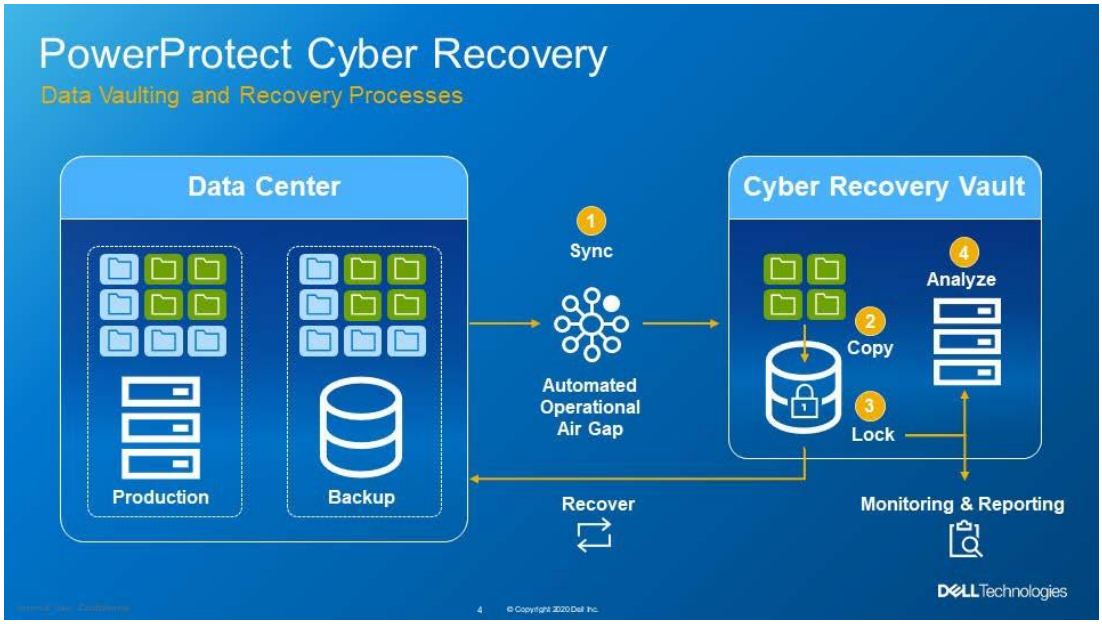
Secure Data Vaulting and Recovery

As a next step in maturing cyber resilience and cyber recovery, many organizations decide to securely "vault" a copy of select critical data and applications to provide the strongest protection against a destructive or encryption attack.

In some cases, the decision to use a vaulting capability is based upon regulatory or best practice guidelines, some of which are listed here:

Even if a regulation does not require the deployment of a secure vaulted copy, many organizations choose to do so to reduce their risk.

The PowerProtect Cyber Recovery solution is a powerful capability that protects a copy of data, providing immutability, isolation and intelligence.



PowerProtect Cyber Recovery provides many options for organizations in both deployment and operation. Organizations may deploy Cyber Recovery on-premises in their own data centers, in a public cloud, in a multi-cloud or "cloud adjacent" environment. Organizations can run daily operations and recovery in-house or they can use Dell or Dell Partners to provide those services.

You can obtain more information about PowerProtect Cyber Recovery here.

Where to start?

Two key issues that organizations must evaluate as part of a successful vault deployment process are:

- identifying data, applications and other components that should be protected in the vault; and
- planning and procedures to identify the process for recovering from the vault after an attack.

Vault Contents. The contents of the vault should reflect an organization's understanding of its key business services. At the highest level, the vault should contain whatever an organization requires to rapidly restore its most critical business services in the event of a devastating attack on the production environment. Often this information is available in a Business Impact Analysis (BIA) or similar disaster recovery planning document and can provide a valuable starting point.

Regardless, the contents of a vault normally mature over time. Start by protecting critical infrastructure components such as active directory, copies of gold images for servers and end-user devices, firewall rules, etc. From there, protect the components (databases, applications, etc.) that deliver the most important services to the business. Think of the process as delivering maturity over time.

Recovery Processes. The other critical factor in vault capabilities is understanding and planning for the recovery process. In a minor attack impacting just a few servers, the incident response process may be able to quickly re-secure the production environment and validate that the bad actors have not maintained persistence. The contents of the vault can then be accessed to recover those components – which might be virtual machines, databases, files, active directory or other components.

In more damaging attacks, more work will be required, and it will usually take the incident response team longer to determine root cause and ensure that bad actors are not persisting in the environment. In those situations, organizations may have to wait many hours or day before they can begin their actual recovery operations. Where that delay is not acceptable, organizations can plan for other recovery capabilities such as to alternate locations, clean room environments or even using the vault as a temporary production environment. Planning and training are critical components in ensuring success of more sophisticated plans but are necessary for sophisticated organizations that cannot tolerate delays in beginning the recovery process.

Incident Response

None of these capabilities exist within a vacuum, and must be integrated within an overall incident response plan that includes communications plans, integration with law enforcement, regulators and insurers, provides for the possibility of collecting evidence, etc.

Many organizations do not have these capabilities in-house, or they need supplemental assistance if a large-scale attack occurs. Meeting that need requires focused, expert capabilities to be responding and onsite within hours to assist with incident response and recovery activities. Dell's Incident Response capabilities meet all these requirements and can also be used for proactive reviews. You can find more information about Dell's Incident Response capabilities here.

Protecting Other Data and Services

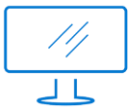
Many organizations deploy critical applications on a SaaS basis, or processing more data at the edge or even at end-user endpoints such as laptops and desktops. Many of those capabilities do not lend themselves to standard data protection techniques, so other capabilities are necessary to enhance resilience.

For SaaS offerings such as Microsoft 365 and endpoints, our APEX Backup Service provides an efficient data protection capability along with ransomware recovery capabilities.

More information about APEX Backup Services is available here.

Conclusion

Today, becoming more cyber resilient is a key focus for almost every organization concerned about the threat landscape. Leverage your existing Dell Data Protection investments to quickly become more resilient. And consider available best-in-class technologies from Dell to take your cyber resilience to the next level.



Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

View more Security Solutions Resources

Join the conversation with #PowerProtect