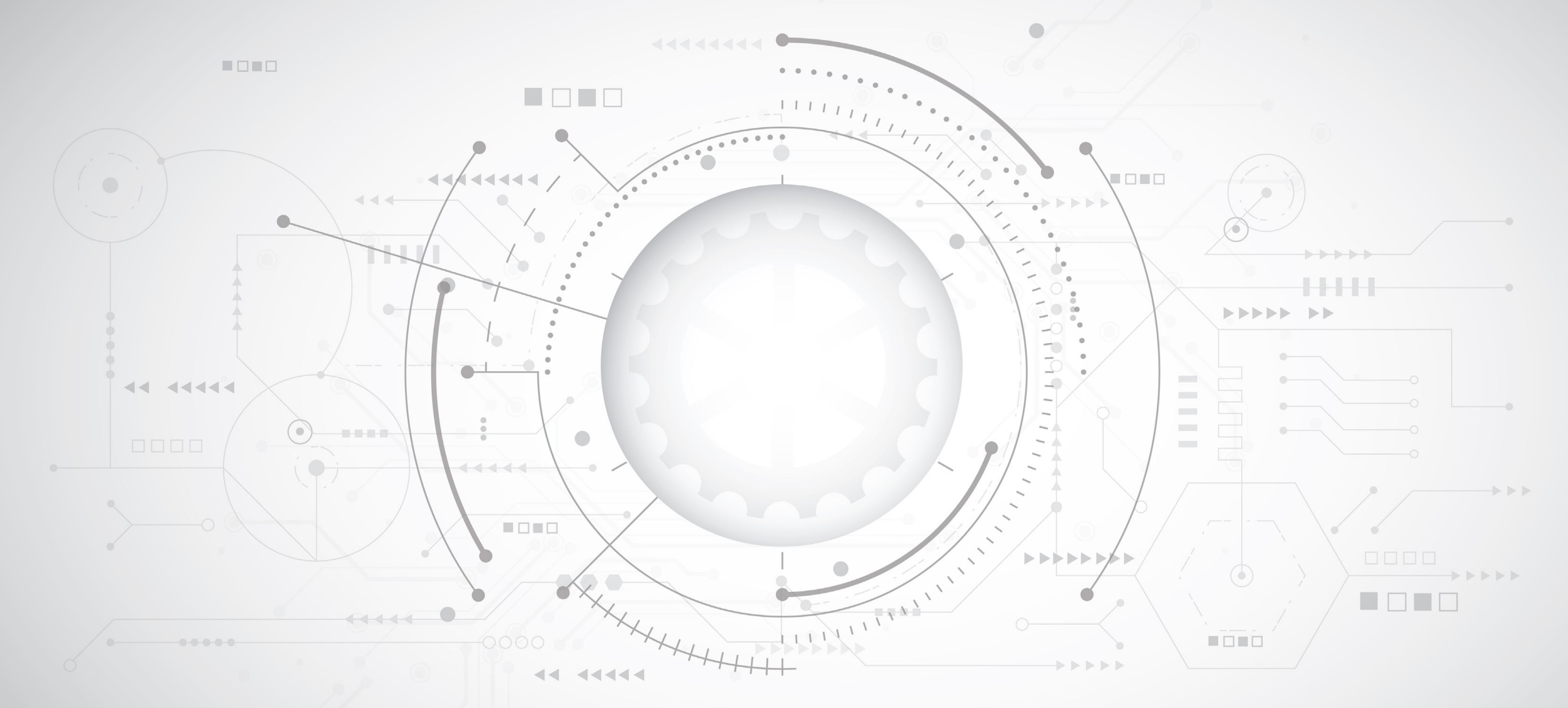


PowerScale

Cyber Protection Solution

Avgerage Cost of cyber attack by industry[1]

$18.4M	Banking
$17.8M	Utilities
$16M	Software
$15.8M	Automotive
$15.8M	Insurance
$14.7M	High Tech
$13.9M	Capital Markets
$13.8M	Energy
$13.7M	US Federal
$11.9M	Consumer Goods
$11.9M	Health
$11.4M	Retail
$10.9M	Life Sciences
$9.2M	Media
$8.2M	Travel
$7.9M	Public Sector

State of cyber vulnerability

43%
involved small business[2]

71%
are financially motivated[2]

$13M
average cost of cyber crime[1]

600,000
open reqs in Cybersecurity[3]

Cyber attacks are growing in frequency, severity and scope and it is a matter of when and not if, that organizations become a target of these attacks. On the other hand, with the rapid digital transformation happening today, data has become an organization's most critical asset. Attackers know this very well and target their attack to gain access to data that is business critical, and then either manipulate or destroy the data or hold it for ransom depending on their intent.

The cost of an average cyber attack is also on the rise, which Accenture in their annual report on Cyber Security estimates to be $13M. There is no wonder that Cyber security has become the number one priority for IT organizations. Ransomware attacks are cyber attacks where the attackers demand huge ransom against data that they encrypt and make inaccessible until their demands are met. The trouble doesn't end with ransom, increasingly governments are mandating prompt reporting of such attacks and any ransom paid. This makes cyber attacks a very public event that can have huge impact on the reputation of the companies.

Today's cyber attacks take a multi-vector approach to breach the security of IT systems to get to the data that is of high value to organizations. With access to sophisticated cyber attack tools and technology, it is much easier than ever to launch such attacks. In recent incidents like the LAPSUS$ attack on Okta, a software company in the area of Identity Management, teenagers have been found to be the masterminds behind the attack.[4] Add to this an estimated 600,000 unfilled job openings in the Cybersecurity domain. With increased ease of attack and acute shortage of qualified personnel, IT organizations need to take a more comprehensive detection and resilience approach that goes well beyond the traditional network security best practices. In this eBook we particularly discuss how to fortify the data layer.

[1] https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
[2] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[3] https://www.bloomberg.com/news/articles/2022-03-30/hackers-path-is-eased-as-600-000-cybersecurity-jobs-sit-empty
[4] https://siliconangle.com/2022/03/23/teen-hacker-linked-lapsus-okta-provides-details-data-breach/

Consequences of cyber attacks

Disrupted Operations

A cyber attack can disrupt operations, causing a service to become unavailable for your partners and customers, potentially causing a ripple effect (e.g.: Recent attack on Colonial Pipeline)

Data Theft/ Breach

Cyber attackers try to target data that is most critical for an organization like medical records data for Health care organization, the media files related to the latest movie from a reputed studio, files with sensitive pricing strategies of a retailer and so on. With regulations like GDPR there is a very high price for organizations to pay in case of data protection lapses that can lead to data breaches.

Ransom Money

Although not advised, some organizations pay a ransom to prevent an attack or recover from a cyber attack. This is very expensive and how can you be sure that another attack isn't following?

Business Reputation

In recent times cyber attacks and data breaches have often lead to lost business reputation that takes years to re-build. With strict regulations that require prompt reporting of breaches as well as any ransom paid, these attacks can hardly go unnoticed.

Insuring against cyber attacks

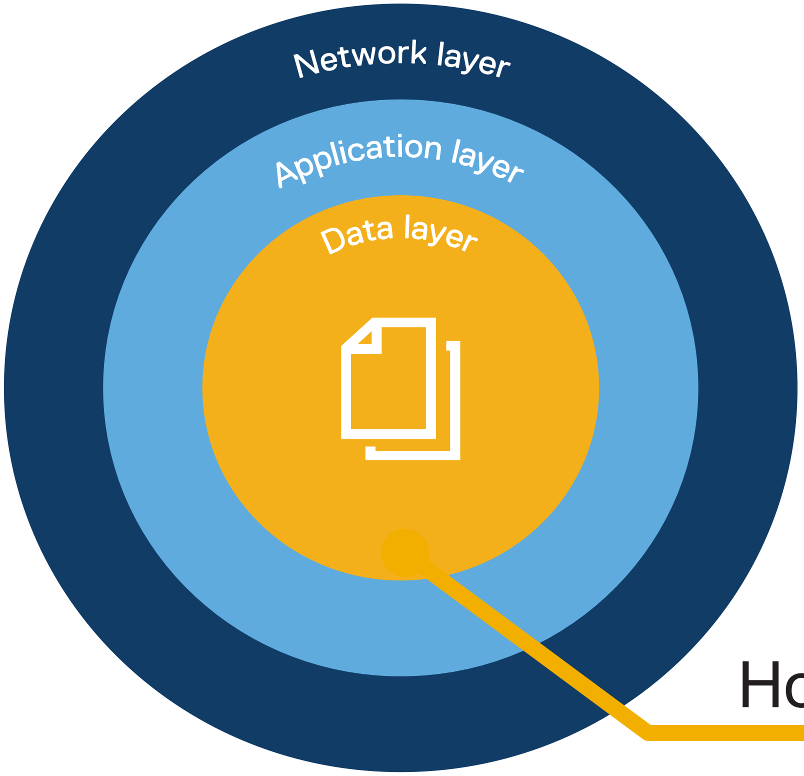
What does your insurance cover and what is the deductible?

There are several components that increase the financial impact of a Ransomware attack. In the wake of an attack, thousands of man hours are required to fully assess the scope of the attack and determine data and systems impacted as well as recovering data and restoring business critical applications. Then there is the cost of operational disruption to key business functions that impacts the top line revenues of business units. The increasing regulations mean potential fines and legal expenses. The insurance industry is therefore raising the self-insured retention (deductible) for Cyber events and encouraging companies to boost their good cyber defenses and attack resilience.

> “We currently have a $20M per loss self-insured retention….the insurance market was pushing it to $50M.
>
> Anything a corporation can do to mitigate its risk is key… if you don’t have the right processes in place, you are going to have a difficult time even getting insurance.”

– **Julie Young,** Dell Technologies

Cyber defense at the data layer



Cyber Security tools and frameworks exist across the IT ecosystem. Most of these are attack detection mechanisms at the end-point, network and application access layers and understandably so given these are the layers attackers need to get through to reach the all-critical data layer. Some of these include:

- End-point security tools like anti-virus, anti-malware, anti-phishing tools
- Network intelligence through advanced firewalls
- Identity management and access control
- SIEM systems to detect threats from infrastructure logs

Now the question is how intelligent and fortified is the data layer itself to detect the actual data manipulation employed by attackers. We present a cyber protection and recovery solution that is acting at the data layer that boosts the overall cyber resiliency of your business operations that depend on data!

How do you fortify **the data layer?**

Introducing cyber resiliency at the data layer

DATA ISOLATION

Network separation is a critical component of Cyber resiliency: this is the last defense at the data layer

INTELLIGENT DETECTION

Monitoring data access for suspicious activity puts a step ahead of attackers by limiting the damage

RAPID RECOVERY

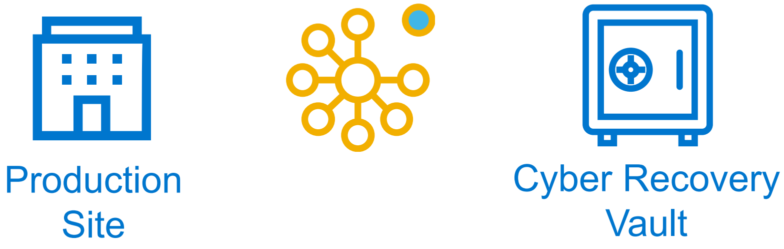
Not all airgap targets are the same. A petabyte of data on PowerScale can be recovered within a few hours!

Intelligent airgap

Isolate
Smart Airgap

IT teams are well aware of traditional data copies like backup and DR copies. Cyber Recovery at the surface appears to be almost identical implementation of Disaster Recovery but there are some key differences. The main difference is that a Cyber Recovery copy is completely isolated from the primary network using an airgap mechanism. This means that incremental syncing of the cyber recovery copy cannot happen continuously because of the airgap. Instead a smart airgap establishes intermittent connection between the two copies only after checking for the absence of any alerts indicating a compromise.

Selection of storage target is also a key decision that determines the speed of data restore. In case of PowerScale Cyber Protection solution the cyber recovery storage platform is also a PowerScale. This accelerates data recovery and restore to just a few hours for a petabyte of data.



Production Site

Cyber Recovery Vault

Powered by Superna **Enterprise Airgap**

DR versus Cyber Recovery

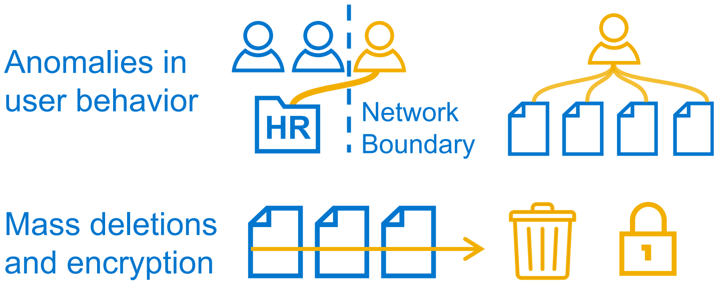
While disaster recovery is a well-established framework of managing a secondary datacenter that the applications can be failed over to, from the affected primary datacenter. Cyber Recovery at the surface appears to be almost identical implementation of Disaster Recovery but there are some key differences. The main difference is that a Cyber Recovery copy is completely isolated from the primary network using an airgap mechanism. This means that incremental syncing of the secondary copy cannot happen continuously in case of cyber recovery storage because of the airgap. Instead a smart airgap establishes intermittent connection between the two copies only after checking for the absence of any alerts indicating a compromise. Following is a summary of the key operational differences between traditional Disaster Recovery and Cyber Recovery.

	Disaster recovery	Cyber recovery
Protection against	Natural disasters, localized outages	Cyber attacks with the intent to destroy or alter data or to hold data for ransom
Network connection	Connected for continuous replication	**Isolated** with intermittent replication.
Location	Remote	Local or remote
Admin privilege	IT admins	Restricted to CISO
Failover purpose	To support most of the business operations	To support only the most critical operations

AI powered detection

Detect

Real-time threat detection at the data layer

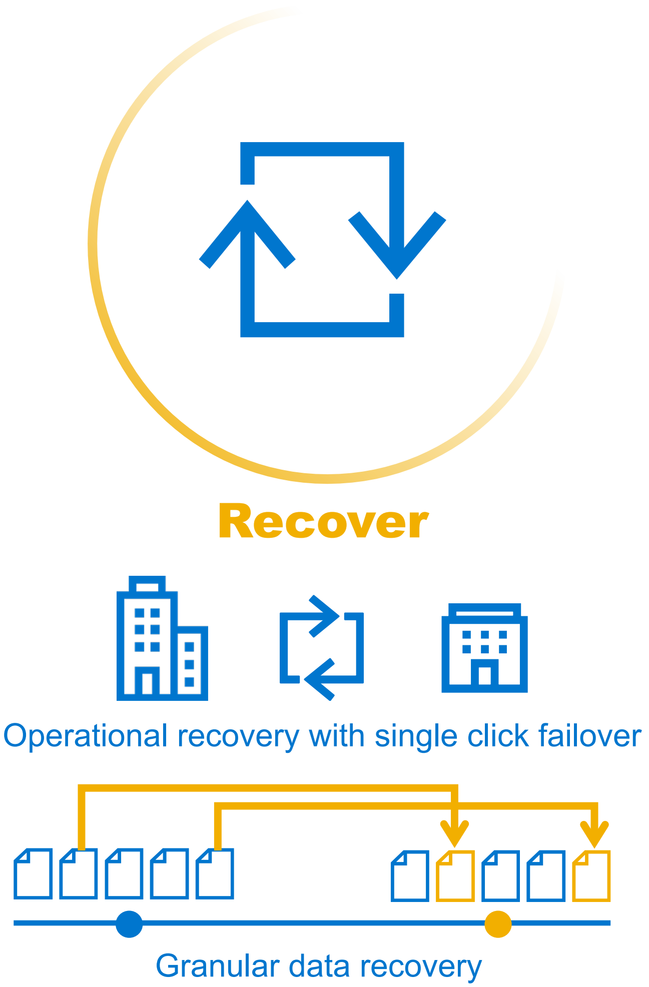


Anomalies in user behavior

Mass deletions and encryption

Cyber security is a great use case for Artificial Intelligence and Machine Learning and has been extensively used to identify anomalies in user behavior on networks and applications. Ransomware Defender extends this further to the data layer by looking for patterns of data access that are indicative of compromise. The detection system learns over time what is normal behavior for a particular application or volume in terms of the different user groups, the network paths they normally use and the files that are used. With this baseline the system can detect anything out of the ordinary and generates alerts. Admins can also use these even triggers to setup automatic response actions like blocking certain users, creating more snapshots, terminating any replication to the airgapped copy and so on.

Single click failover and rapid data recovery



Recover

Operational recovery with single click failover

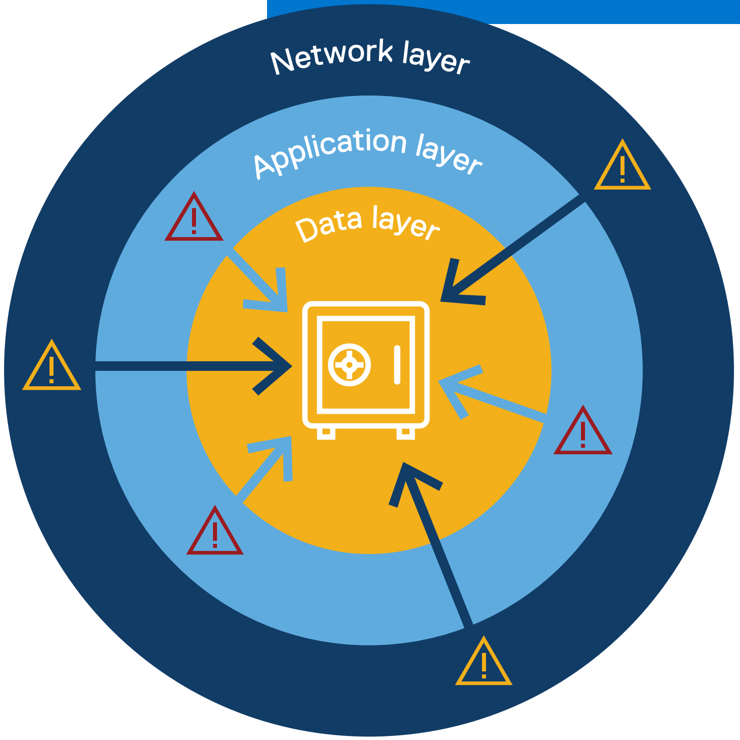
Granular data recovery

Recovery is a key step in the cyber resilience and preparedness and many of the processes are directly performed or monitored by someone like a Chief Information Security Officer (CISO). From an operational recovery standpoint a CISO may decide to give very selective applications and users access to the vault copy to minimize the disruption to business operations. The continuous monitoring of DR readiness ensures that there are no surprises in terms of RTO compliance at the time of failovers. From a data recovery standpoint the granular snapshots help to restore only affected files while keeping the latest version of the unaffected files.

Zero Trust API

Respond to suspicious activity at network and application layers

API alerts from network and application layers enable rapid response at the data layer



The Zero Trust API enables cascading of security events that are at multiple layers of the IT ecosystem to the data layer (Dell PowerScale Cyber Protection). The API provides an integration point to connect detection systems at the network and application layers, for example email gateways, Intrusion detection system, Firewalls, SIEM tools, endpoint protection etc. By connecting these threat warnings to the intelligent storage layer defenses, the Zero Trust API can provide a hand off for decisions and responses to the storage layer to take proactive actions to safeguard the data before the impending attack advances.

Learn more: white paper ↗

Resources

Product Overview: **Explainer Video**

Solution Brief: **PowerScale Cyber Protection**

Solution Brief: **Cyber Protection Solution for ECS Object Storage**

Solution Brief: **UDS Cyber Protection & Recovery for Government**

Solution Brief: **UDS Cyber Protection & Recovery for Healthcare**

White Paper: **Zero Trust API: Integration with Network & Application Layers**