FACTION®

Multi-Cloud Cyber Recovery Strategy for Dell Technologies PowerScale, Superna and Faction

Author:

Ray Kalmbach - Field CTO Alliances

Purpose:

In this document we look to examine a comprehensive strategy for cyber protection and restoration in reference to file and block data on Dell PowerScale platform in multi-cloud environments.

- The Current State of Cyber Attacks
- How are the Bad Actors Doing It
- Differences Between Disaster Recovery (DR) and Cyber Recovery (CR) Strategies
- Framework of a Comprehensive Cyber Recovery Strategy
- What's Needed to Protect Multi-Cloud Environments
- What's Needed to Recover

The Current State of Cyber Attacks

Cybercrime, including ransomware attacks on data, is seeing a 15% increase year over year, and is estimated to reach $10.5 trillion annually by 2025 (ref #1).

Customers large or small in all segments must start asking not if, but when are we going to have a cyber or ransomware attack?

- Healthcare
- Financial Services
- Oil & Gas
- Manufacturing & Retail
- Government

The days of these bad actors accessing data and practicing corporate espionage on the dark web are in the past. Criminal organizations have found it much more profitable and easier to delete and/or encrypt your data and attempt to hold it hostage, forcing you to pay large ransom amounts in the hopes they will have integrity and provide you with the correct encryption keys.

For example Darkside, the criminal organization responsible for the Colonial Pipeline attack, stated,

"Our goal is to make money and not create problems for society."

Regardless of your organization's size, you are not immune to a ransomware attack. The new reality is that you must have a comprehensive strategy in place for not if, but when that attack comes.

Differences Between DR and CR Strategies

When we think about a cyber recovery strategy it's important to recognize and understand the difference between this strategy and what we may normally consider a disaster recovery plan.

A DR strategy is going to be a plan to mitigate against:

- A natural disaster
- Regional outage
- Mass hardware failure
- Planed code, application, or infrastructure changes that have unforeseen outcomes

These remediation strategies will include connected systems, backups, tools and resources to bring your restoration and business continuity plans online and active.

A CR strategy should be to protect against:

- Malware/ransomware exploiting data on your network, shared and not shared
- External threat actors that have breached your network security
- Internal employees with infected systems unknowingly giving access to your network
- Rogue employees that have been compromised for financial gain or political/social activism
- Infrastructure compute, storage, networks and backups that have been compromised or are untrusted

Framework of a Comprehensive Cyber Recovery Strategy

The National Institute of Standards and Technology (NIST) framework breaks this strategy into 5 key pillars and should be considered requirements for a comprehensive strategy they refer to as CCRS.

https://www.nist.gov/cyberframework

Identify

Understanding your data and what format it exists and everywhere it exists

- Is it on-prem in your physical infrastructure?
- Do you have data outside of your on-prem environment?
- Is data in use in any of the public clouds providers such as AWS, Azure or GCP?

Protect

Do you have tools in place to protect the various data formats in your on-prem and cloud environments?

Detect

What tools are in place, not only at a network layer but also at a data layer, to inspect and recognize when an attack or threat is happening?

Respond

How do these tools respond, mitigate and then notify you of an attack?

Recover

In the case that your current infrastructure is untrusted or in quarantine by law enforcement for forensic analysis, where are you recovering the data to?

How long can you be without access to your data? What is your Recovery Time Objective (RTO) time before serious financial, legal and/or social reputation damage is done?

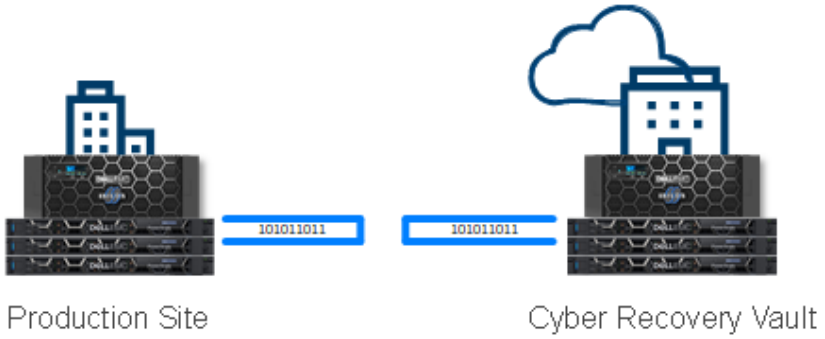
Cyber Recovery Solution

As you *Identify* your sensitive data, and as an Isilon, PowerScale customer, you can use Superna's Eyeglass suite of products combined with Dell's Multi-Cloud capabilities powered by Faction, to easily create a comprehensive cyber recovery solution that maintains the security of the data via an air gap for protecting your file data on-prem and in multiple cloud environments.

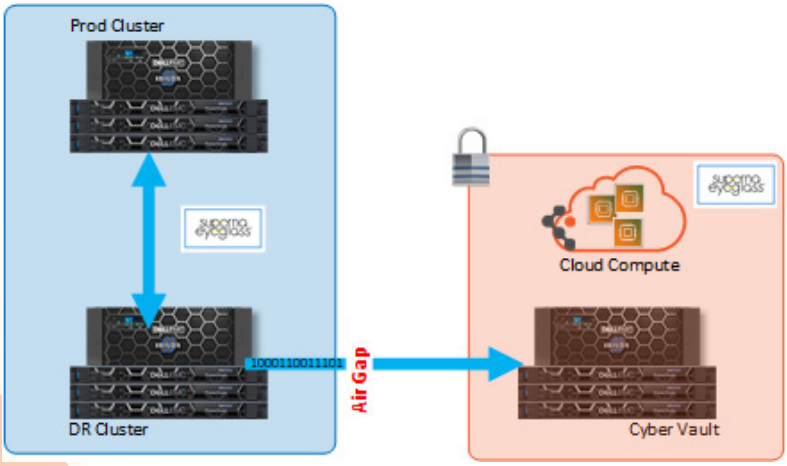
The 2nd pillar of the NIST CCRS is *Protect*. When protecting your most sensitive data, it is critical to have the data replicated to an air gap protected vault.

What is an air gap?

"An air gap, air wall, air gapping[1] or disconnected network is a network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.[2] It means a computer or network has no network interfaces connected to other networks" – Wikipedia



With Superna's Eyeglass Data Protection Suite [(https://www.supernaeyeglass.com/products)](https://www.supernaeyeglass.com/products) deployed onto Faction, your sensitive data is replicated to Isilon/PowerScale appliances located in Faction where the data is air gapped in an offsite location in a protected cyber vault.



Here, the challenges and additional financial responsibilities around maintaining an offsite data center or co-lo space is alleviated along with eliminating the internal bad actor threat from physically accessing your vaulted data.

With solutioning for the Detect, Respond and Recover portion of NIST CCRS, Superna's Eyeglass meets these challenges with their Data Protection Suite which includes;

Ref #1
https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

Eyeglass DR

Eyeglass Dr offers a full failover automation, DR readiness monitoring, data migration tool using SyncIQ performance and RPO monitoring, Continuous DR testing, 3rd copy SAN box DR testing, cluster configuration reporting and change tracking.

- Replicates configuration data, quotas, permissions & shares on the DR side
- Automates failover/failback with several options (Microsoft DFS, Access Zone, and/or per SyncIQ policy)
- Provides Isilon configuration reports, RPO/RTO trend reporting
- DR readiness testing with DR RunBook Robot
- DR rehearsal mode
- Isilon to Isilon migration
- LiveOps DR testing (test DR without impact to production)

Ransomware Defender

Real-time per user behavior-based detection, per user lockout automated response and file system data protection and recovery automation with snapshots.

- Reduces the impact of a malware attack, accelerates recovery, root-causes the source of the breach and protects data from inside threats
- Automated security penetration testing ensures defenses are fully operational by testing detection and lockout on a scheduled basis
- AirGap 2.0 feature monitors copy jobs and protects/secures a third copy of data throughout transfer

Easy Auditor

Real-time active-auditing features with scheduled reporting for auditing compliance

- Real-time detection of security audit conditions: mass file delete detection, data loss prevention of secure shares, “Where did my folder go?” detects folder and file renames/deletes by users
- Real-time wiretap a user, share or path to see all file activity as it happens for security auditing and logging
- Policy-based real-time response to audit events
- Scalability: support for billions of audit records with inline compressed HDFS storage on Isilon. Can scale to any size cluster with scale out auditing
- Parallel Syslog forward to Syslog with conditional forwarding feature. High performance syslog forwarding
- Easy Auditor platform can extend the vault auto close replication criteria using Easy Auditor active auditing, protecting the vault data by using built-in triggers for DLP, Mass delete or even custom triggers to control vault replication. This allows user aware, network aware policies that can halt replication for any active events.

Reference Architecture

Protection

As we look at implementing a comprehensive cyber protection strategy, the Superna Eyeglass suite of products has made this effortless and seamless. The solution starts with using Eyeglass DR to leverage and manage the cluster's native tool, SyncIQ, to replicate the data from the production cluster to the DR cluster where it undergoes inspection in real time with Eyeglass Easy Auditor.

Deployment

Eyeglass

To start deploying Superna Eyeglass please download the Eyeglass OVF, VHDX from Superna web site following instructions here: Latest Appliance Download

Eyeglass is delivered in an OVF format for easy deployment into your vCenter environment. Deploy the OVF and then follow the wizard to set up networking for this Linux appliance.

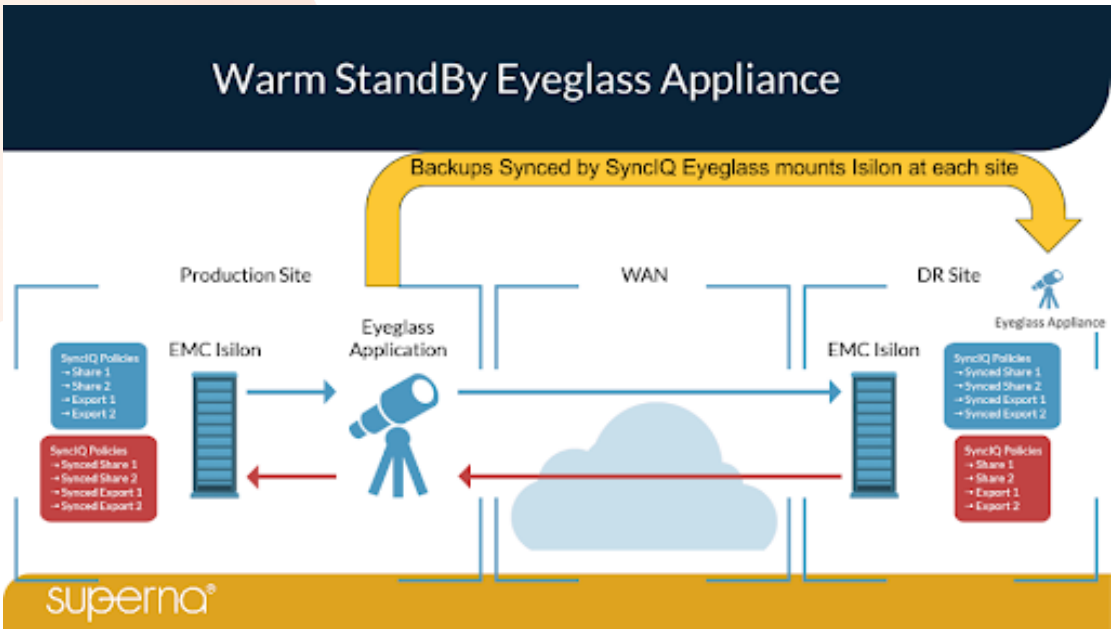
Thing you will need to know:

For detailed instructions please reference: Eyeglass PowerScale Edition Quick Start Guide

Eyeglass DR, Easy Auditor and Ransomware Defender

Eyeglass DR, Easy Auditor and Ransomware Defender are delivered and deployed in an Eyeglass Clustered Agent vAPP format. For specific install instructions please reference: Eyeglass Clustered Agent vAPP Install and Upgrade Guide

Note: DR and Easy Auditor should be deployed in a "Warm Standby" configuration.



For this protection model please reference deployment instructions found here:

[Superna Eyeglass Start Here]

[Eyeglass Warm Standby Direct Sync Guide]

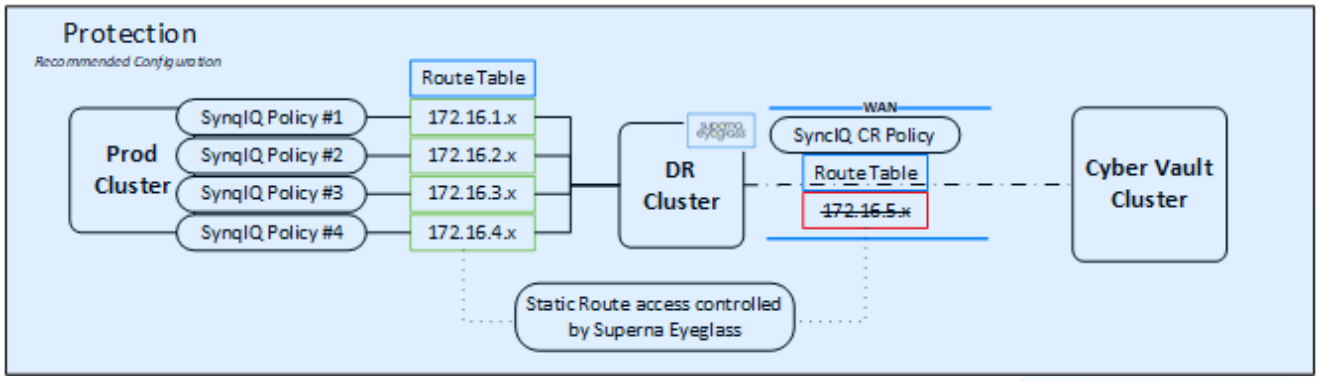
WAN Connectivity

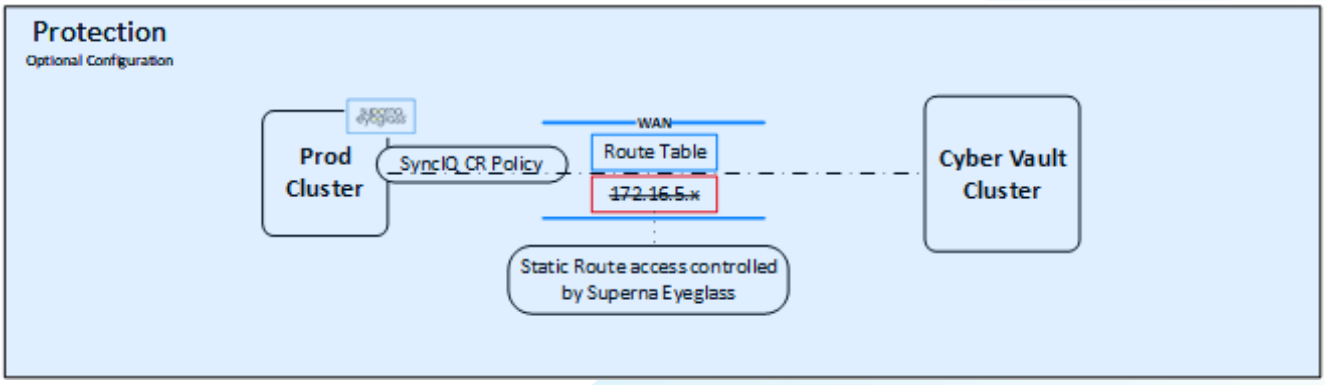
When considering WAN connectivity options, data throughput should be the highest consideration. The goal of the WAN connection should be to get the data and taking into account the change rate moved to the cyber vault as quickly as possible. The goal should be to have the data path for access to the vault accessible as little as possible.

Cyber Vault

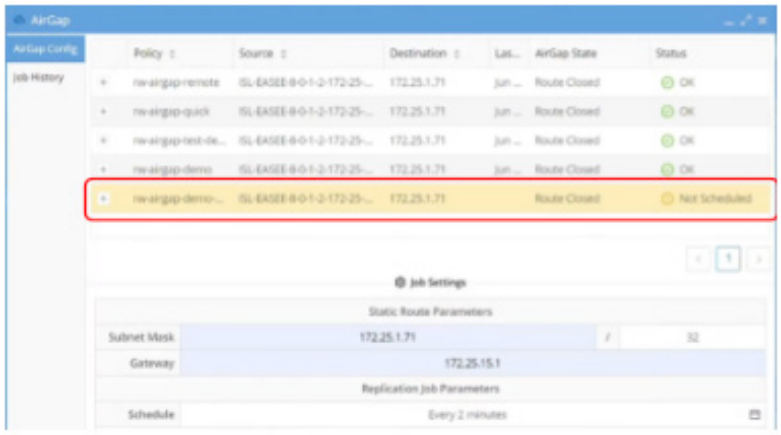
The Cyber Vault Cluster should be located in a 3rd party solution limiting who has physical access to the data. This naturally creates a seperation of duty and can mitigate the risk of physical damage to the arrays storing the data. This is no different than a normal standard 3-2-1 DR strategy where you should keep your cyber vault in an offsite location. By having this 3rd copy of the data in an offsite location, you protect it from unforeseen disasters and from bad actors by eliminating their physical access to the data.particular cloud

[Buyers Guide to Cyber Vaults]





Now that the data has been protected from a DR perspective, inspected and audited on the DR cluster, we can now use Superna's Ransomware Defender to control the virtual air gap by maintaining the static routes that the SyncIQ policies have access to. By managing the static route used to access the cyber vault cluster that the SyncIQ policy has access to, while the route is disabled, the data in the cyber vault cluster is protected.



Recovery

When performing a recovery, the ability to use the same tools from the protection strategy are vital. If the on-prem environment is still available, we can simply reverse the SyncIQ policy back to the DR cluster where replication from it to the production cluster is seamless. Only having to replicate the changed or altered "bits" back to the prod cluster makes the RTO times much shorter.

If the on-prem environment isn't available, due to being compromised or under confiscation by legal authorities, this creates a major challenge. Designing a recovery solution that can support different and/or multiple recovery options becomes paramount. A solution that has the capabilities to restore to a private hosted environment, virtual cloud infrastructure, cloud native solutions or VMware Cloud solutions on the public hyperscalers can lower your RTO

Deployment

Cyber Vault

From the protection deployment, this should already be deployed and configured.

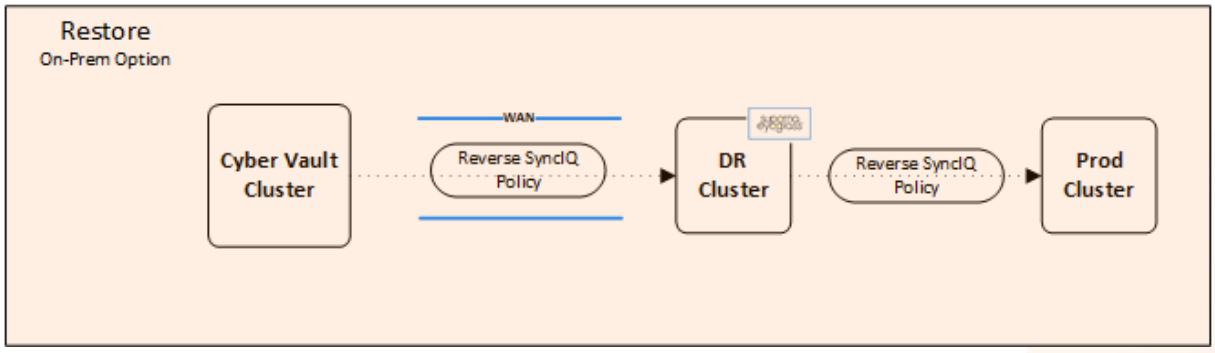
Additional compute resource in the form of a ESX environment is needed to support the deployment of the Eyeglass OVA and the Eyeglass DR vAPP to manage the restoration process.

WAN

Continuing from the recovery deployment, the WAN connectivity should already be established and should be able to support the replication of restored data to meet the desired RTO.

DR and Production Clusters

DR and production clusters should be fully vetted to ensure they are not compromised and are fully trusted before data is replicated back to the environment.



Framework of a Comprehensive Cyber Recovery Strategy

Cyber Protection

Additional compute resource in the form of a ESX environment is needed to support the deployment of the Eyeglass OVA and the Eyeglass DR vAPP to manage the restoration process.

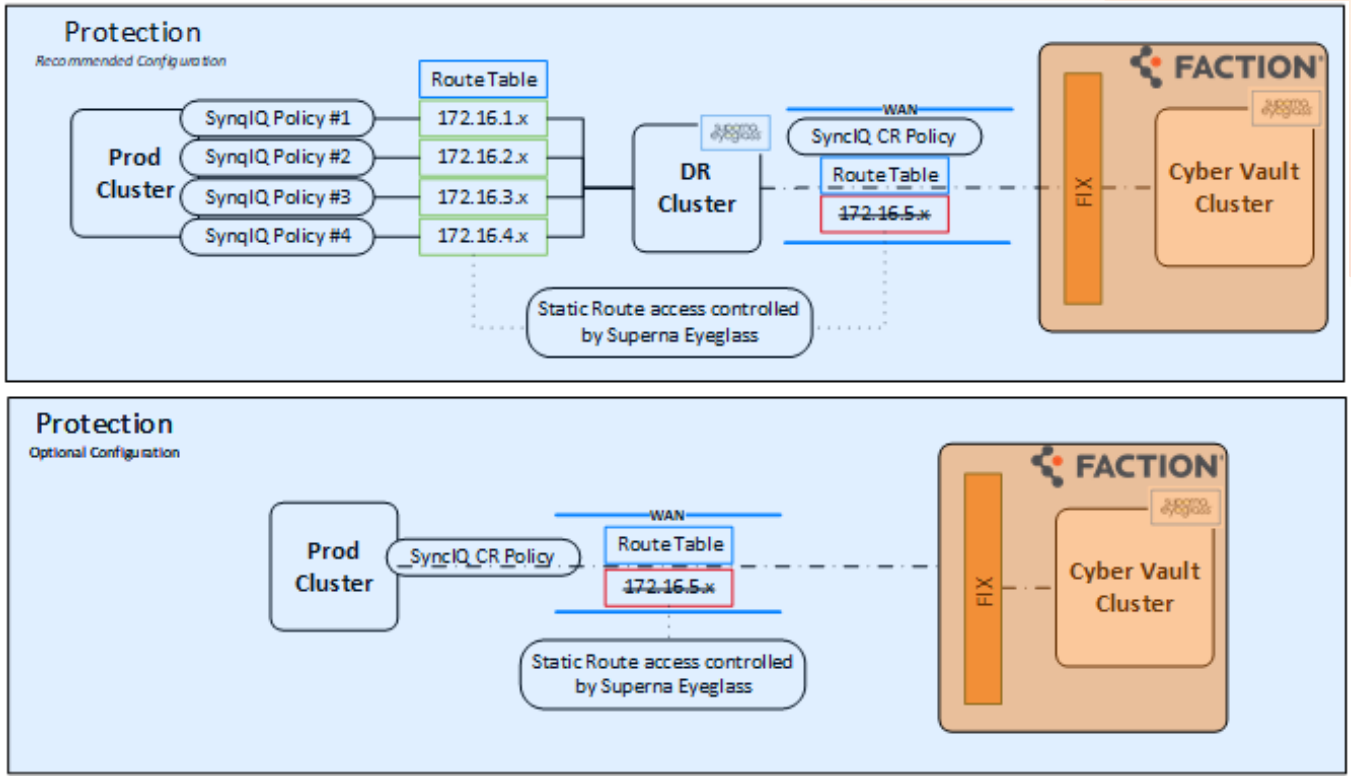
In current times when all businesses are finding themselves targets for cyber and ransomware attacks, protecting workloads and data from attacks can be a daunting task. When deploying a cyber protection strategy on-prem there are ancillary components and supporting services that need to be accounted for when architecting a well-designed solution:

- Floor space that is flexible and can scale when needed
- A secure data center cage
- Physical security
- Controlled access to the cage
- Physical racks, power, cooling
- Data center engineering
- Hardware monitoring
- Hardware patching and failure remediation
- Remote hands
- Support

Delivering These as a Service

When investing in your cyber recovery strategy with Faction, these ancillary and supporting services are included in your cyber protect and recovery strategy. By providing a hosted and secure virtual vault, the added capex expense and tasks are included:

- Virtual Vault
    - Floor space
    - Secure cage
    - Physical security
    - Controlled access
- Physical Racks, Power, Cooling
- Data Center Engineering
- Resources for VMware Environment
    - VMware licensing (6.7 Enterprise Plus)
- Hardware Monitoring
- Hardware Patching and Failure Remediation
- Remote Hands
- Support



Cyber Recovery

Recovering from a cybersecurity incident can be a daunting undertaking, but you can limit the damage to your company and your reputation by developing a solid recovery plan in advance and proactively test your ability to restore your data. It's not just about protecting your data; you must also have a strong recovery plan. What happens to the applications producing and consuming that data?

During a cyber attack, how do you get your internal and external customers back online? A strong response plan addressing what happens after the attack is key.

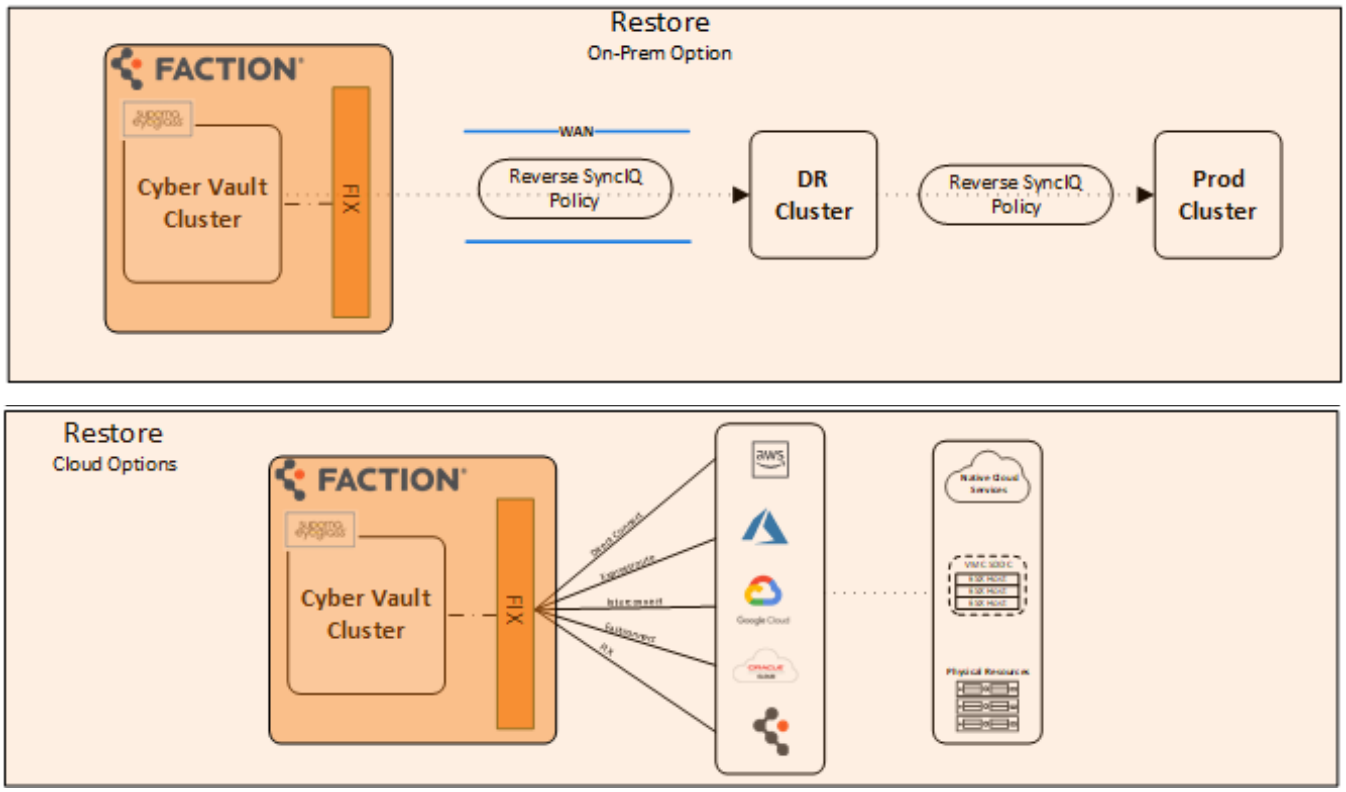
This means you must think about your recovery motion:

- First, can I ensure the integrity of my data that is being recovered?
- Where am I going to recover the data and my apps to?
- What's my RTO?
- How are my internal and external customers going to access the data and apps?
- How do I protect the new data that is being created during the current attack?
- What is my role back strategy; how do I get my data back to my primary site after it has been secured?
- How do your teams manage the recovery infrastructure while they are trying to handle the active attack?

Assuming the environment is on lockdown or untrusted, in an on-prem strategy you must have a clean room environment on standby. These are resources and costs that are incurred even though they aren't actively being used.

The resources to build out an on-prem recovery environment (cleanroom) could include:

- Professional services for setup
- Co-location: upfront and monthly costs
- Power and cooling, racks PDUs
- Networking (firewalls, routers, switches)
- Monthly remote hands
- External connectivity (carrier services)
- Hardware support contracts
- Software support contracts
- Engineering labor (time and money spent managing the physical infrastructure)
- 24/7 proactive monitoring tools
- Public cloud connectivity (hyper scalers)



The Faction Cyber Recovery solution answers these needs and includes them into the Faction Cyber Recovery platform:

- Environment setup
- Co-location: upfront and monthly costs
- Power and cooling, racks PDUs
- Networking (firewalls, routers, switches)
- Remote hands
- Hardware support
- Engineering labor
- 24/7 proactive monitoring
- Uptime SLAs
- Public cloud connectivity (hyper scalers)

The Faction Cyber Recovery platform simplifies these challenges by offering multiple recovery clean environment options that can be added to the cyber protection proposal and used for proactive testing.

- Private pre-staged compute
- Virtual VMware Cloud environments
- Public cloud options

Conclusion

With criminal and nation-state hackers ever increasing their presence and targeting connected data to compromised internal or disgruntled employees, the need to have a comprehensive cyber protection strategy could never be more critical. The ability to protect against the financial cost and the reputation damage in the form of system downtime, outages, and in conjunction with financial cost of paying a ransom, could never be more paramount.

The best disaster recovery plan does not solve the challenges around a cyber-attack. When backing up data, if it's encrypted by ransomware, there is a chance you are backing up bad data.

The Superna Eyeglass suite of products deployed on the Multi-Cloud Cyber Recovery platform by Faction provides a strong plan to replicate the data to an air gapped cyber vault that also mitigates physical access concerns.

By also offering a recovery solution that offers multiple recovery options including the ability to recover back on site or into a private hosted solution, virtual infrastructure or native cloud service with the ability to proactively test the recovery and it's RTO, you can be sure to defend and recover from a ransomware attack effectively and efficiently.

Contact Us

Want to learn more, or have questions or comments?

Reach out to us.

www.factioninc.com

1855-532-4734

@factioninc