Enterprise Guide to Cyber Resilience

Organizations are grappling to safeguard their data assets against an ever-broadening array of risks, including malware, ransomware, and potential breaches in cloud security. The rise in cybercrime, coupled with the widespread adoption of public cloud services and the emergence of hybrid and multi-cloud architectures, has significantly extended the scope of vulnerabilities that businesses must address. To ensure uninterrupted access to data and application continuity across diverse hybrid and multi-cloud application and network infrastructures, there needs to be a shift in how we approach data protection strategies, including vault, backup, and recovery solutions.

It is more important than ever to focus resources on protecting high-value, high-risk data, including application data that, if compromised, would affect the availability of mission-critical applications. A strategy of physically isolating data in an off-prem, off-cloud infrastructure provides maximum protection and operational efficiency by consolidating backup and vault data and applications across multiple clouds. Off-cloud backup and recovery solutions ensure flexibility, allowing applications to be recovered to any compatible cloud platform without the upfront cost of deploying and managing compute resources, thus optimizing test and recovery processes.

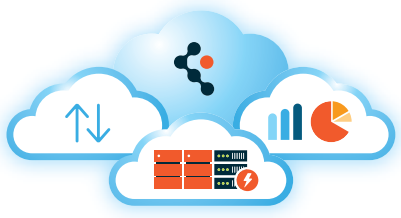
By leveraging the Faction® Multi-Cloud Cyber Vault solution, organizations can protect mission-critical data and ensure operational continuity for data and applications residing in distributed infrastructure environments, including one or more public clouds and on-prem infrastructure. Valuable features of the Multi-Cloud Cyber Vault include:

- Physical isolation of your data within the vault environment via off-prem, off-cloud infrastructure
- Air-gapped and immutable copies with timed backups
- Access to CyberSense software paired with Dell PowerProtect hardware
- A seamless path for data and applications recovery to either one public cloud, or multiple clouds, and/or on-prem environments

Additionally, Faction's Multi-Cloud Cyber Vault solution provides a seamless path for data and applications to recover to one or more public clouds (including multiple availability zones) and/or on-prem environments. This ensures the availability of clean-room resources and facilitates recovery to an uncompromised application environment.

Industry Drivers That Necessitate a Multi-Cloud Cyber Vault

In light of escalating cyber threats and the growing complexity of cloud environments, the question arises: Why is now the right time to consider a Multi-Cloud Cyber Vault for increased cyber resilience?



Distributed Hybrid and Multi-Cloud Environments

The adoption of public cloud and multi-cloud environments — including hybrid and multi-cloud architectures — expands the attack surface available to cybercriminals. It also introduces greater complexity associated with protecting a distributed application footprint, spanning both cloud and on-prem environments.

Hybrid and multi-cloud infrastructure models require a centralized and physically isolated backup and vault solution that is capable of supporting a distributed application footprint and facilitating recovery across multiple cloud and on-prem environments.

Escalating Threat from AI

In addition to more common cybersecurity threats (e.g., phishing, malware), a new foe has emerged – cybercrime powered by Artificial Intelligence (AI). In fact, a recent cybersecurity report published by CFO.com found that 75% of security professionals reported an increase in cyberattacks, and 85% attributed that rise to bad actors using generative AI.

Operational Disruptions

Application unavailability due to cyberattacks and ransomware can cause significant financial losses and reputational damage for organizations, highlighting the need for a flexible and rapid cyber recovery that supports a diverse and distributed application environment.

The consequences of failing to protect application continuity and data access across diverse platforms and infrastructures are increasing. IBM's Cost of Data Breach Report reveals the global average cost of a data breach reached USD 4.45 million in 2023, marking a 15% increase over three years. Additionally, ransomware attackers extorted over $1 billion from victims in 2023, as reported by Chainanalysis. Moreover, according to a recent report from Statista, organizations require an average of 24 days to recover from a ransomware event. Prolonged interruptions due to the need for extensive remediation efforts, data restoration processes, and the rebuilding of systems make unplanned downtime the most expensive aspect of cyberattacks.

Cyber threats aren't limited to on-prem infrastructure. Cyber attacks in the cloud are increasing at an alarming rate. According to CheckPoint, 2022 saw a 48% increase in cyber attacks in the cloud. This increase is driven both by an overall increase in cyber attacks and by enterprise adoption of the cloud for core business applications, making the cloud a more high-impact target for cybercriminals.

Faction's Multi-Cloud Cyber Vault solution integrates Dell PowerProtect Cyber Recovery hardware with CyberSense® software. We empower enterprise organizations to leverage the rapid innovation of the public cloud while protecting high-value and mission-critical on-prem and cloud application data in a physically isolated environment. Additionally, our Multi-Cloud Cyber Vault enables application recovery to an uncompromised cloud infrastructure in the event of a cyber incident. CyberSense seamlessly integrates with the Dell PowerProtect Cyber Recovery hardware, enabling automated scans of backup data to ensure its integrity and prompt detection of any suspicious activity. When CyberSense identifies corruption, it employs robust AI-based machine learning models to issue alerts with 99.5% accuracy.

Self-Assessment Checklist for Multi-Cloud Cyber Vault Readiness

Are you ready to adopt a Multi-Cloud Cyber Vault? Take this assessment to find out.

Data Security Needs

Does my business have mission-critical application data that would impact my business if I were to experience downtime in the event of a cyber/ransomware attack?

Is my organization's application infrastructure spread across on-prem and one or more public cloud environments?

Disaster Recovery Preparedness

Are we lacking a robust recovery plan in response to a ransomware attack that disrupts the availability of mission-critical business applications or our access to critical data?

Are we unsure of our organization's ability to recover critical data and applications across cloud and on-prem infrastructure?

Integration and Accessibility

Are we experiencing challenges protecting high-risk, high-value data residing in diverse on-prem and cloud environments?

Are our current data recovery processes efficient and effective in restoring critical data in the event of a cyberattack or operational disruption?

Risk Mitigation Strategies

Is protecting my organization's reputational capital a critical imperative?

Do we need a trusted partner that offers comprehensive data protection, recovery, and security solutions tailored to our specific needs?

If you answered "Yes" to even a few of these questions, then you may benefit from the added resilience and security of a Multi-Cloud Cyber Vault that protects and ensures the recovery resilience of your mission-critical applications and data.

Next Steps

According to Dell Technologies, despite the urgent need for a cyber recovery strategy, a staggering 67% of IT decision-makers lack confidence in recovering critical data post-cyberattacks, emphasizing the need for robust protection solutions.

If your organization is rapidly adopting cloud infrastructure and is challenged to protect access to mission-critical data and ensure application continuity across an expanding application footprint, reach out to a Multi-Cloud Cyber Vault expert at Faction.

We're in the business of storing and protecting multi-cloud data for large enterprise organizations. We'll be delighted to discuss your application footprint, backup and vault requirements, and how a Multi-Cloud Cyber Vault with fully managed infrastructure might help you achieve your cyber resilience objectives. At Faction, we aren't just multi-cloud data experts, we are your strategic partners, committed to delivering the solutions and expertise you need to get the most out of your data.

For more information, visit FactionInc.com.

About Faction

Successful digital transformation requires a data-first approach to storing, managing and presenting data. As the pioneer of Multi-Cloud Data Services (MCDS), Faction offers the industry's most comprehensive suite of solutions tailored to meet your Production Application, Cloud Data Pipeline, and Data Protection requirements. Faction's Multi-Cloud Data Services accelerate business outcomes from third-party services including Artificial Intelligence (AI), Machine Learning (ML), and Business Intelligence (BI), speeding up time to innovation. Our flagship product, **Faction Cloud Control Volumes® (CCV)**, offers highly scalable, cloud-integrated storage that leverages low-latency, high throughput network connections to multiple clouds via our proprietary network fabric, the Faction Internetwork eXchange™ (FIX). Faction MCDS deliver the agility, performance, scalability, security, and data sovereignty necessary to realize the promise of data-driven transformation. To learn more about Faction, visit www.factioninc.com and follow us on X (formerly Twitter) and LinkedIn.