Protect Your Multi-Cloud Data from Cyber Threats

Cyber Recovery with Multi-Cloud Data Services for Dell EMC PowerProtect

DELL Technologies

Learn More

Cybercrime — an Existential Threat to Your Business

Data is the lifeblood of organizations, fueling global economies and our professional, social and individual lives. Cybercrime and cyber warfare are outpacing preventive solutions and are terminal threats to businesses, governments and all data-driven entities. Modern threats require modern protection, isolation and intelligence to enable recovery in the wake of a successful ransomware or cyber attack.

DISRUPTED OPERATIONS

DATA THEFT/BREACH

FINANCIAL IMPACT

BUSINESS REPUTATION

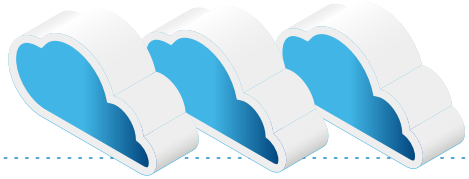
EVERY 11 SECONDS
A CYBER OR RANSOMWARE ATTACK OCCURS[1]

$6T Total global impact of cybercrime in 2021[2]

$13M Average cost of cybercrime for an organization[3]

[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021
[2]Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[3]Accenture Insights, Ninth Annual Cost of Cyber Crime Study, March 2019: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Security is a Barrier to Cloud Adoption



Ensuring your valuable data, that is spread across multiple cloud services, is protected from modern threats and recoverable at all times has proven to be a daunting task for many organizations. It often holds back strategic cloud initiatives. But none of these challenges have to slow you down from embracing public cloud.

...this is how we will help you secure your data on-premises and in the cloud

ISOLATION

Physically and logically isolated vault environment, disconnected from corporate networks via operational air gap

IMMUTABILITY

Immutable data copies in a secure off-premises vault maintaining data integrity

INTELLIGENCE

Intelligent analytics provide machine learning and full-content indexing within the vault

RECOVERY

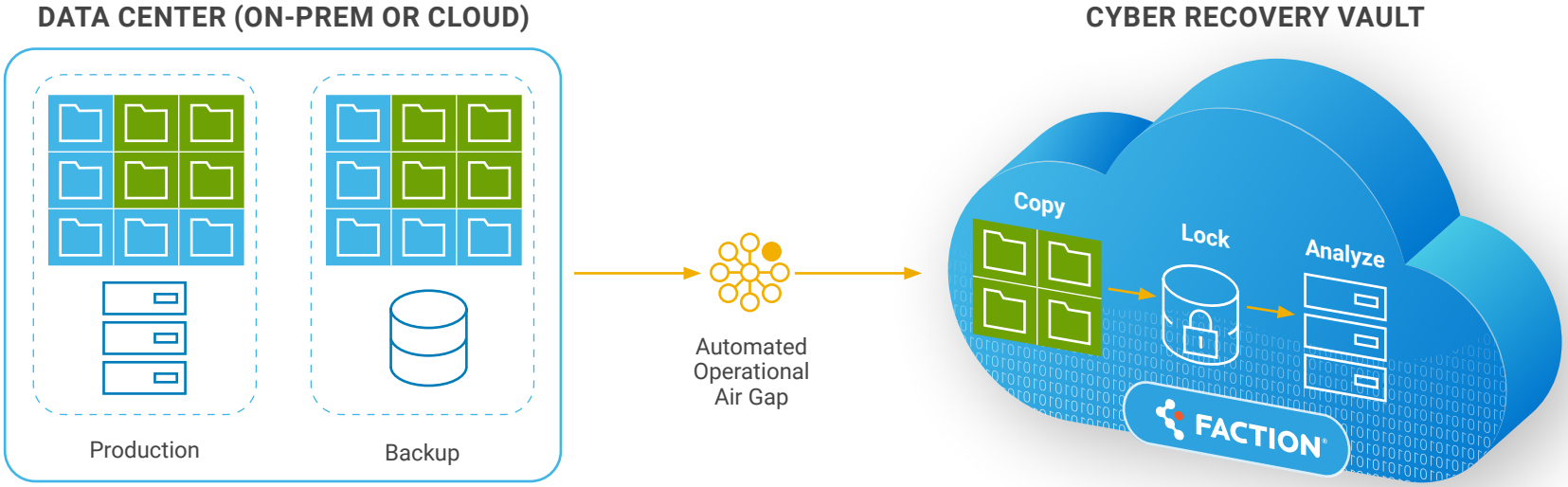
In case of an attack, recover your data with confidence

Protect Your Critical Cloud Data in a Vault Environment

ISOLATION

Multiple levels of physical and logical isolation including an operational air gap

The secure data vaulting service is a logically air-gapped vault built upon secure, multi-cloud-enabled infrastructure that safeguards your critical data from cyber attacks. Combined with the physical security and isolation of the vault, this solution includes an operational air gap — this air gap enables access to the vault only long enough to replicate data from the primary system and even then, access is severely limited. At all other times, the vault is disconnected from the client's production environment.



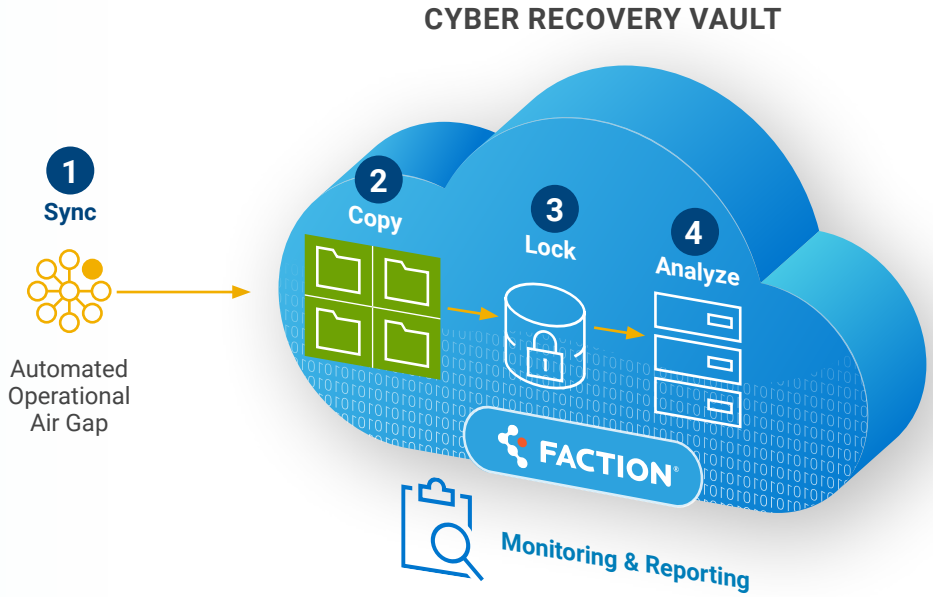
Create Immutable Copies of Your Data

IMMUTABILITY

Ensure the original integrity, confidentiality and availability of the vault data is preserved

The vault operates in 4 basic steps:

1 Sync	Data representing critical applications is synced through the air gap, which is unlocked by the management server into the vault and replicated into the vault target storage. The air gap is then re-locked.
2 Copy	Immutable copies of user-selected data are created in the Cyber Recovery vault hosted in a Faction data center. Once a copy of the selected data is safely within the secure, isolated vault, the data cannot be altered, deleted or otherwise changed for a prescribed duration.
3 Lock	The data is retention locked to further protect it from accidental or intentional deletion.
4 Analyze	The data is optionally analyzed by our analytics engine, CyberSense.



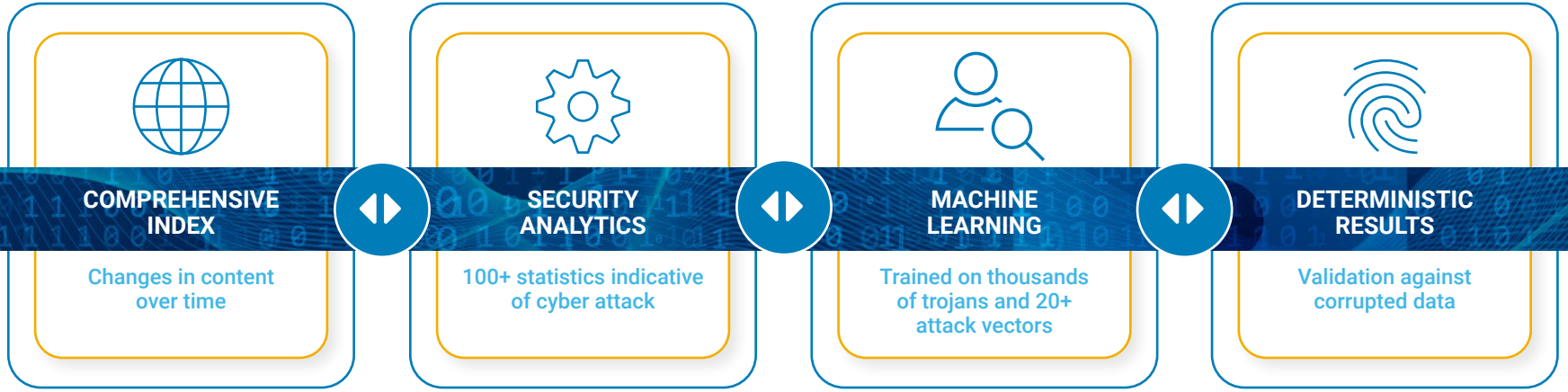
 |

Ensure Data Integrity with Intelligent Analytics

INTELLIGENCE

CyberSense machine learning enables early detection and rapid recovery from a cyber attack

CyberSense leverages machine learning within the safety of the vault to identify known good backups and alert to ongoing threats. Every time CyberSense sees a new backup image, statistics are generated from that scan, and compared to previous scans. These analytics are input into the machine learning model. The results are deterministic regarding the data's integrity and if the data has been corrupted by a ransomware attack.



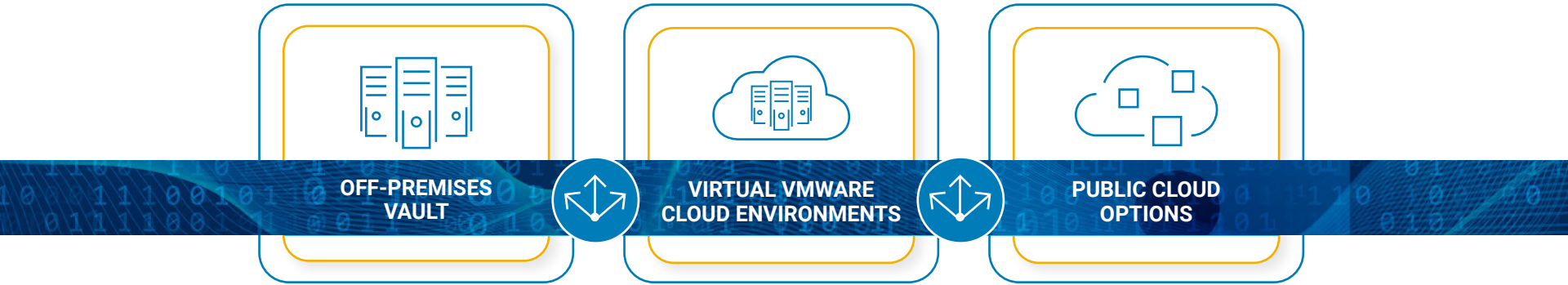
 |

Solving the Recovery Complexity for You

RECOVERY

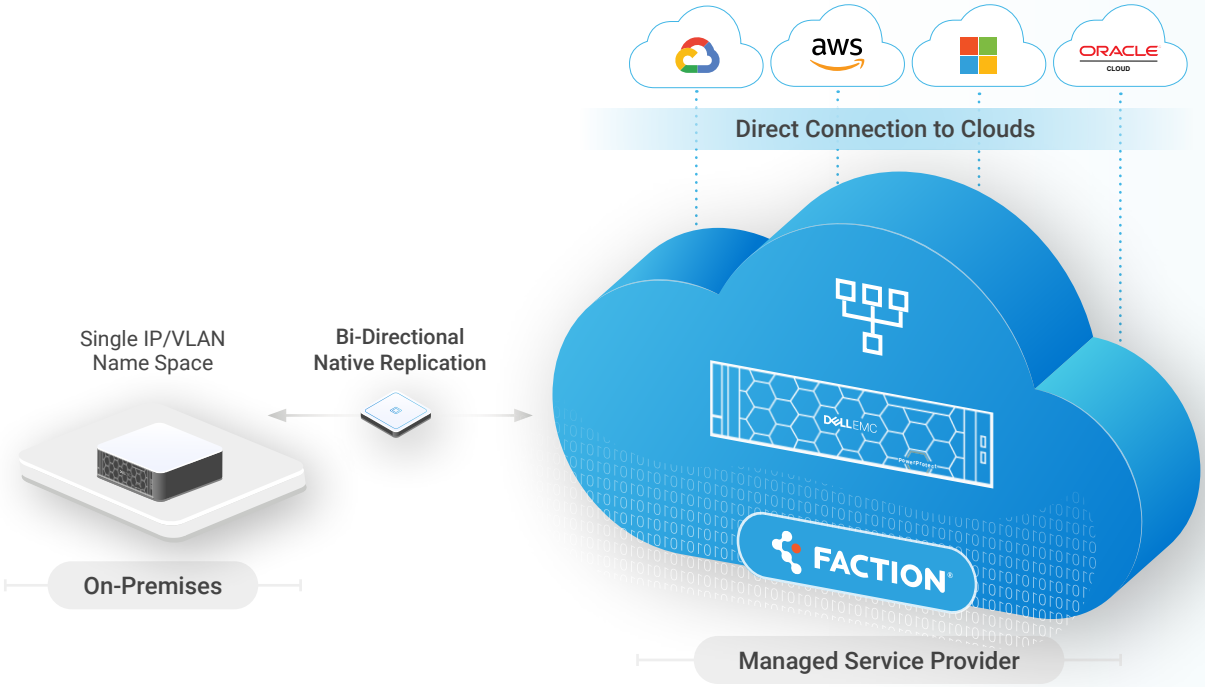
Whether your data is on-premises or in the cloud, in the event of an attack, you need to be able to restore your data and applications quickly and confidently. In an on-premises strategy, assuming the environment is on lockdown or untrusted, you must have a clean room environment on standby. These are resources and costs that are incurred even though they aren't actively being used.

Multi-Cloud Data Services for Dell EMC PowerProtect simplifies these challenges by offering multiple recovery options to enable resumption of normal business operations with confidence. When data recovery is required, you can choose to restore your data from your vault to your chosen public cloud, to a VMware Cloud environment, back to your on-premises environment, or some combination — allowing you to pick the right solution for your needs.



What About Data that Exists in Multiple Clouds?

Cyber Recovery with Multi-Cloud Data Services



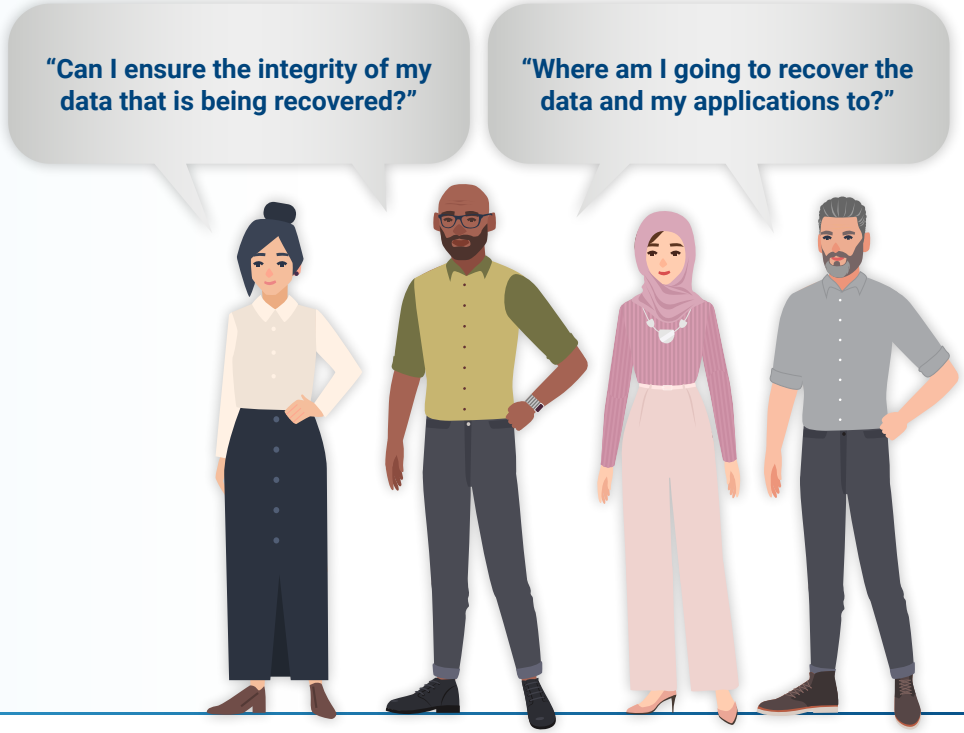
Multi-Cloud Data Services for Dell EMC PowerProtect

- Core vault infrastructure delivered as a fully managed service
- Available high-bandwidth, low-latency direct connection to public cloud providers
- No excessive egress fees
- Protect critical data that resides either in the cloud or on-premises
- Restore data to a public cloud provider seamlessly
- Gain the flexibility and convenience of the cloud without compromising on security

Teams Are Wrestling with Data Security Challenges as They Move to the Cloud

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. It's not just about protecting your data; you must also have 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.



Multi-Cloud Customer Use Case

Multiple clouds present new data protection challenges

Customer Concerns

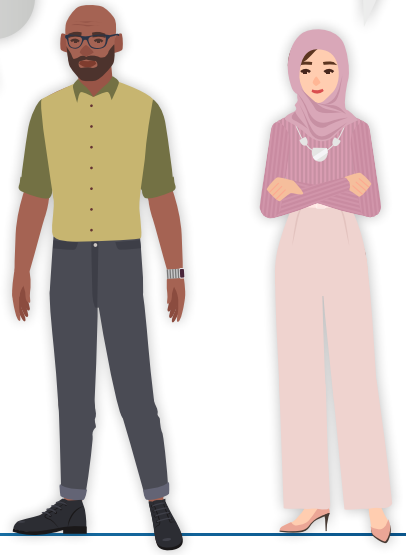
1> Hybrid and multi-cloud environments offer operational flexibility, the ability to scale up quickly, and access to innovative services and hardware.

2> Scattering and duplicating data across multiple clouds can lead to new security and compliance risks, potential synchronization issues, and increased resource costs.

3> This approach can also reduce visibility across your various environments, leading to insufficient protection from today's constantly evolving cyber threats.

"We need our data to be simultaneously accessible to multiple public cloud providers without compromising security, retain our freedom to choose any cloud provider and avoid vendor lock-in."

"We already use Dell EMC PowerProtect DDVEs in multiple public clouds to protect our data, but we also want to prioritize securing our critical applications, but we are concerned about the cost."



Role: VP/Director of Security
Workloads: Critical applications kept in multiple clouds

Role: Backup Admin
Workloads: Critical applications kept in multiple clouds

All enterprises will struggle with app modernization and data integration across cloud silos.*

*IDC FutureScape: Worldwide Cloud 2021 Predictions, December 2020

Multi-Cloud Use Case Solution

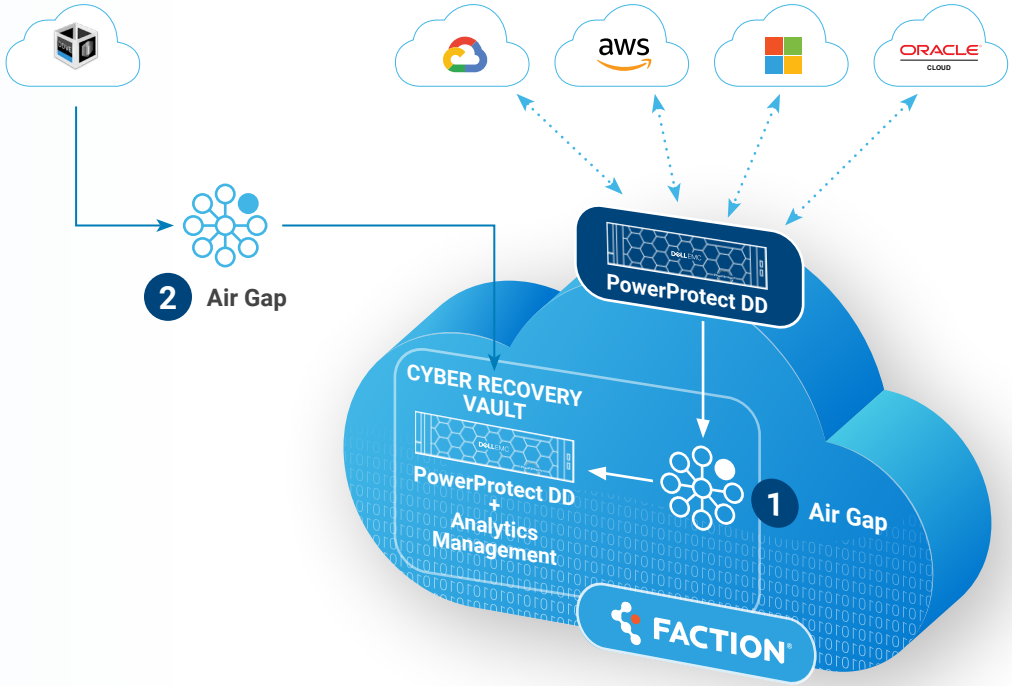
Gain the flexibility and convenience of the cloud without compromising on security

This solution provides high-bandwidth, low-latency direct connection to public cloud providers with up to 200Gb/s direct cloud connect with ~1ms latency. It is also cost-effective, with zero-dollar egress with Microsoft Azure and Oracle Cloud and reduced costs for other clouds.

1. Air Gap 1 provides a secure Cyber Recovery Vault for customers utilizing the Multi-Cloud Data Services for Dell EMC PowerProtect in Faction Cloud.

   Data residing in any public clouds can backup to the same PowerProtect DD residing in Faction.

2. Air Gap 2 provides a secure Cyber Recovery Vault for customers that have deployed Dell EMC PowerProtect DDVE in the public cloud.



Private Cloud Customer Use Case

Off-premises solution to protect on-premises data

Customer Concerns

1> Disaster Recovery and replication strategies usually fail in response to a cyber attack which allows the corruption to be replicated very quickly.

2> The risk from insider threats is high and needs to be considered.

3> Cybersecurity teams do not always understand that the backup is at risk or that you do not leverage tape as a backup medium.

4> Off-premises location adds physical security to the solution, independent of Disaster Recovery.

5> More organizations are prioritizing their most critical applications.

"We are looking at hardening our on-premises backup infrastructure. We are looking for an offline or logical air-gap solution."

Role: CIO/VP of IT
Workloads: Critical applications kept on-premises

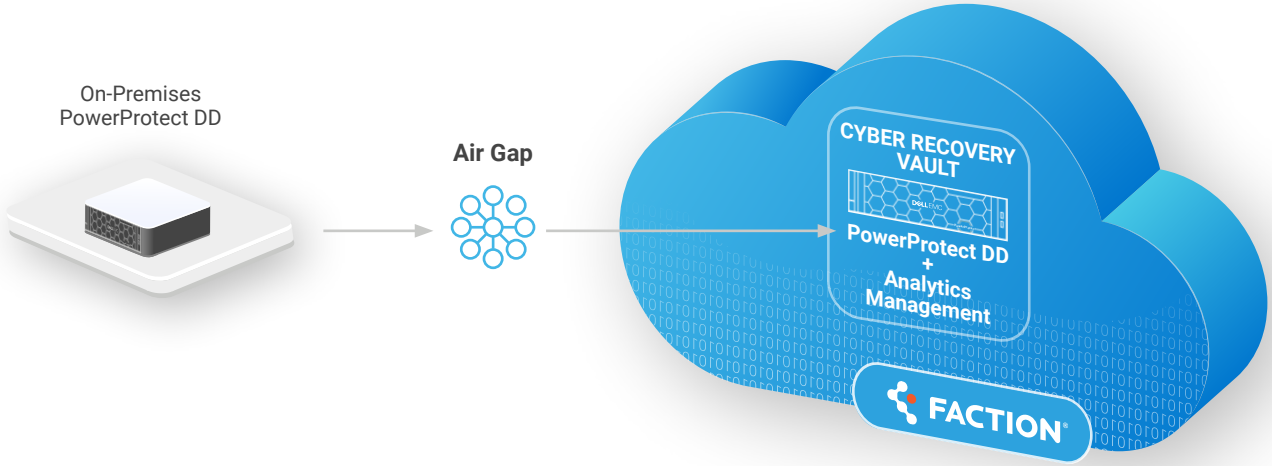
Private Cloud Use Case Solution

Customers can replicate data from an on-premises PowerProtect DD to a Cyber Recovery Vault in one of Faction's data centers. This gives organizations the best possible chance for recovery when their production or primary backups have been compromised or their DR location has been breached or infected.

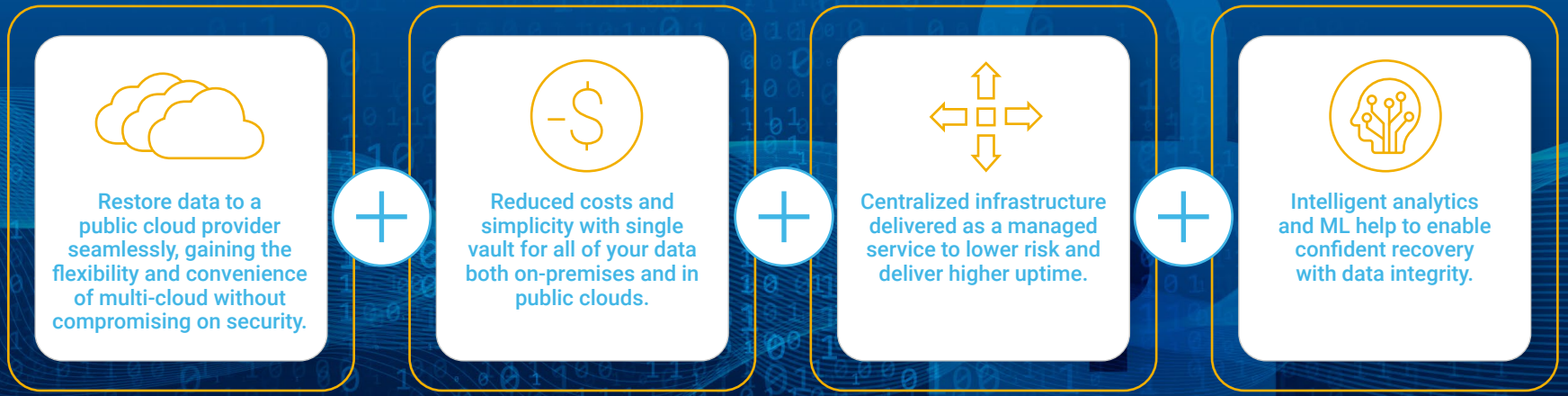
If a cyber attack occurs, they can quickly identify the most current clean copy of data within the remote Cyber Recovery Vault and recover their critical systems back on-premises, or choose to recover into the cloud if their service has been architected with this recovery motion.

Off-premises vault for their on-premises data:

Provides a secure Cyber Recovery Vault for customers who need to protect data residing in their on-premises Data Center.



Protect Your Critical Data Across Clouds Today…



Multi-Cloud Data Services for Dell EMC PowerProtect

Learn more at **DellTechnologies.com/CyberRecovery**