FAQS SHEET

DRworx℠
Disaster Recovery by Alvaka

Are Alvaka DRworx cloud backups stored off-site? And where?

Yes, the backups are stored off-site away from your facility. DRworx backups are encrypted and sent off-site to a cloud storage location in the United States. We won't state where here, but upon further discussion and NDA with Alvaka, we can disclose where geographically your backup data is stored.

Does Alvaka DRworx provide any method for validating that the synchronization of the data to the off-site facility is complete and current?

The Alvaka DRworx Global Management Portal displays replication status and history. Reporting can be setup as well.

What are the default retention policies of backup data that is synced to the DRworx off-site facility?

Storage based licenses: Retain all snapshots for 14 days.
After 14 days, retain last snapshot of day for 30 days.
After 14 days, retain last snapshot of week for 10 weeks.
After 14 days, retain last snapshot of month for 6 months.
After 14 days, retain last snapshot of year for 3 years, or 10 years (depending on license type).

End Point licensing: Retain all snapshots for 14 days.
After 14 days, retain last snapshot of day for 30 days.
After 14 days, retain last snapshot of week for 10 weeks.
After 14 days, retain last snapshot of month for 6 months.

Does Alvaka DRworx provide off-site virtualization capability (the ability to spin up and run VMs in the remote site)? What is the cost model?

Yes, spinning up servers remotely in the event of an emergency is available. Billing is by the week depending on the size node that is required.

Is it the client's responsibility to spin up VMs in the off-site datacenter to validate?

Yes, this needs to be done in conjunction with Alvaka's DRworx Support Team's initial assistance.

What assurances are available that backups are validated to be fully recoverable?

DRworx performs a bootvm to validate that the machine can virtualize. While the machine is virtualized, we perform an autoverify process that checks the integrity of the data. You will be alerted if this process fails.

What security measures do we have in place for ransomware protection (air-gapping, MFA, MDR on off-site repository)?

A form of Air-Gap is at the local level, as well as in the cloud.

What assurances does DRworx offer that backups are not vulnerable to threat actors?

The DRworx Air-Gap feature has a physical barrier to protect the data against bad actors.

FAQS SHEET

DRworx℠
Disaster Recovery by Alvaka

Are DRworx backups encrypted in transit and at rest (local and off-site)? If so, how are encryption keys managed?

Yes, Cloud Encryption method. In transit it uses TLS 1.2.

Can DRworx backup databases, and if so, are the databases quiesced prior to backup and likely to be recoverable?

Yes, DRworx uses VSS for the backup of databases. That data processes in our autoverify process for usability.

Can DRworx backup Exchange, and if so, can it provide single email and/or mailbox recovery?

Yes and yes, with our DRworx DirectRestore software.

Can DRworx backup O365, and if so, can it provide single file, email and/or mailbox recovery?

Yes, with our DRworx x360Cloud solution.

Do we get access to a DRworx Console for self-service administration?

Yes, we can set that up for you.

What is the DRworx SLA and how do clients initiate System Failover to off-site data center?

Access to the DRworx Continuity Cloud node is <60Min. The machine is virtualized and the client gains access by a remote method like VPN or RDP.

What other features and benefits differentiate the DRworx offering from in-house Veeam?

- DRworx has chainless backups. Veeam is forever incremental, or reverse incremental, depending on selection.
- DRworx uses less storage.
- DRworx has no rollups or consolidation process, reducing the risk of corruption to historical backups.
- DRworx has Air-Gap locally and off-site. Veeam has ‘safety archive’ but that is just a different retention policy and uses excess storage in the off-site only.
- DRworx, by default, performs bootvm and autoverify processes. Veeam requires additional resources and a ‘sure backup’ process.
- DRworx uses an ISO on an appliance that has all features baked into the system. Veeam requires multiple components to work in the same fashion. (A HyperVisor of choice, Windows OS, Storage device, resources to perform local failover, an off-site destination)