DISASTER RECOVERY
as a Service

EXTRAVAR

Why Disaster Recovery

- Hardware faults

Every piece of hardware is rated for five nines of availability, but what happens if something fails? How does that impact what is running on it?

What if there is data corruption because of it, or hardware replacement is more than four hours away?

- Software faults

Let’s be honest, no software package is perfect. Between integration into multiple systems, patches, vulnerabilities and common errors, what happens if your primary application has an issue that potentially loses data or fails to start?

- Malicious software

You can’t read the news without hearing the latest security vulnerability or worse, a ransomware or cryptolocker scare. If your organization’s data is held hostage, how will you recover?

- Malicious users

You hope that no one would ever intentionally do something to compromise customer or employee data, but it happens. With no recovery options in place this can be a burden on IT to resolve quickly, while also dealing with the human aspect of the disaster.

- Accidents

Sometimes, someone just makes a mistake. It happens to everyone. Some mistakes are minor and can be solved easily, while others are more pressing and require immediate IT intervention.

IT Resiliency

Every organization has backups, and many feel that is all they need to protect their environment. When looking at budget items, DR becomes an insurance item for something that hasn't happened so far and companies decided to pass and roll the dice. Backups are necessary for multiple reasons – long-term retention, file recovery and even system recovery. But backups are not disaster recovery. For a complete, fully resilient business continuity solution, organizations must employ both backups and DR.

Recovery Point Objective (RPO)
is how far back in time you will go when recovering data in an event. Backups are traditionally run once a day at off hours, and thus can lead to unacceptable RPO timeframes. Imagine that a nightly backup is all that you have and something happens an hour or two before the next backup can occur. This potentially puts your organization back 20+ hours. How much data was lost? How many orders? How many projects? What is the impact of having to find and recreate 20+ hours of data?

Recovery Time Objective (RTO)
is how long it takes you to recover that information. Large data sets or even full systems can take hours to recover. When combined with an old dataset, your business could be down for over 24 hours from the recovery process time and the last known good state of your data. These numbers might be fine for certain tiers of workloads but every application and process needs to be evaluated. If it is mission-critical to your organization, and you can't afford for it to be down for 24 hours, it needs to be protected with disaster recovery techniques that meet the appropriate RPO and RTO.

Cloud and DR

Instead of buying duplicate hardware, with maintenance and all of the associated secondary site costs, you simply pay for the storage you need, and in the case of a disaster, pay only for the resources you consume. Cloud brings:

- Affordability
- Scalability
- Agility

Another significant benefit to cloud Disaster Recovery as a Service (DRaaS) is in the ability to tier your workloads for the proper RPO/RTO and manage costs based on that. If you are building a secondary site, you still need to purchase everything up front whether it’s your tier 0 mission-critical app, or those development servers that get used once a month. With a cloud consumption model, you can decide what gets protected, how often and how or if it’s brought online in the case of a disaster.

For who is ExtraVar Disaster Recovery as a Service for?

This solution is ideal for:

- Existing Veeam customers who have Veeam on-premises backup and who are looking for a DR solution

- Customers looking for a DR solution who know a second site is too costly and want to investigate cloud DRaaS.

- Customers with existing DR infrastructure that is nearing end of-life and are looking for alternatives to refreshing their old infrastructure.

- Customers looking for additional ransomware protection and recovery. While DRaaS is just one piece of the defense-indepth strategy a company should be taking to protect against ransomware, the ability to quickly restore any virtual machine to a point in time before ransomware strikes is invaluable

DISASTER RECOVERY
as a Service

EXTRAVAR

Cost Effective Consumption of CPU/RAM

Fully Integrated with Veeam

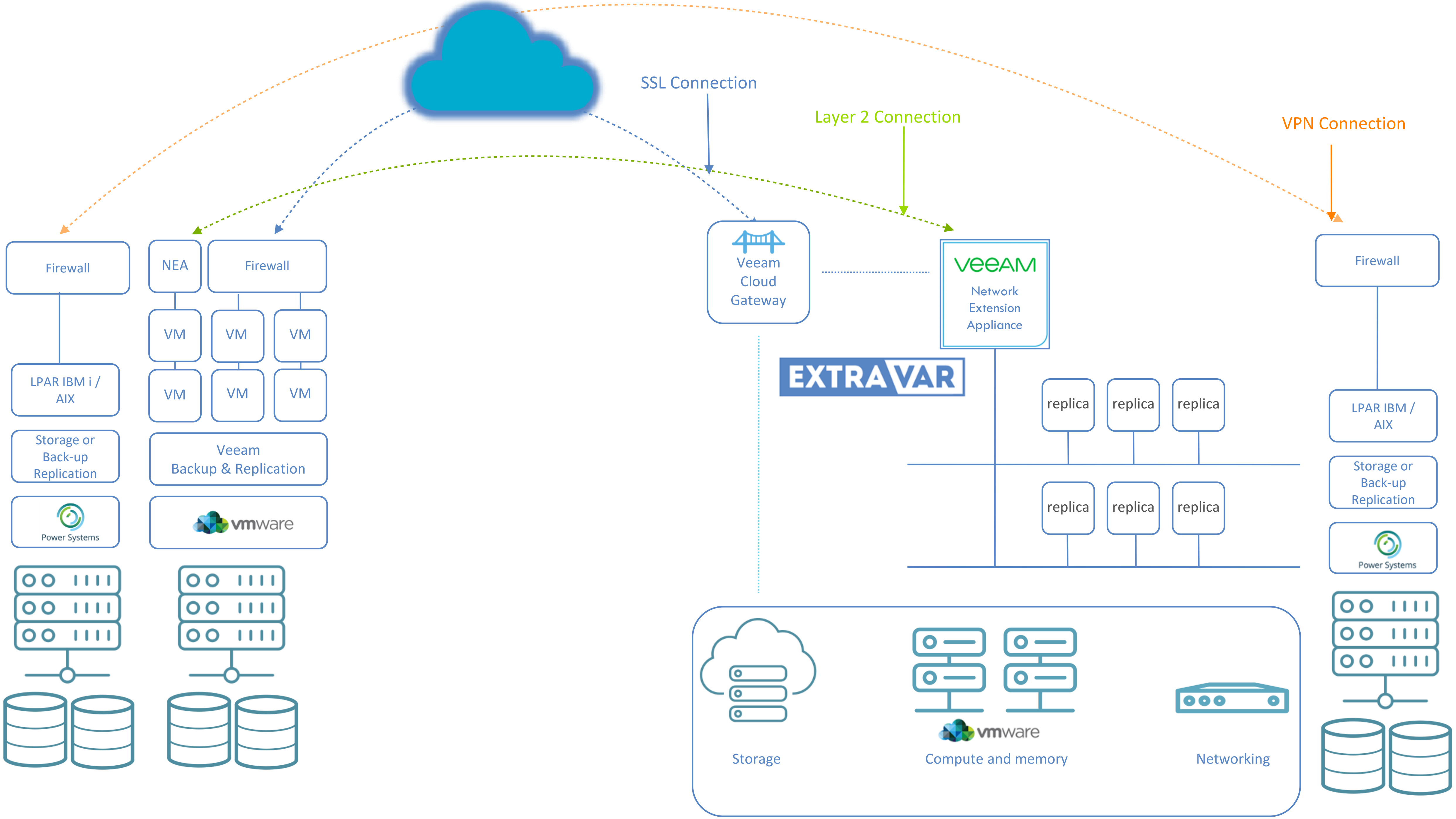
Super Simple Partial Failover

Native & Familiar VMware based

Test Failover & Failback

Encryption in flight & at rest

Directly integrate your on-premises Veeam environment with an extension to ExtraVar's Cloud infrastructure, providing secure and robust replication & failover capabilities for Disaster Recovery.


SSL Connection
Layer 2 Connection
VPN Connection
Firewall
NEA
Firewall
VM
VM
VM
VM
VM
VM
LPAR IBM i / AIX
Storage or Back-up Replication
Power Systems
Veeam Backup & Replication
vmware
Veeam Cloud Gateway
VEEAM Network Extension Appliance
EXTRAVAR
replica
replica
replica
replica
replica
replica
Firewall
LPAR IBM / AIX
Storage or Back-up Replication
Power Systems
Storage
vmware
Compute and memory
Networking