# Scaling Paragon Protect & Restore

## *Best Practices*

*last updated: October 2013*

## Overview

Paragon Software's Protect & Restore (PPR) offers a unified system and data protection solution for virtual and physical machines. PPR delivers comprehensive agentless protection for virtual environments hosted by VMware vSphere or standalone ESX servers[1], and agent-based protection for physical and virtual Windows systems on any hypervisor. As its backbone, PPR uses a patent-pending distributed architecture allowing for efficient centralized and remote management of hundreds or even thousands of machines.

In this document we will discuss the scalability potential of PPR. We will consider various production environments and provide recommendations on how to configure PPR within each environment to get the most out of the product.

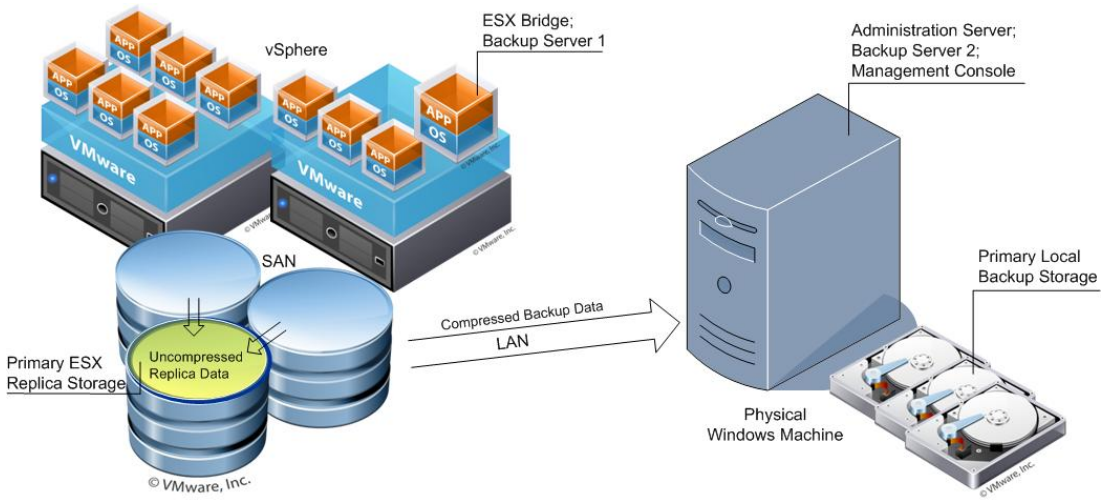
## PPR Architecture

Protect & Restore utilizes a very flexible modular architecture that allows the user, taking into account the available hardware and budget as well as internal data security policies, to configure their PPR solution in the way that will best meet their specific requirements for data protection and system performance. The product can be installed with all of its components on one machine, or with the components spread across multiple physical and virtual machines to distribute the load and to take advantage of the multiple-tier backup storages and management points.

## Protection of vSphere Guests

As our first example we'll imagine a small company with a limited IT budget, but high backup/DR-requirements in terms of sophisticated backup strategies. Target servers and workstations reside on VMware vSphere.

### Basic Backup Strategy




[1] Agentless Hyper-V support is scheduled for December 2013.

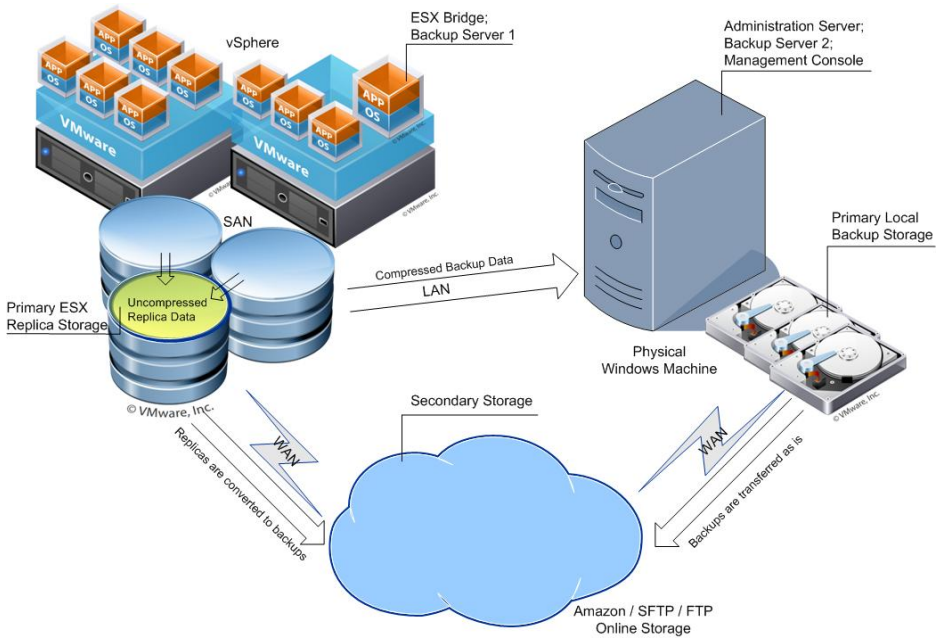
**Backup strategy highlights:**

- Enables agentless protection for guest machines of VMware vSphere (Windows, Linux, etc.);
- Mission-critical machines are replicated to the main ESX datastore in the VMware native format for best RPO and RTO performance;
- Other machines are backed up to a dedicated Windows based storage server. The use of Paragon's pVHD storage format helps minimize backup storage and network bandwidth requirements.

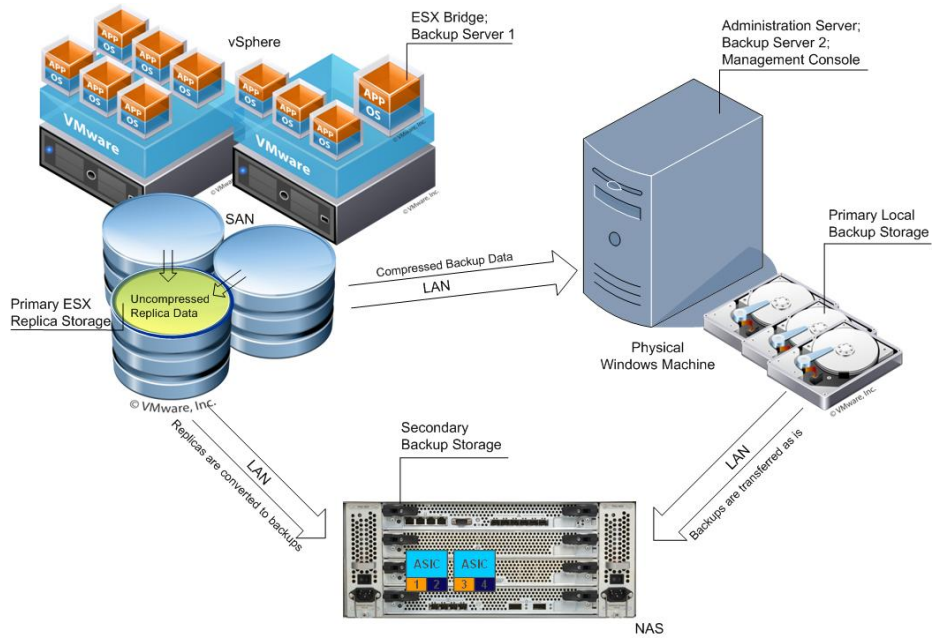
## Using One Secondary Backup Destination

To further increase the level of data protection, the first scenario can be expanded by the use of either online (cloud) storage via SFTP or FTP, or NAS (Network Attached Storage).

**With Online Storage:**




**With NAS:**

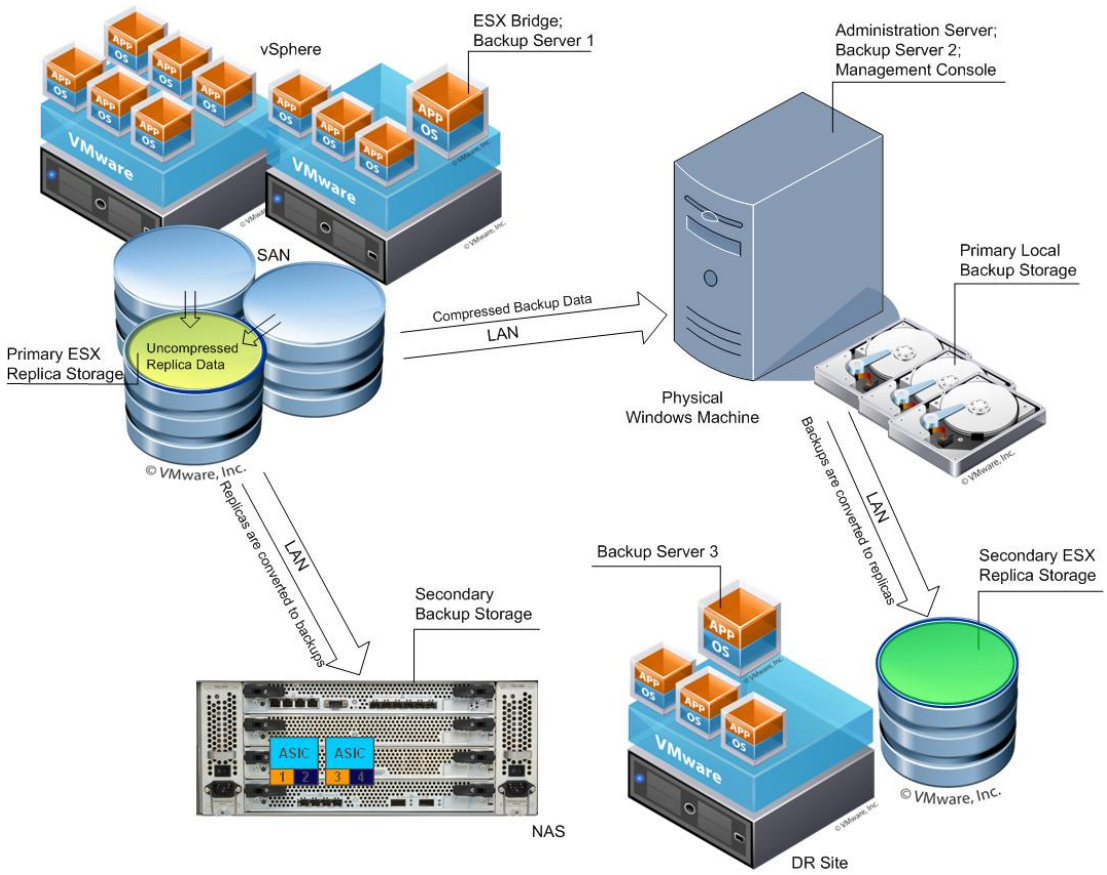


**Backup strategy highlights**

In addition to the benefits of the basic backup strategy with local backups, adding a secondary backup destination allows dual protection – backup data (archives) located on the local storage are replicated to online (cloud) storage via SFTP or FTP, or to a NAS device, preferably at times when the impact on the production environment and the network can be minimized, e.g. the weekend.

## Using Two Secondary Backup Destinations

A scenario with two types of secondary backups in addition to your primary backup provides the highest level of data protection and the highest degree of flexibility in terms of restore options.

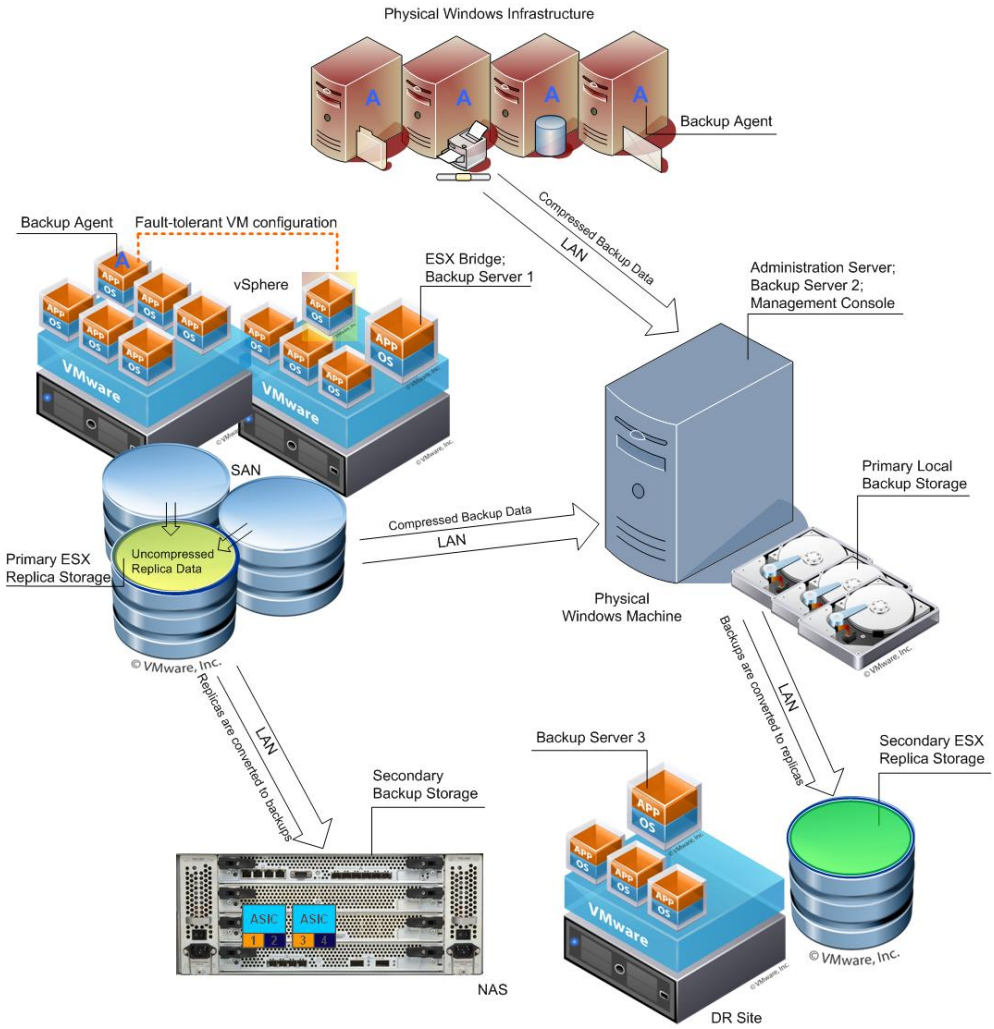



**Backup strategy highlights**

Going far beyond the benefits of the basic backup strategy, this scenario offers comprehensive dual protection - backup data (archives) located on the local storage are replicated to NAS and a standby ESX environment, preferably at times when the impact on the production environment and the network can be minimized, e.g. the weekend. Depending on the target secondary storage, VM replicas can be automatically converted to pVHD images and vice versa.

## Protection of vSphere Guests and Physical Machines

As the last example we'll look at a comprehensive disaster recovery plan as you might find it at a larger organization, where a hybrid environment consisting of VMware virtual machines as well as physical Windows machines is being protected:




**Backup strategy highlights**

- Agentless protection of virtual machines on VMware vSphere (Windows, Linux, etc.)
- Agent-based protection for physical Windows machines
- Agent-based protection of VMware fault-tolerant systems and/or guests hosted by non-commercial ESX
- P2P ready - Paragon's Adaptive Restore technology allows for the seamless restore of physical Windows machines to dissimilar hardware (HIR)
- V2P ready – the combination of agent-based backup and Paragon's Adaptive Restore technology allows for the easy conversion or restore of a virtual machine to physical
- Comprehensive dual protection - backup data (archives) located on the local storage are replicated to NAS and a standby ESX environment, preferably at times when the impact on the production environment and the network can be minimized, e.g. the weekend. Depending on the target secondary storage, VM replicas can be automatically converted to pVHD images and vice versa.

## Conclusion

The distributed architecture of Protect & Restore in combination with the product's two-tiered backup approach offers maximum scalability and flexibility to meet the diverse backup requirements of companies of different sizes and with different types of IT environments.

For additional information, please contact us at: **www.paragon-software.com**, **www.protect-restore.com** or **+1 (888) 347-5462**.