FUTUREWEI
Technologies

OceanProtect®
Secure Recovery Solution

Futurewei Intelligent Data Lab

5/21/2021

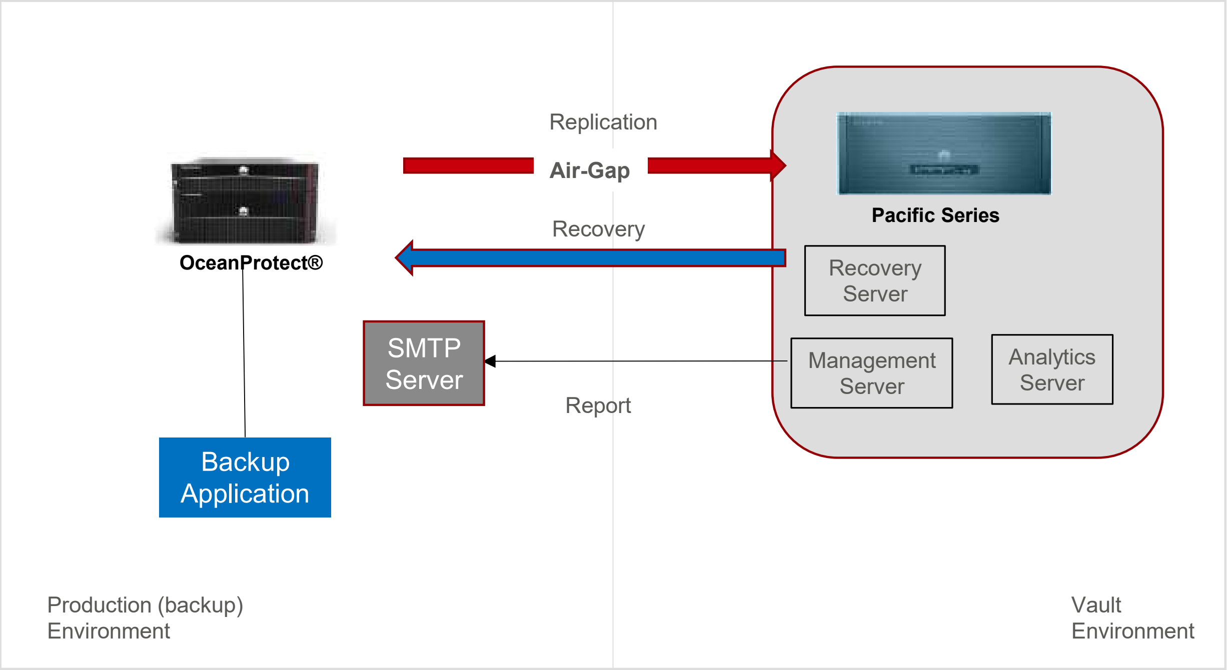
Objectives

For mission-critical applications/data, keep at least one copy at a secure location and protect data against:

- Cyber attacks & Ransomwares
- Insider attacks
- Production site data corruption

And mitigate cyber risks to a minimum level

Solution



Source: OceanProtect® X/A
Destination: OceanStor Pacific Series

Data-In path: Source -> Destination
Data-Out path: recovery Server -> Source
Event path: management host -> SMTP server

Production Environment

- OceanProtect ® A/X is used as source for application data backup
- Source sends copies of backup data to destination periodically
  - Use asynchronous replication software
  - Synchronization interval is determined by established RPO
- SMTP server (physical or logical) receives events from vault server
  - One way tunnel
  - Security should be designed in advance (dedicated link, VPN)
- (Optional) Recovery from vault to source
  - Physically (manually)
  - If via network, security should be designed in advance, such as dedicated link, VPN

Vault

- Physically isolation
  - Dedicated space with physical access requirements and access records
  - Management server /analytics server /recovery server inside vault
  - Strict security access (RBAC) & multifactor authentication for server access
- Network isolation
  - Network segmentation or other technologies to isolate vault from production network
  - Air-gap allows limited access only when replicating data from source
- FW and VPN for communication between production and vault environments
  - Data-in path: air-gap
  - Data-out path: optional
  - Event path

Data-In: Replication

- Use existing async replication software
- Air-gap
  - Link connects target directly
  - Management software enables replication interface on target only during replication, and disables it when replication is done
- FW to ensure only expected traffic can pass the link
- Encrypted traffic

Recovery Server

- In-vault data recovery
  - Using existing recovery software
  - Identify recovery point
  - Remediate backup files
  - Recover to recovery server inside vault
- (optional) Manually send data or backup files to source (OceanProtect® A/X) and source platform performs recovery
- (optional with secure dedicated link) Move data to the production environment for data recovery

Management Server

- Physical or logical server
- Management software runs on management server
  - Use existing device manager with additional functionality
  - Enable/disable replication interface and/or ethernet port on target
  - Performs system-level health check
  - Initiate data recovery jobs
  - Initiate analytical jobs with the help of analytical server
  - Send SMTP alerts to outside world

Analytical Server

- Physical or logical server
- Use third-party anti-virus software or home-developed software
  - Use anti-virus software to scan backups
  - Remove malwares
  - Send warnings and reports to management software
- System-level analytics (management software)
  - Health check for backup copies
  - System health issues such as network issues

Event Path

- Secure (one-way VPN) tunnel to production environment
- Send SMTP/SNMP alerts to SMTP server

Thank You.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Futurewei may change the information at any time without notice.

FUTUREWEI
Technologies