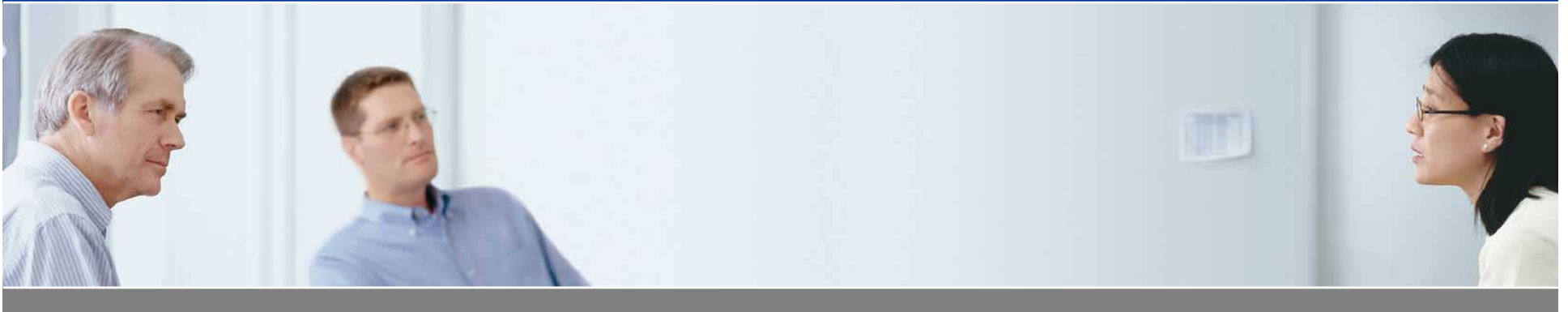


# Providence Health & Services



## Securing Data With Tape Encryption – A User Experience

Mack Kigada

Data Storage Engineer

# Company Profile

Providence Health & Services is a not-for-profit network of hospitals, health plans, physicians, clinics, home health services, and affiliated health services.

With services in Alaska, Washington, Oregon, Montana and California, we continue a tradition of caring that the Sisters of Providence began more than 150 years ago.

# Problem

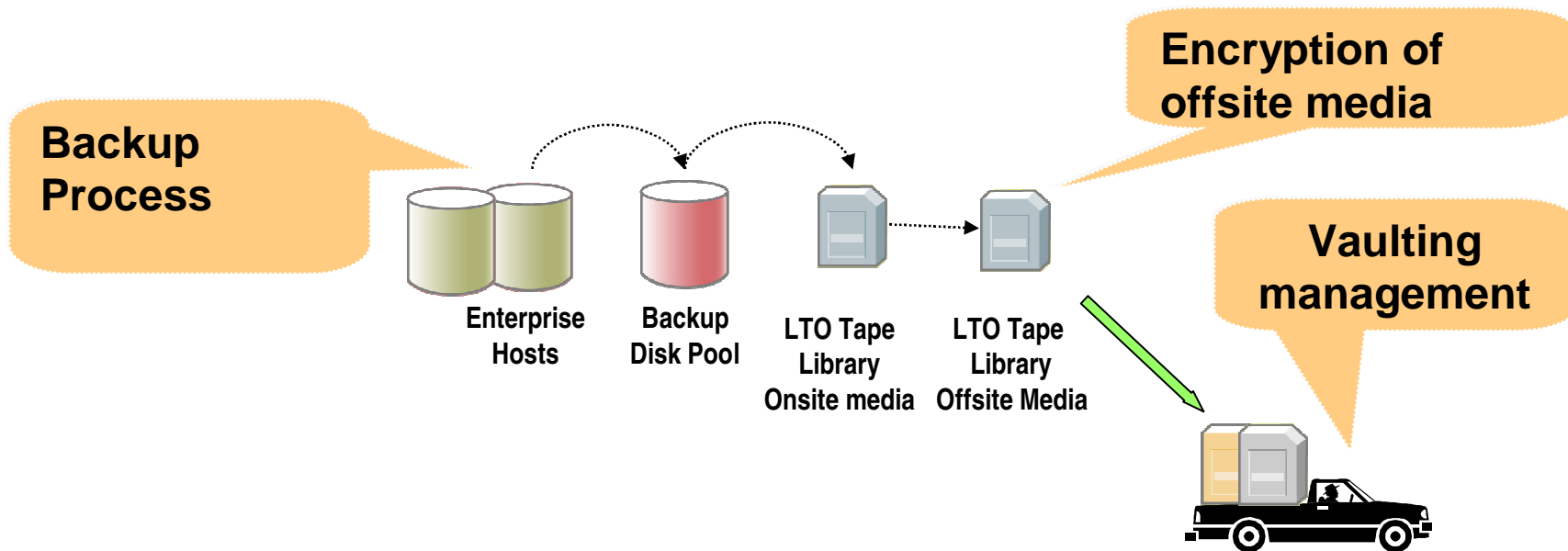
- Needed to be assured all offsite critical patient data was securely protected
- Current data protection process was insecure/unverifiable
- Difficulty managing consistent backup and restore processes
- Major facility and services consolidation projects

# Objective

- Secure all off site media
- Use strong encryption
- Centralize backup operations
- Meet established SLAs

# Approach

- Implement enterprise backup solution at major data centers
- Central server acting as the backup server and managing tape backups
- Implement an LTO-4 tape library (800GB / cartridge uncompressed)
- Midrange disk array as the disk pool for tape backups
- Effectively establish a disk to disk to tape storage strategy



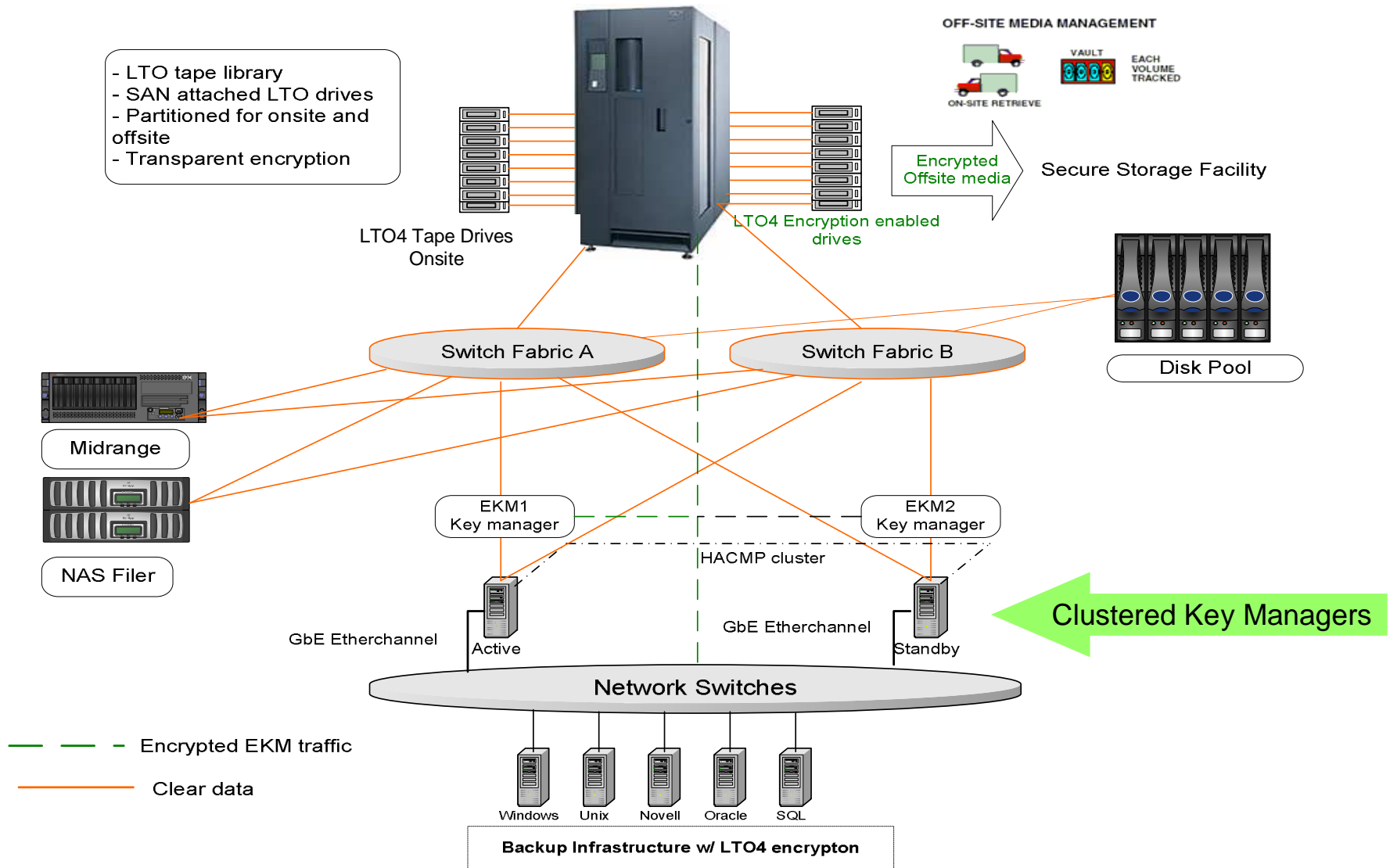
# Environment

- Six data centers in five states
- All six data centers are encrypting off-site media
- Simple process: once equipment was installed, took only 1-2 days to implement encryption systems
- The sixth site has been encrypting since day one.
- Daily backups are between 3 – 15 TB per site

# Encryption Process

- Data is first written to disk
- Onsite copy is then streamed to tape
- Offsite tapes made by duplicating onsite tapes
- Library requests encryption key from Java based encryption key manager (EKM) software
- Key is sent to the drive
- Two encryption key manager systems clustered for continuous availability
- Cartridge data is compressed then encrypted as it is written
- Virtually no tape drive performance impact: Less than 1% overhead due to encryption
- Returned cartridges are read and decrypted in real time

# Architectural Overview





# Results

- Centralized, automated data protection system
- Eliminated manual management of tape backups
- Allows the center to align its backup strategy to its online data access and archiving needs
- Tape system reduces disk requirements and gives better access to historical data
- No longer necessary to retrieve tapes from offsite locations
- Assured data is protected
- LTO-4 Encryption addresses security and compliance requirements

# Critical Success Factors: Lessons Learned

- Encryption with LTO-4 does not change backup process
- Choose compatible upgrades: upgrade to LTO-4: reads and writes LTO-3 cartridges, reads LTO-2
- Centralized, automated data protection system
  - Easier to manage
  - Better TCO
  - Simplified infrastructure
- Blended system of tape and disk help meet objectives:
  - Performance
  - Data Protection
  - Data Security
  - Cost and Energy Control