Storage Security Panel:
Learning From Others Experiences

Blair Semple, NetApp
The material contained in this tutorial is copyrighted by the SNIA.

Member companies and individuals may use this material in presentations and literature under the following conditions:

- Any slide or slides used must be reproduced without modification
- The SNIA must be acknowledged as source of any material used in the body of any document containing material from these presentations.

This presentation is a project of the SNIA Education Committee.
Abstract

Storage Security: Learn From Others Experience

- This is a panel discussion made up of end-user organizations that have deployed various storage security solutions within their enterprises.

- The goal of this session is to help IT management and administrators learn from the challenges and successes other have had in deploying storage encryption and key management solutions.
Panelists:

➤ Moderator: Blair Semple
  ♦ Security Evangelist, Network Appliance

➤ David D. Murray
  ♦ Chief Information Security Officer, Genworth Mortgage Insurance

➤ Neil Strand
  ♦ Storage Engineer, Legg Mason

➤ Dave Stauffacher
  ♦ CIS System Administration, Direct Supply Inc.
Security Deployments in Storage

1. Application-level
2. Filesystem-level
3. Network-level
4. Device-level
Overview of Panelists’ Deployments

Each panelist will briefly describe their deployment:

- Tape, Disk, or both?
- Architecture deployed (appliance, embedded, software)
- Key Management
- Scale of Deployment
Areas of Discussion

Pre-deployment Phase

- What were the primary business drivers that lead you to initiate this project?
- Describe the data-inventory or data-classification process you undertook
- What were the primary product/vendor selection criteria you considered in making your technology selection?
- What functional areas of your corporation were involved in this project?
Areas of Discussion

♦ Deployment Phase
  ♦ How critical were third-party services in your deployment?
  ♦ Did you have any difficulty with system downtime during your deployment?
  ♦ Describe the deployment process you employed – phased, hard cutover, etc.
  ♦ Were your existing staff able to manage the security aspects of your solution, or was it necessary to bring on new resources with different skill sets.
Areas of Discussion

Post-Deployment Phase

- Have you expanding, or are you considering doing so, the scope of your security deployments?
- Have you gone back and re-evaluated the vulnerability profile of your sensitive data?
- Has your deployment met its requirements for performance, manageability, etc....?
- How do you envision storage security evolving within your organization over the next 2-5 years?
- What is the number one lesson you learned during this deployment that would enlighten our audience?
Your Questions....
Q&A / Feedback

Please send any questions or comments on this presentation to SNIA: tracksecurity@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Blair Semple, CISSP-ISSEP

Eric Hibbard, CISSP

Roger Cummings