Centralized Backup & Recovery

Protecting data from ransomware and other disasters

Today's speakers

**Cody Hall**
Technical Account Manager
Synology

**Robert Hendricks**
Web and Server Systems Manager
University of Washington
Why disaster recovery

Accidents and human error
Ransomware attacks
Natural disasters

75%
Cyber crime increase

$100k
Average ransomware payment

Poll

Has your organization suffered from a ransomware infection?

1. Yes, one or more devices has been infected in the past
2. No, we have not been targeted by ransomware (knock on wood)
Ransomware preparedness

Prevention
Identify and protect at risk systems.

Response
Detect and mitigate attacks in real-time.

Recovery
Restore affected systems from previous backups.
Backup is key
Back up devices regularly

7:00 AM  7:05 AM  7:10 AM

Backup is key
Back up devices regularly
Detect and neutralize attack

7:00 AM  7:05 AM  7:10 AM  Attack
Backup is key

- Back up devices regularly
- Detect and neutralize attack
- Restore from previous backup

Don't pay to recover data

---

Case study

University of Washington

School of Social Work

- Founded in 1934
- #1 among social work schools
- 15 research & innovation centers
Case study

University of Washington

Hundreds of faculty devices
PCs were on campus and at home

Sensitive information
Such as student and research data

Recovery was slow
Needed ability to restore data quickly and easily

300+
Local and remote workstations

Synology NAS
**Synology Active Backup**

- PCs
- Servers
- VMs
- SaaS

**Why local backup?**

- **Reduced costs**
  Saved over $200k per year compared to subscription services

- **Data governance**
  Able to maintain complete control over data access permissions

- **Fast recovery**
  Not limited by download speed when recovering large amount of data
Poll

Do you back up user devices from different locations?

1. Yes, some users are on campus and some are at home
2. No, all users are at the same location

Flexible work...

...Requires flexible backup
Ensure privacy during transit
Work seamlessly across locations
Walkthrough
Streamline PC backups

Poll
If a user PC breaks or disappears, how long does it take to recover on average?

1. Less than 1 hour
2. Between 1~4 hours
3. Over 4 hours
Flexible recovery options

- **Single file/folder**: Quickly download specific files and folders
- **Full system**: Requires more time, but recovers entire PC
- **Virtual machine**: Quickly spin up entire PC as virtual machine

Self-service recovery

- Let users restore files themselves
- Speed up recovery time
- Reduce number of tickets
Virtual machine
Spin up PC as virtual machine
Find deleted files or folders

Walkthrough
Exploring PC restoration options
Ransomware recovery tips

- **Keep automated, multi-version backups**
  Restore to a point in time before the attack happened

- **Implement a tiered disaster recovery plan**
  Recover data from second device if first is compromised

- **Use unique admin credentials**
  Use different accounts and passwords for each backup destination

---

**Tiered disaster recovery**

1. Primary backup
2. Off-site backup
3. Cloud backup

- PCs
- Servers
- VMs
- SaaS
Tiered disaster recovery

1. Snapshot local data
2. Off-site backup
3. Cloud backup

Snapshot Replication
Protect data on backup destination
Take snapshots every 5 minutes
Retain monthly or yearly versions
Walkthrough
Snapshots and recovery

Tiered disaster recovery

1. Primary backup
2. Off-site backup
3. Cloud backup
Tiered disaster recovery

1. Primary backup
2. Off-site backup
3. Cloud backup

PCs, Servers, VMs, SaaS

Snapshot Replication
Copy snapshots to remote server
Flexible architecture options

Office, Second location
Snapshot Replication
Copy snapshots to remote server
Flexible architecture options

Walkthrough
Replication to off-site server
Tiered disaster recovery

1. Primary backup
2. Off-site backup
3. Cloud backup

- PCs
- Servers
- VMs
- SaaS
Backup to cloud
Works with major providers:
Microsoft, Google, Amazon, Dropbox, and more

Synology C2 Storage
Integrated cloud backup
No download or restoration fees
Encrypt data before uploading
Walkthrough

Backup to Synology C2 Storage

Win a Synology NAS!
Take our survey and enter to win a Synology DS220+
Selecting hardware for your backup plan

Things to consider

- Number of devices
  Including PCs, servers, and others
- Amount of data
  Now and over next three years
- Retention requirements
  Number of years to keep backups
- Off-site backup
  Server at second location... or cloud?
Things to consider

- Might require more computing power
- Prioritize cost per gigabyte of storage
- Check encryption and privacy options

Good options for backup

- 10 PCs: DS920+
- 100 PCs: DS1621xs+
- 300 PCs: DS3617xs
Good options for backup

100 PCs  
RS820+

300 PCs  
RS3621RPxs

1000 PCs  
SA3600

Questions?
Thank you for watching