Protecting scattered data

Backup and recovery for onsite and cloud data
Today’s speaker

Josue (ho-sway) Guzman

Senior Technical Account Manager

Synology
Synology

Data storage, backup, and more
Unified hardware and software
"Our data is always at risk from various sources...
Tornadoes happen regularly, which could destroy our servers (and school). Cyber attacks often target schools like ours. And we have thousands of students who want to ‘hack’ into our systems to change their grades."

– Technology director, school in southeastern US
Protecting scattered data

- Servers
- SaaS
- PCs
Protecting scattered data

Servers

SaaS

PCs
Liberal Arts College

Faculty & staff needed data storage
Save files, collaboration, and more
Adhere to grant guidelines
Grant-friendly data storage?

- Separately managed
- Local and remote backup
- Limited access permissions
Challenges

- **Maintenance**: Keeping devices updated when you don’t own them
- **Security**: Enforcing best practices among separate teams
- **Disaster Recovery**: Planning for unexpected data loss and disasters
Centralized backup & management

Managed by faculty

Managed by IT
Centralized management

Monitor status of all servers
Receive security alerts
Push system updates
Backup and recovery

Backup server

Cloud backup
Recovery options

Snapshots
Roll back overwritten or deleted files locally

Restore from archive
Copy and restore to replacement file server

Failover
Access files on secondary failover server
Protecting scattered data

Servers

SaaS

PCs
Protecting scattered data

- Servers
- SaaS
- PCs
Oil pipeline ransomware attack

Paying the ransom might not help

Data was encrypted
Pipeline operations ceased due to ransomware attack.

Paid $5m ransom
Within hours of receiving ransom notice.

Decryption was slow
Decryption tool provided by attacker was too slow.

Used backups anyway
Recovering with company backups was faster.
Case study

University of Washington

300+

Local and remote workstations

Hundreds of faculty devices
PCs were on campus and at home

Sensitive information
Such as student and research data

Recovery was faster
Wanted ability to recover devices quickly
Poll Question:

Does your organization back up PCs locally or to the cloud?

1. We back up to the cloud
2. We back up to an on-premises solution
3. We back up to a mixture of both
4. We do not backup PCs
Active Backup Suite

Local backup for PCs, VMs, servers
Centralized management
No license or subscriptions
Why back up **locally**?

- **Reduce recurring costs**
  The school saved $200k compared to subscription services

- **Control access to data**
  Admins were able to maintain control of who could access sensitive data

- **Recover data faster**
  Data could be restored without waiting for downloads from the cloud
When file recovery isn’t enough...

My computer died and I need an excel file on it right away.

No problem. What is the file or folder name?

I dunno... It’s in excel. Whenever I open excel, it’s always at the top.
## Recovery options

<table>
<thead>
<tr>
<th></th>
<th>Windows PC</th>
<th>Windows Server</th>
<th>VMware Hyper-V</th>
<th>File Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full system restore</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File-level restore</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-service file restore</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant restore to VM host</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cross-platform recovery</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Instant restore to Synology VMM</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
# Recovery options

<table>
<thead>
<tr>
<th></th>
<th>Windows PC</th>
<th>Windows Server</th>
<th>VMware Hyper-V</th>
<th>File Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full system restore</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File-level restore</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Self-service file restore</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Instant restore to VM host</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Cross-platform recovery</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Instant restore to Synology VMM</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Instant restore as VM

Run PC as virtual machine
Virtual Machine Manager
Server with image backups

Temporarily recover a critical system
Walkthrough

Restore a system as a virtual machine
Protecting scattered data

Servers
SaaS
PCs
Protecting scattered data

Servers

SaaS

PCs
Adoption of SaaS

Remote work and learning has accelerated adoption of cloud email and collaboration.
Poll Question:

Does your organization backup Microsoft 365 or Google Workspace?

1. Yes
2. No, but we will use one in the next year
3. No, and we don’t plan to use one
Case study

Vocational college

Greater flexibility
SaaS helped with remote work and learning

Retention obligations
Must keep current and former student data

Cloud ≠ backup
Seeking a backup solution for SaaS data

60k email accounts
30k drive accounts

SaaS platform

18,000 students
1,000 faculty
Isn’t cloud data backed up already?
Data protection is your responsibility

Google Shared Responsibility Model

Data protection is not only the responsibility of the business using Google Workspace for Education services; nor is it only that of Google in providing those services. Data protection in the cloud is instead a shared responsibility, a collaboration between the customer and the Cloud service provider (CSP).

The Google Shared Responsibility Model visually describes the various security responsibilities that our customer and Google are together responsible for. Google Workspace for Education is software as a service (SaaS) where almost everything except the content and its access policy is the responsibility of the CSPs. In the SaaS model, CSPs manage all of the physical and virtual infrastructure and the platform layer while delivering cloud-based applications and services for customers to consume. Internet applications that run directly from a web browser or mobile applications are SaaS applications. With this model, customers don't have to worry about installing, updating, or supporting applications—they simply manage system and data access policies.

Important: As a Google Workspace for Education customer, you are responsible for the security of components that you provide or control, such as the content you put in Google Workspace for Education services, and establishing access control for your users.
Accidents (and attacks) happen

Accidental deletion
Admins might delete important email, documents, and other items by accident

Malicious deletion
A disgruntled IT consultant deleted 1,200 email Microsoft 365 accounts of former employer

Cyber attacks
Hackers may gain access to email accounts and delete data to cover their tracks
Cloud-to-cloud backup

- No hardware maintenance
- Easily scale capacity
Cloud-to-local backup

No subscription or license costs
Access and privacy control

Google Workspace / Microsoft 365

Local backup
Cloud backup
Case study
Vocational college

- 60k email accounts
- 30k drive accounts

- SaaS platform
- On-premises backup

- 18,000 students
- 1,000 faculty
Why **local** backup of SaaS?

<table>
<thead>
<tr>
<th>Recovery</th>
<th>Archiving</th>
<th>Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore files regardless of internet service</td>
<td>Control how institutional data is retained</td>
<td>One organization saved $60K annually on fees</td>
</tr>
</tbody>
</table>
Active Backup Suite

Local backup for...
- Drive
- Email
- Contacts
- Calendar
Walkthrough

Backing up and recovering SaaS data
Avoid single points of failure

Retain weekly, monthly, and yearly versions
Malicious actors and malware is often undetected for months

Back up data to multiple devices or locations
If a disaster compromises the primary backup, recover from secondary backups

Maintain good IT admin practices
Don’t save login credentials, use remote desktop software for critical systems, and others
Poll Question:

When was the last time you tested your backups for restoration?

1. One (1) month ago
2. Three (3) months ago
3. About a year ago
4. I have not tested my backups
Disaster and recovery planning

- **2,000** Google Workspace users
- **2,000** Windows PCs
- **10** Virtual machines

Backup repository

Local backup

Second backup

Off-site backup
Snapshot Replication

Replicate backups to second server
Good for failover to second site
Walkthrough

Setting up replication to second Synology NAS
Disaster and recovery planning

- **2,000** Google Workspace users
- **2,000** Windows PCs
- **10** Virtual machines

Backup repository

Local backup

Second backup

Cloud backup
Hyper Backup

Works with major providers: Amazon, Microsoft, Google, S3-compatible services, and more
Synology C2 Storage
Integrated cloud backup
No extra restoration costs
Encrypt data before uploading
ENTER TO WIN

Take our survey for a chance to win a Synology DS220+ NAS ($300 value).

Scan the QR code to enter!
Questions?
Thank you!