Data Protection in the Cloud

7 Critical Office 365 Data Restore Questions (And Answers)

Microsoft Partner

Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

7 Questions to Ask Yourself:

- What data backup and restore options does Microsoft offer and what is our responsibility?

- How quickly do different workloads need to be restored and in what format?

- How often should we perform test restores?

- Who can perform what restores?

- How granular does the restore data need to be?

- What restore options are available and practical for disaster recovery?

- How does GDPR and other data privacy regulations impact my data restore operations?

We Are AvePoint

Leader in Microsoft 365 data management solutions

25%
Fortune 500

7M
Cloud Users

88
Countries

7
Continents

AvePoint is headquartered in Jersey City, NJ, with approximately 1,500 employees across 29 offices, 14 countries, and five continents.

Microsoft Partner

Microsoft

5x
Partner of the Year Award Winner

AVPT
NASDAQ

Global Cloud Footprint

99.5% Availability | 24/7 Support
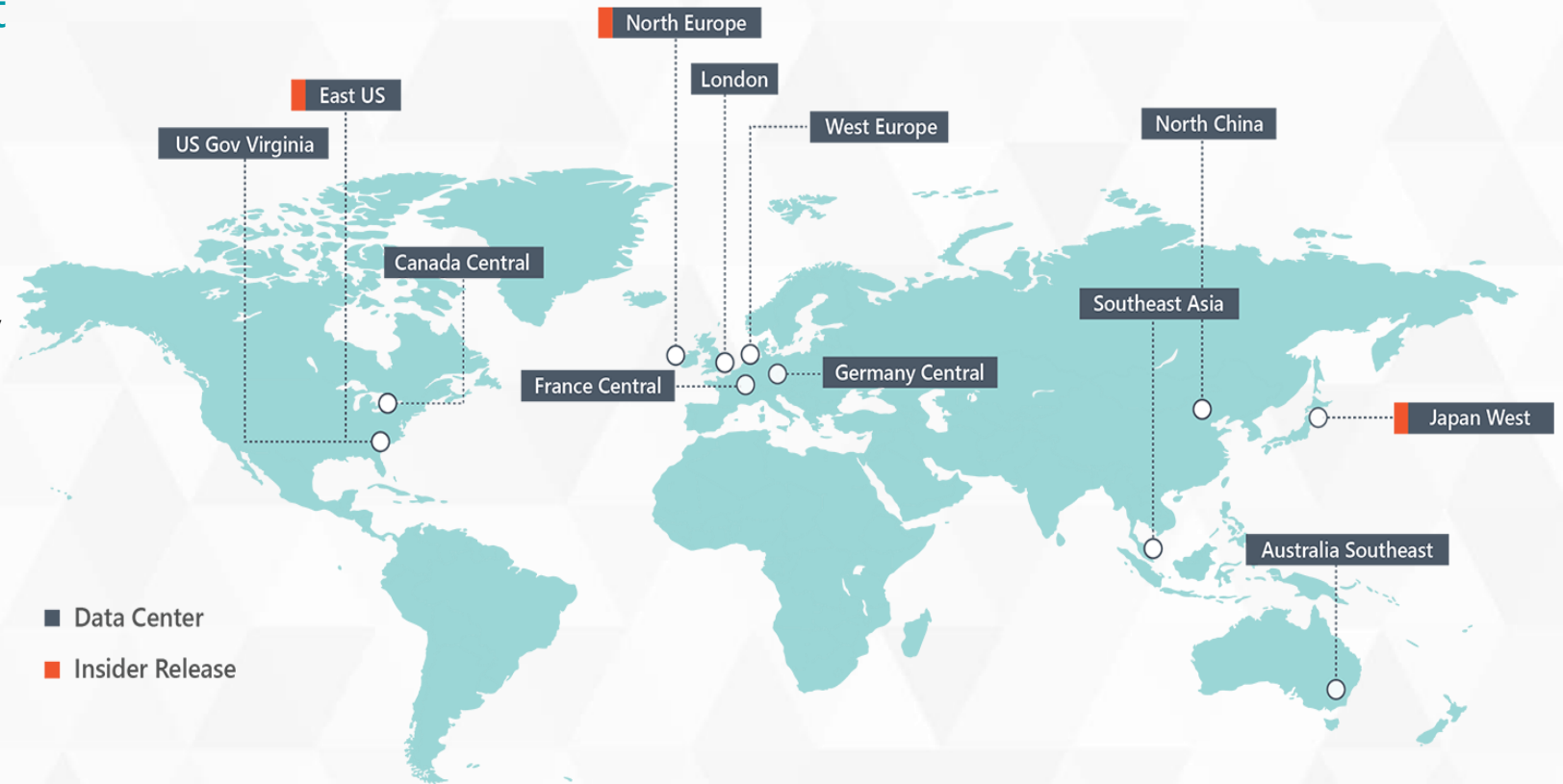Uptime backed by Microsoft Azure and World-Class Support

12 Global Cloud Instances
Hyper Scale: Regional Redundancy; Cloud Service Resiliency; Data Residency Availability Geo Replication

7 Million Office 365 Supported Seats
Providing Operational Efficiency for Office 365

Managing 40PB+
Customer Data Worldwide

North Europe

East US

London

West Europe

North China

US Gov Virginia

Canada Central

Southeast Asia

France Central

Germany Central

Japan West

Australia Southeast

■ Data Center

■ Insider Release

Critical M365 Data Restore Questions

Isn't that why I went with a cloud service?

Doesn't my cloud provider have me covered?

Do I really need it?

How would I do that anyway?

Your Responsibility for Backup

Microsoft Protection

- ✓ Loss of <u>service</u> due to hardware or infrastructure failure
- ✓ Loss of <u>service</u> due to natural disaster or data center outage
- ✓ <u>Short-term</u> user-error with recycle bin / version history (including new OneDrive "<u>Files Restore</u>")
- ✓ <u>Short-term</u> administrative error with soft-delete for Groups, Mailboxes or services-lead rollback

Customer Responsibility

- ❑ Loss of data due to departing employees and deactivated accounts
- ❑ Loss of data due to malicious insiders / hacktivists deleting content
- ❑ Loss of data due to malware / ransomware
- ❑ Recovery from prolonged outages
- ❑ Long-term accidental deletion coverage with selective rollback

Forrester: "Backup Your SaaS Data – Because Most SaaS Providers Don't", Naveen Chhabra, December 2017

Native Tools and Coverage

Low Impact

Out-of-the-box tools

- Version Control (minimum 100)
- Recycle Bin (93 days total)
- Deleted E-mail (14 days default – 30 max)

Scenario

- ☐ User Error, document corruption
- ☐ User Error, document deletion
- ☐ User Error, e-mail deletion

High Impact

- Soft-delete Sites / Groups / Teams (30 days)
- Retention settings (legal holds)
- "Files Restore" – OneDrive / Sites / Teams
- Restore from Microsoft Backup (14 days)

- ☐ Owner / Admin error, deletion
- ☐ Legal Retention Only
- ☐ Ransomware
- ☐ Corruption / Ransomware

RPO vs. RTO

Last Backup

Data Recovered

Recovery Point

RPO

RTO

Recovery Time

7 Questions to Ask Yourself:

- What data backup and restore options does Microsoft offer and what is our responsibility?

- How quickly do different workloads need to be restored and in what format?

- How often should we perform test restores?

- Who can perform what restores?

- How granular does the restore data need to be?

- What restore options are available and practical for disaster recovery?

- How does GDPR and other data privacy regulations impact my data restore operations?

Key Takeaways

- **Microsoft's M365 Backup as a Service is designed for platform outages, not common data-loss scenarios**
  Consider your granularity and frequency requirements, and RPO/RTO objectives

- **Check your backups regularly**
  Annual at least, but more frequent is better for critical information

- **Know your restore options, and who has access**
  Test your restore granularity, and ensure data-access is controlled