Journey to Better Backup & Intelligent Data Management for the Multi-Cloud Data Center

Ryan Narinesingh
Director, Partner & Alliances Canada
Veeam Software
@NarinesinghRyan
$963M
2018 Bookings

+73
Net Promoter Score

330K+
WW Customers
Adding 40,000+ / year

18M+
Servers Protected
The 4 corners of the cloud

CEO
“We’ve already moved to the public cloud.”

CIO
“We need to finish our public cloud migration.”

Infrastructure & Operations teams
“We need to develop a private / public / hybrid cloud strategy.”

Storage and Backup IT practitioner
“The cloud? Not on my watch!”
Our workloads are shifting to numerous clouds...
Public Cloud Adoption

- AWS: 64% Running, 16% Experimenting, 8% Plan to use
- Azure: 45% Running, 22% Experimenting, 9% Plan to use
- Google Cloud: 18% Running, 23% Experimenting, 15% Plan to use
- IBM Cloud: 10% Running, 11% Experimenting, 9% Plan to use
- VMware Cloud on AWS: 8% Running, 14% Experimenting, 14% Plan to use
- Oracle Cloud: 6% Running, 10% Experimenting, 9% Plan to use
- Alibaba Cloud: 3% Running, 4% Experimenting, 2% Plan to use

Source: RightScale 2018 State of the Cloud Report
81% of organizations have a Multi-Cloud strategy

Key outcomes:
- Increase innovation
- Speed time to market
- Optimize cost
Will Your Data Rain When the Cloud Bursts?

Public clouds can fail

- In September, 2013 Nirvanix initially gave customers 2 weeks to retrieve all data.
- A $5K expense question escalates into a $100K must-do.
The 3-2-1 rule: basic data protection with cloud solutions

3
Different copies of data

2
Different media

1
of which is off site

Air-gapping for extra resilience
How to prepare for ransomware attacks

1. Keep all software up to date

2. Perform a threat analysis with your security team:
   a. Penetration testing to find any vulnerabilities

3. Train staff on cyber security practices on:
   a. Not opening attachments or links from unknown sources
   b. Inform employees if a virus reaches the company network.

4. Back up all information every day

5. Back up all information to a secure, offsite location
Data protection for a multi-cloud strategy

- **Cloud backup and DRaaS**
- **IaaS and SaaS data protection**
- **Cross-cloud data protection**

Remote managed services

- **To the cloud**
- **From the cloud**
- **Within the cloud**
We have to architect against the loss of data and downtime.

Public clouds can fail

- In September, 2018 Azure suffered an issue.
- This affected multiple regions.
AWS shared responsibility model
Why Protect Data in the Cloud?

It’s your data. You are responsible for protecting it.

• Published cloud SLAs typically do not address loss of data.
• SLAs of 99.99% relate to: 1) network and storage availability, 2) immutability, and 3) durability.
• Liabilities are limited.

Amazon AWS customer agreement
10. Disclaimers.
THE SERVICE OFFERINGS ARE PROVIDED “AS IS.” EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, WE AND OUR AFFILIATES AND LICENSORS (A) MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND (B) DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (I) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (II) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (III) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, AND (IV) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR ALTERED.

Source: (http://aws.amazon.com/agreement/#2) updated November 1, 2018
Microsoft shared responsibility model

On Premises
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Infrastructure (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Platform (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

Software (as a Service)
- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualization
- Servers
- Storage
- Networking

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
The Office 365 Shared Responsibility Model

Microsoft’s Responsibility
Learn more from the Office 365 Trust Center

YOUR Responsibility

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
The Office 365 Shared Responsibility Model

Microsoft’s Responsibility

Learn more from the Office 365 Trust Center

Primary Responsibility

MICROSOFT GLOBAL INFRASTRUCTURE

Uptime of the Microsoft Office 365 Cloud Service

YOUR Responsibility

YOUR OFFICE 365 DATA

Access and control of your data residing in Office 365
The Office 365 Shared Responsibility Model

Microsoft’s Responsibility

Learn more from the [Office 365 Trust Center](#)

Primary Responsibility

MICROSOFT GLOBAL INFRASTRUCTURE

Uptime of the Microsoft Office 365 Cloud Service

Supporting Technology

Office 365 Data Replication

DC to DC geo-redundancy

YOUR Responsibility

YOUR OFFICE 365 DATA

Access and control of your data residing in Office 365

Office 365 Backup

Copy of your data stored in a different location

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
# The Office 365 Shared Responsibility Model

## Primary Responsibility

<table>
<thead>
<tr>
<th>Microsoft's Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MICROSOFT GLOBAL INFRASTRUCTURE</strong></td>
</tr>
<tr>
<td>Uptime of the Microsoft Office 365 Cloud Service</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office 365 Data Replication</strong></td>
</tr>
<tr>
<td>DC to DC geo-redundancy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>YOUR Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YOUR OFFICE 365 DATA</strong></td>
</tr>
<tr>
<td>Access and control of your data residing in Office 365</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recycle Bin</strong></td>
</tr>
<tr>
<td>Limited, short term data loss recovery (no point-in time recovery)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office 365 Backup</strong></td>
</tr>
<tr>
<td>Copy of your data stored in a different location</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supporting Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Data Retention</strong></td>
</tr>
<tr>
<td>ST &amp; LT retention filling any/all policy gaps, granular &amp; point-in time recovery options</td>
</tr>
</tbody>
</table>
The Office 365 Shared Responsibility Model

Primary Responsibility

MICROSOFT GLOBAL INFRASTRUCTURE

Uptime of the Microsoft Office 365 Cloud Service

YOUR OFFICE 365 DATA

Access and control of your data residing in Office 365

Supporting Technology

Office 365 Data Replication
DC to DC geo-redundancy

Recycle Bin
Limited, short term data loss recovery (no point-in time recovery)

Office 365 Backup
Copy of your data stored in a different location

Full Data Retention
ST & LT retention filling any/all policy gaps granular & point-in time recovery options

Security

Infrastructure-Level

Physical Security
Logical Security
App-level Security
User/Admin Controls

Data-Level

Internal:
Accidental Deletion
Malicious Insiders
Employee Retaliation
Evidence Tampering

External:
Ransomware
Malware
Hackers
Rogue Apps

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
The Office 365 Shared Responsibility Model

Microsoft’s Responsibility

- MICROSOFT GLOBAL INFRASTRUCTURE
  - Uptime of the Microsoft Office 365 Cloud Service

Supporting Technology

- Office 365 Data Replication
  - DC to DC geo-redundancy

- Recycle Bin
  - Limited, short term data loss recovery (no point-in-time recovery)

Security

- Infrastructure-Level
  - Physical Security
  - Logical Security
  - App-level Security
  - User/Admin Controls

- Data-Level
  - Internal:
    - Accidental Deletion
    - Malicious Insiders
    - Employee Retaliation
    - Evidence Tampering
  - External:
    - Ransomware
    - Malware
    - Hackers
    - Rogue Apps

Regulatory

Role as data processor

- Data Privacy
- Regulatory Controls
- Industry certifications
- HIPAA, Sarbanes-Oxley

Role as data owner

- Answer to corporate and industry regulations
- Demands from internal legal and compliance officers

YOUR Responsibility

- YOUR OFFICE 365 DATA
  - Access and control of your data residing in Office 365

- Office 365 Backup
  - Copy of your data stored in a different location

- Full Data Retention
  - ST & LT retention filling any/all policy gaps
  - Granular & point-in-time recovery options

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
Office 365 Trust Center

Welcome to the place where we share our commitments and information about security, privacy, and compliance.

Watch all security-related videos From Inside the Cloud

With Office 365, it’s your data. You own it. You control it. And it is yours to take with you if you decide to leave the service. The core tenets of our approach to earning and maintaining your trust are:

**Built-in security**
- Service-level security through defense-in-depth

**Privacy by design**
- Your data is not used for advertising
Mailservice Ransomware

Hello, a new feature!

Mailservice Ransomware

Mailservice Ransomware


© 2019 Vectra Software, A Fortinet Company. All Rights Reserved. All Trademarks are the property of their respective owners.
Hello, a new feature!

Read and write access to your mail

Mailservice Ransomware

Hello, a new feature! → OAuth Token → Malware encrypting objects

Mailservice Ransomware

Mailservice Ransomware

Hello, a new feature! → OAuth Token → Malware encrypting objects → Bitcoins accepted!


© 2020 Venafi Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
Mailservice Ransomware

What’s Microsoft Protecting & For How Long

Veeam Backup for Microsoft Office 365

Inbox or folder data
- In Office 365 (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Moved to archive

Deleted items (recycle bin)
- In Office 365 (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Permanently deleted

Auto-archived data (set at 1 month)
- In Office 365 (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Moved to archive

Deleted SharePoint Online sites and items
- 1st stage recycle bin (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- 2nd stage (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Permanently deleted

Deleted OneDrive for Business files
- 1st stage recycle bin (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- 2nd stage (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Permanently deleted

Employee leaves the company
- In Office 365 (1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs)
- Permanently deleted

The average length of time from data compromise to discovery is over **140 days**, yet default settings only protect for 30–90 days.

Source: Microsoft Office 365, 6 steps to holistic security, chapter 1
## Meeting Retention & Availability Policies

### Veeam Backup for *Microsoft Office 365*

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbox or folder data</td>
<td>1 wk, 1 mo, 3 mo, 1 yr, 2 yrs, 5 yrs</td>
</tr>
<tr>
<td>Deleted items (recycle bin)</td>
<td></td>
</tr>
<tr>
<td>Auto-archived data (set at 1 month)</td>
<td></td>
</tr>
<tr>
<td>Deleted SharePoint Online sites and items</td>
<td></td>
</tr>
<tr>
<td>Deleted OneDrive for Business files</td>
<td></td>
</tr>
<tr>
<td>Employee leaves the company</td>
<td></td>
</tr>
</tbody>
</table>

**Veeam Backup for Microsoft Office 365** is more than simply filling gaps. It’s about providing access and control to ALL Exchange Online, SharePoint Online and OneDrive for Business data and storing it in one location, making recovery fast, easy and reliable.
Veeam Availability Platform

**Multi-cloud data management:** A layer that sits over multiple cloud platforms and orchestrates the management of resources and the movement of data between them.

<table>
<thead>
<tr>
<th>Monitoring &amp; Analytics</th>
<th>Orchestration</th>
<th>Backup &amp; Replication</th>
<th>Universal APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>DataLabs</strong></td>
<td></td>
</tr>
</tbody>
</table>

Cloud | SaaS | Physical | Virtual

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
**Multi-cloud data management**: A layer that sits over multiple cloud platforms and orchestrates the management of resources and the movement of data between them.

- Monitoring & Analytics
- Orchestration
- Backup & Replication
  - DataLabs
- Universal APIs
  - Cloud: Microsoft Azure, IBM Cloud, Veeam Cloud Service Providers
  - SaaS: Office 365, OneDrive
  - Physical: Windows, Linux, AIX, NAS, Oracle Solaris
  - Virtual: VMware, Microsoft Hyper-V, Nutanix, AHV

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
Cloud backup and DRaaS

Managed Cloud Provider

- Cloud backups & replicas
- Virtual servers
- Workstations
- Physical servers

Disaster recovery failover/failback

To the cloud

Protected with Veeam

Customer Environment
Cloud Data Retention

Infinite capacity for transparent, long-term data retention using native object storage integration for up to 10x cost savings.

**Solutions:**
- Veeam Cloud Tier (AWS, Azure, IBM Cloud, and S3-compatible service providers)
- VTL to AWS or Azure
IaaS and SaaS data protection

From the cloud

Public Cloud

- Public cloud workloads

SaaS

- Microsoft Office 365

Backups stored on premises

Customer Environment

Protected with Veeam
Cross-cloud data protection

Public Cloud

Public cloud workloads

Microsoft Office 365

Your hosted services

Replication between your data centers

Cloud backups & replicas

Your Managed Cloud

Protected with Veeam

Within the cloud
Backup and Disaster Recovery for AWS

- Founded in 2014 out of Israel
- Selling solution through AWS MP since 2014
- 2016 Investment from Insight VC & Veeam
- 2017 Partnership with Veeam
- Veeam acquired N2WS in early 2018
Cloud Mobility

Gain data portability by recovering any on-premises or cloud-based workload across your multi-cloud environment, today or in the future.

**Solutions:**
- Veeam Cloud Mobility
  - Direct Restore to AWS
  - Direct Restore to Azure
  - Direct Restore to Azure Stack
- Veeam has Cloud Mobility with IBM Cloud as Veeam can access the hypervisor in the cloud

*Veeam Backup & Replication
Veeam Agent for Microsoft Windows
Veeam Agent for Linux*
Veeam Cloud Mobility

2 steps for portability and recovery to AWS, Azure and Azure Stack

Data portability is critical for organizations to maintain speed and control of their environment.

- Easy portability and recovery of ANY on-premises or cloud-based workloads to AWS, Azure, and Azure Stack
- Just 2 steps to maintain business continuity and Availability across hybrid-cloud environments.

- Portability of workloads to the cloud
- Restore and recover workloads to the cloud for business continuity
- Unlock test and dev for data backups to the cloud
- Automated UEFI to BIOS conversion for AWS EC2

© 2020 Veeam Software. Confidential Information. All rights reserved. All trademarks are the property of their respective owners.
VCSP Partner Ecosystem
Veeam Cloud & Service Provider

~22,000 VCSP Global Partners

- Cloud backup & Disaster Recovery as a Service (DRaaS)
- Infrastructure as a Service (IaaS) & Software as a Service (SaaS) data protection
- Cross-cloud data protection
- Remote managed services
Thank You!

veeAM
My quote in this article shows why companies don't need to plan on being multi-cloud, they already are. With 81% of companies already multi-cloud today, vendors need to about multi-cloud as an operational reality, not a future state.

#Multi-cloud continues to go full-speed ahead, but some find themselves forced into the model. "Most companies don't choose multi-cloud. They have it thrust upon them because that is the reality of how people work," said @edwinyuen @esg_global