

Cloud Backup – So sichern Sie Ihre Daten einfach und zuverlässig



Patric Hermann

Systems Engineer
Veeam Software GmbH
Patric.Hermann@veeam.com

Modern Data Protection & Cloud Offerings



Cloud



AWS



Azure



Google Cloud

vmware®



vSphere

Microsoft Hyper-V

Virtual



IBM Cloud



Nutanix AHV

A Single Platform

To Protect and Manage All Workloads



Windows



Kubernetes



Linux



MAC



UNIX³



NAS



Office 365



Databases²



Microsoft¹

Physical

SaaS

Apps

¹ Microsoft Active Directory, Exchange, SharePoint

² Microsoft SQL Server, Oracle, Oracle RMAN, PostgreSQL, MySQL and SAP Hana

³ IBM AIX and Oracle Solaris

3-2-1-0 Rule

3-2-1-0 Rule

3

Different copies
of data



2

Different media



1

of which
is off site



0

No errors



Avoiding recovery failure

Veeam's Cloud Offerings

Private | Public | Hybrid | Multi | as a Service

CLOUD-NATIVE



Cloud-native backup and recovery for
AWS, Azure and Google Cloud Platform



Backup, restore and eDiscovery for
Microsoft Office 365

EXTEND TO THE CLOUD



Extended capacity and archive with
Backup to cloud-based object storage



Ransomware stays out with
immutable backups in the cloud



Direct-to-cloud restore functions for
cloud-based dev/test

POWERED BY VCSP PARTNERS



Expert-built, hybrid cloud
BaaS for the data center



Direct-to-cloud backup for laptops
with BaaS for endpoints



Cloud-powered failover
with DRaaS



Cross-cloud backup with BaaS for
Office 365, AWS and Azure

4-in-1 for Best RPOs



1. Backup



2. Replication



3. Storage snapshots



4. CDP

Veeam Cloud Connect

Veeam Cloud Connect

Hosted offsite backup and DR Service, to offer an alternative to having a secondary Data Centre or Disaster Recovery site. Enabling 3-2-1 safety for all workloads

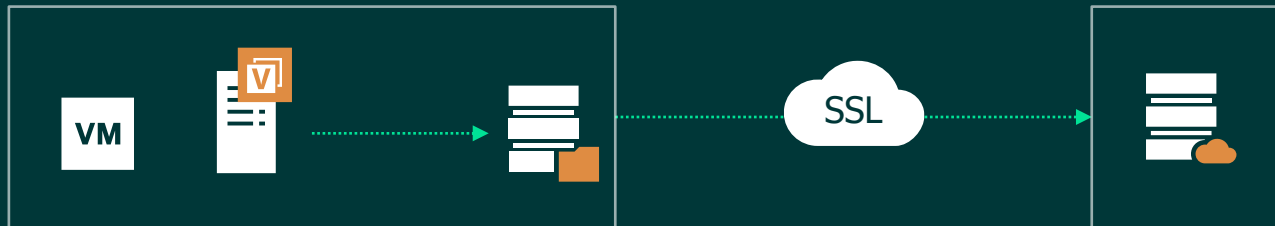
Single SSL Port

- No expensive MPLS, Express Route or VPN connectivity required

Consolidate customer backups to one centralized location

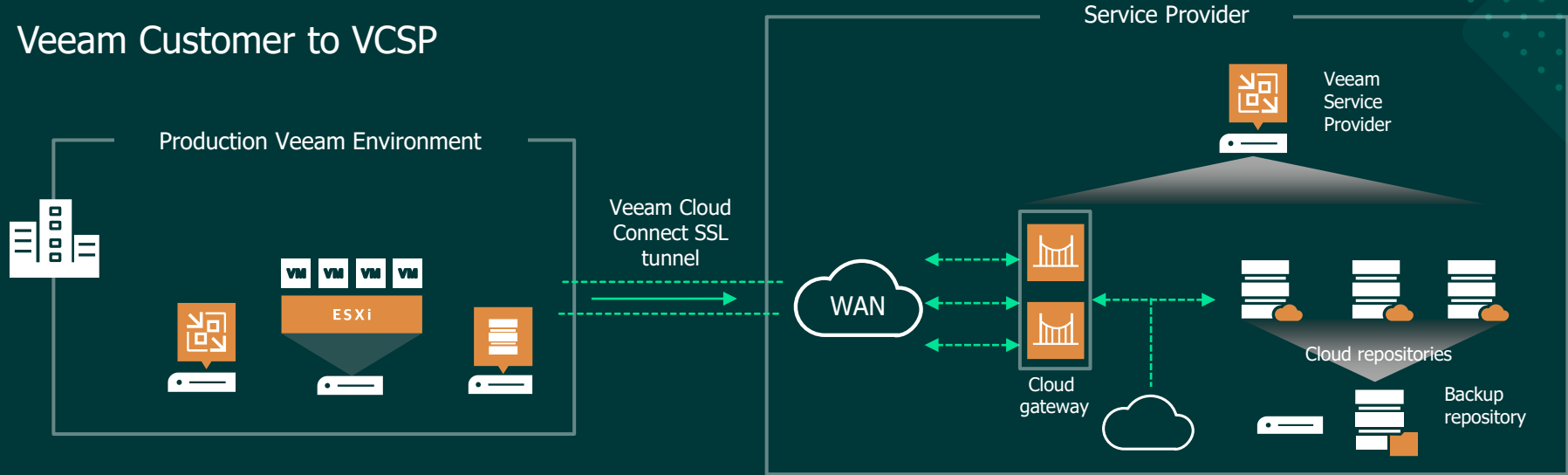
Backup your data directly to the Cloud using Cloud Connect Repositories

- No connectivity to corporate network needed



Veeam Cloud Connect Backup

Veeam Customer to VCSP



Backup data from on-premises to VCSP

Service Provider can leverage AWS, Azure or other IaaS offerings

Customer has no cloud resources to manage

Veeam Cloud Connect Replication

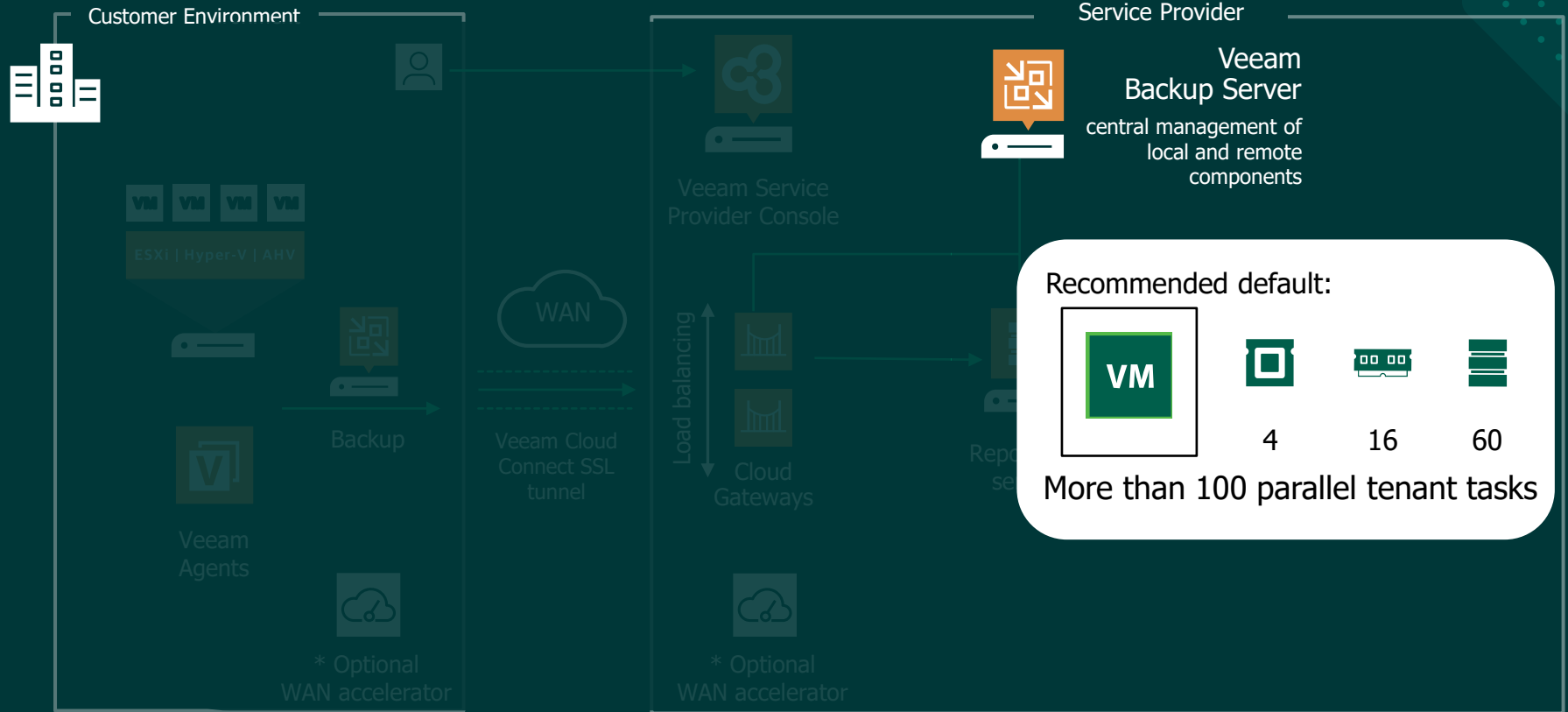
Veeam Backup & Replication provides disaster recovery through **image-based VM replication**.

Provide Veeam Cloud Connect Replication resources for the following virtualization platforms:

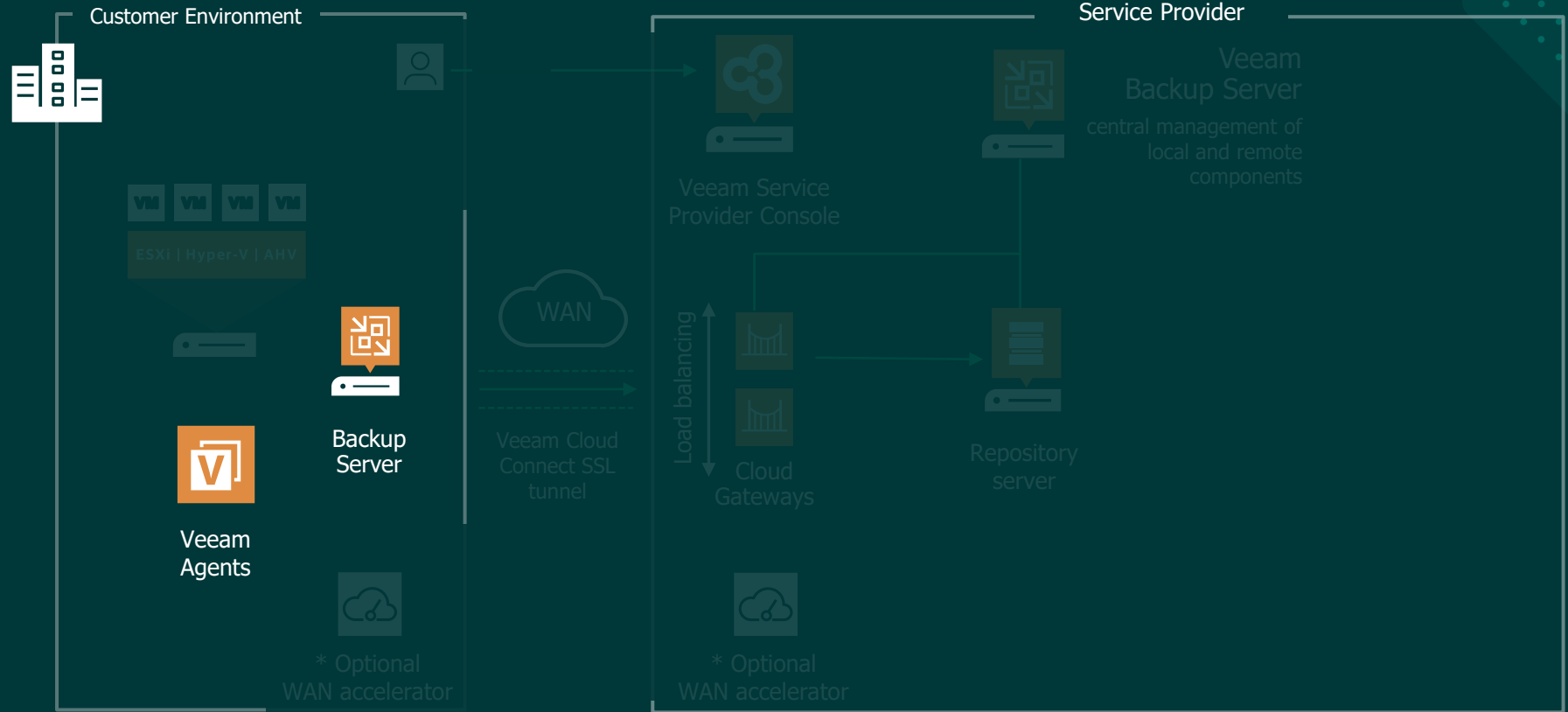
- VMware vSphere / vCloud Director
- Microsoft Hyper-V



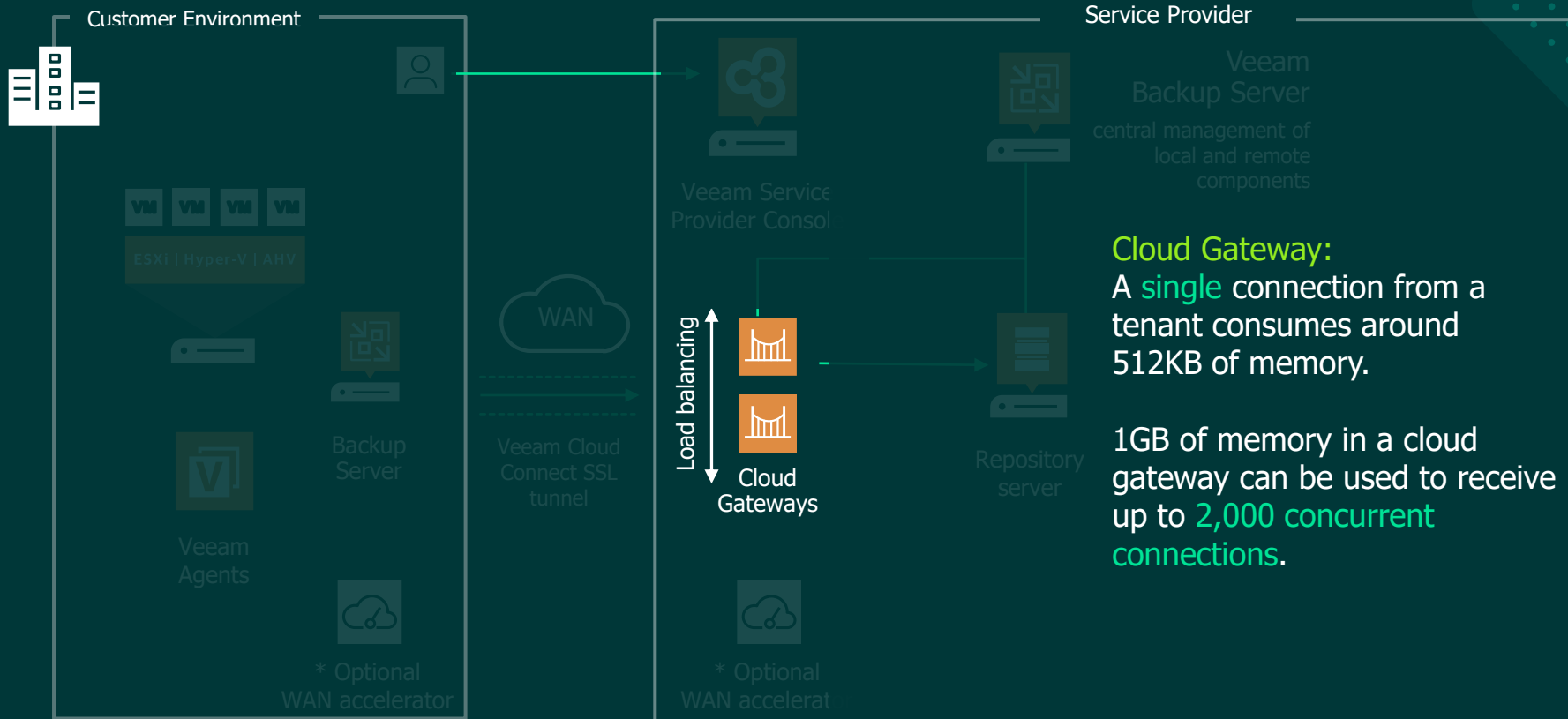
Service Provider Backup Server



Tenant Backup Server or Agents



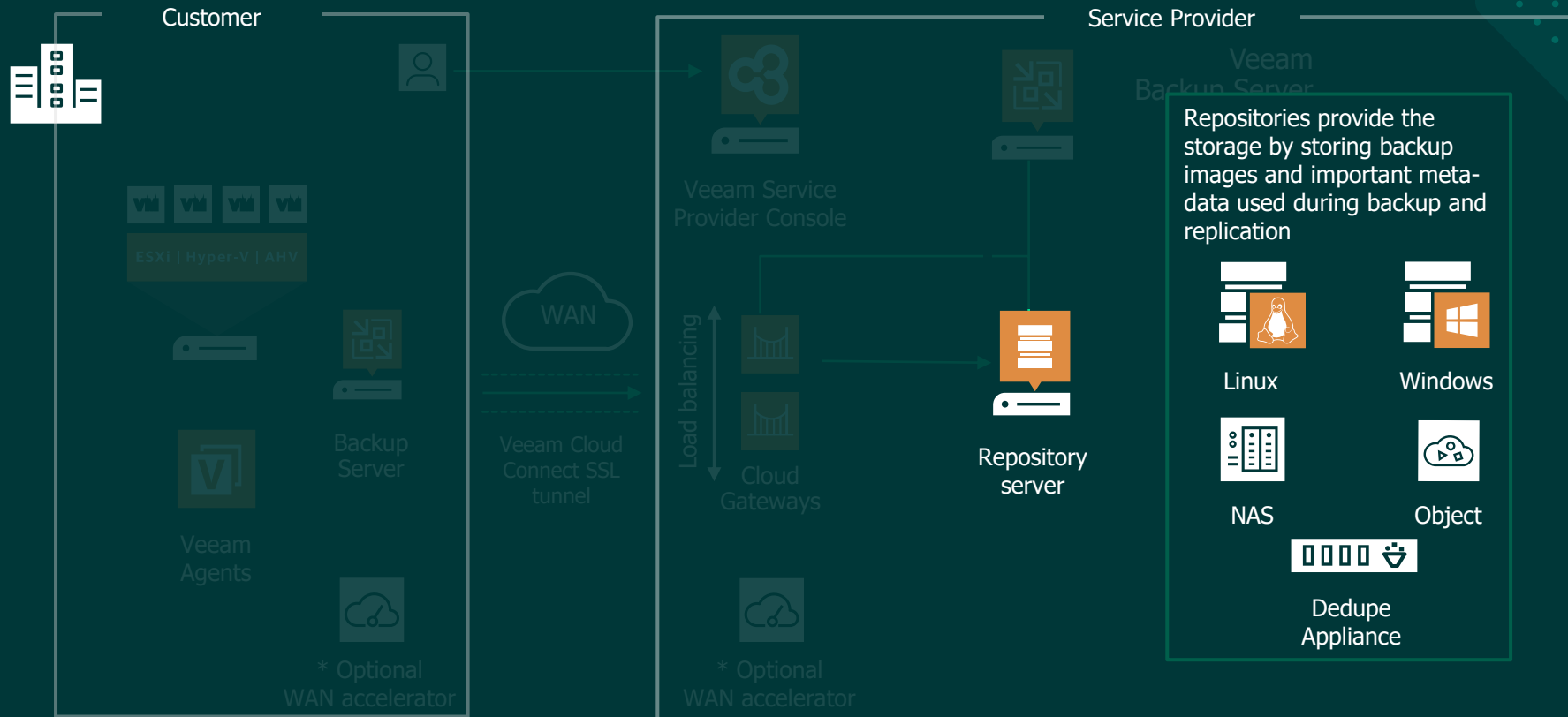
Cloud Gateways



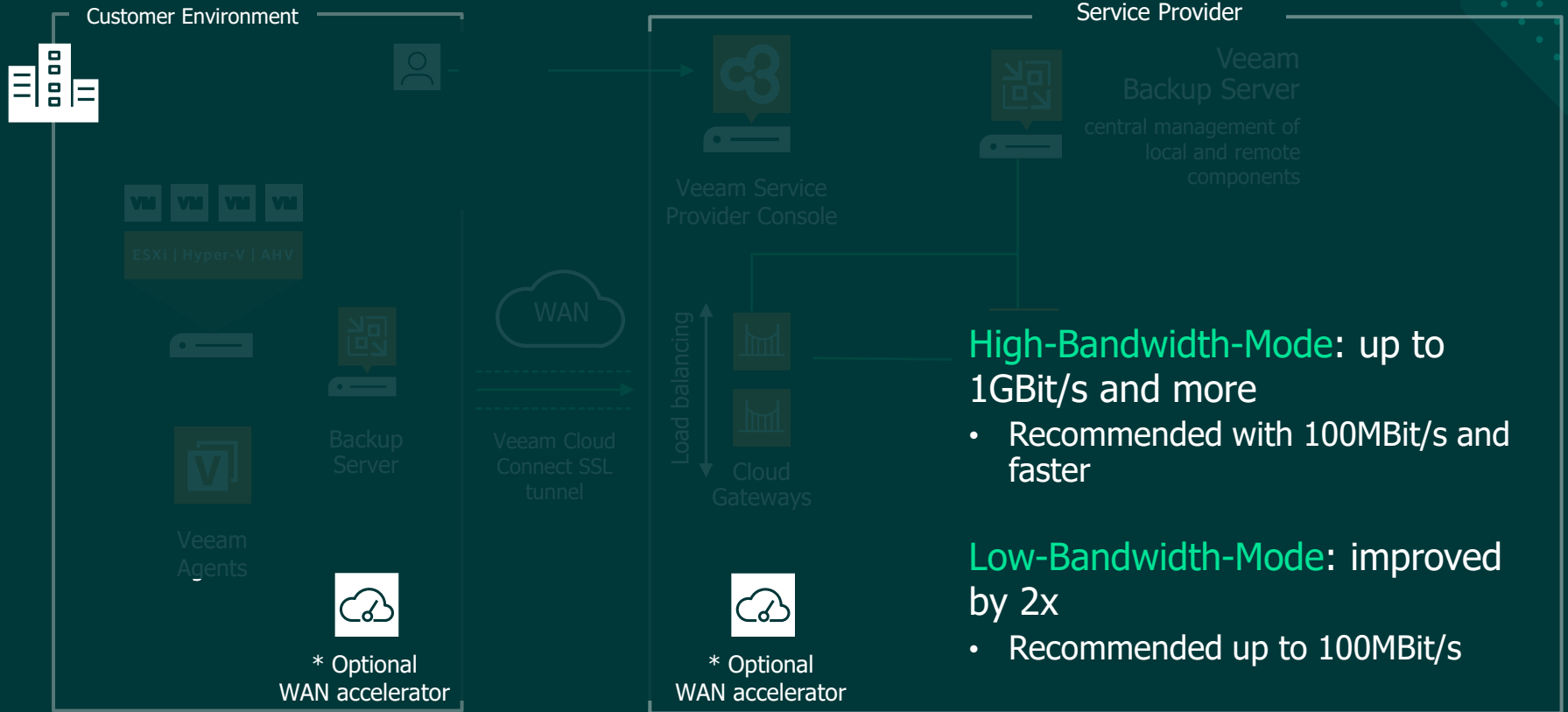
Cloud Gateway:
A **single** connection from a tenant consumes around 512KB of memory.

1GB of memory in a cloud gateway can be used to receive up to **2,000 concurrent connections**.

Cloud Repository



WAN Accelerators



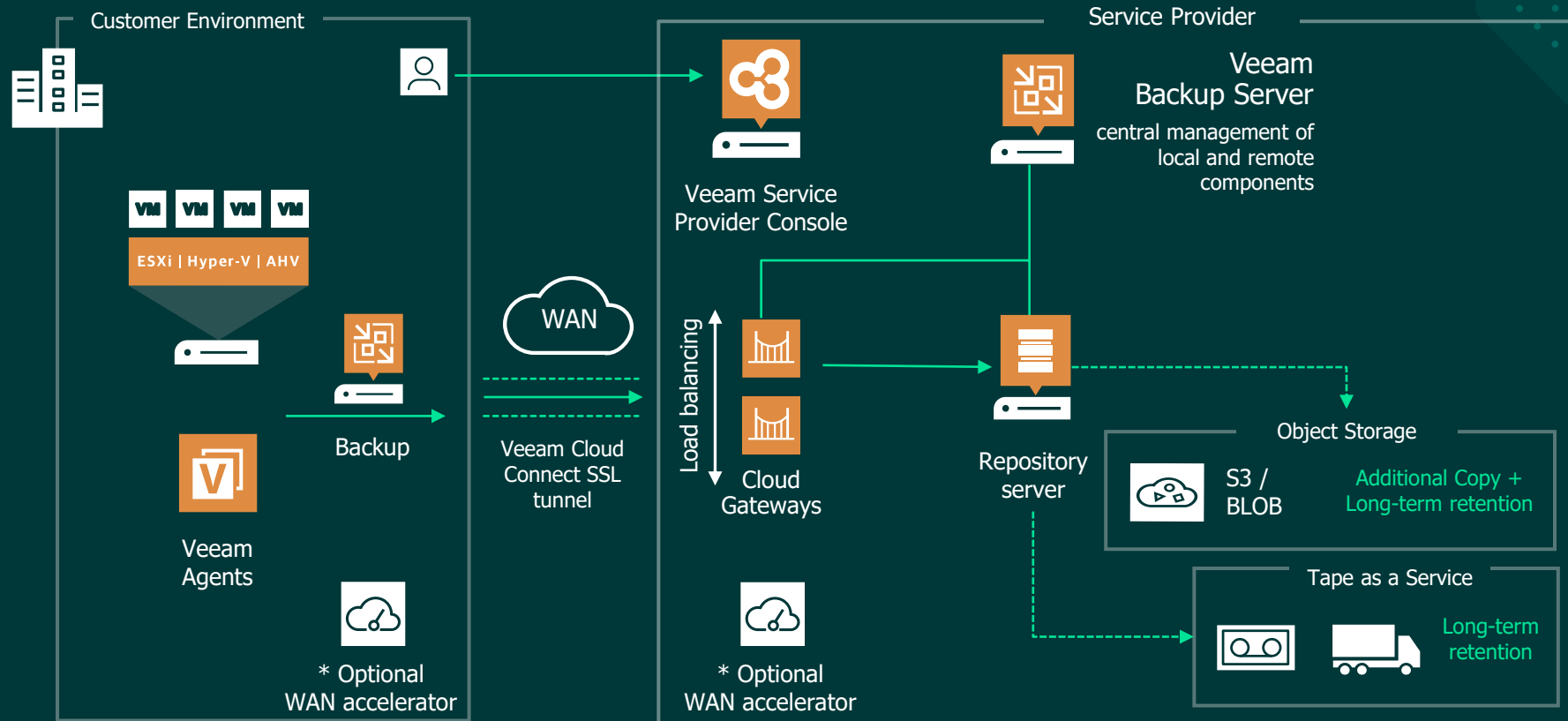
High-Bandwidth-Mode: up to 1Gbit/s and more

- Recommended with 100Mbit/s and faster

Low-Bandwidth-Mode: improved by 2x

- Recommended up to 100Mbit/s

Veeam Cloud Connect - Backup



Encryption

Data encryption helps tenants **protect sensitive** VM data from unauthorized access while this data is stored in the cloud repository.

It is **recommended** that the tenant **enables** the encryption option for backup jobs targeted at the cloud repository.



Network Traffic Throttling

By default, the Veeam backup server shares available bandwidth **equally** between **all tenants** who work with cloud backup and replication resources simultaneously. The bandwidth available to one tenant is equally split between all tasks performed by this tenant.

For example, the cloud repository is used by two tenants simultaneously:

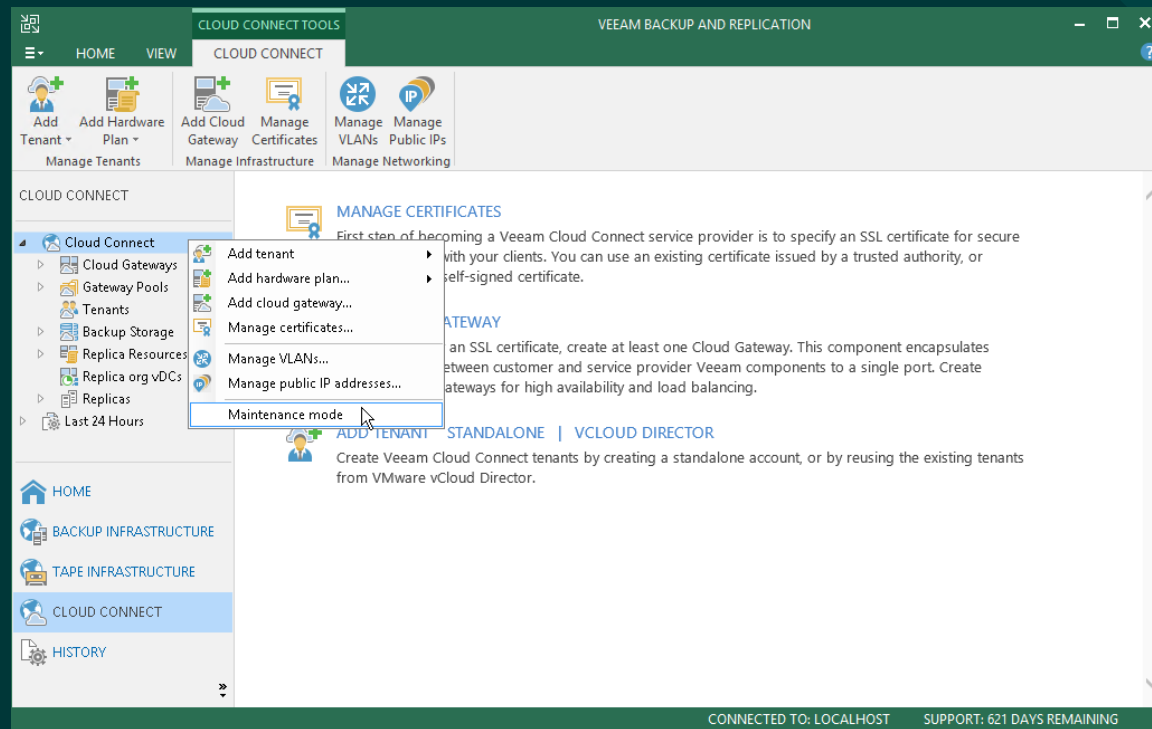
- *Tenant 1* runs 2 tasks, backup and restore.
- *Tenant 2* runs 1 task.

In this situation, *Tenant 1* will get **50% of bandwidth** and this bandwidth will be equally split between 2 tasks: **25% of the initial bandwidth per task**. The task performed by *Tenant 2* will get **50% of the initial bandwidth**.



Maintenance Mode

When the SP backup server activates in **Maintenance mode**, Veeam Backup & Replication notifies tenants who perform backup and/or backup copy jobs that the SP backup server is **under maintenance** and cloud resources are temporary unavailable.



Recover Full VMs, Files and Folders

Restore functionalities include:

- Full VM restore
- VM files restore
- VM guest OS files restore
- Application items restore
- Disk export
- Backup export

The screenshot displays the Veeam Backup and Replication console. The top navigation bar includes 'HOME' and 'BACKUP' tabs. Below the navigation bar is a toolbar with various actions: 'Instant VM Recovery', 'Entire VM', 'Virtual Disks', 'VM Files', 'Guest Files', 'Application Items', 'Amazon EC2', 'Microsoft Azure', 'Export Backup', and 'Delete from Disk'. The main area shows a list of backup jobs with columns for 'JOB NAME', 'CREATION TIME', 'RESTORE POINTS', and 'REPOSITORY'. A context menu is open over the 'apache02' backup item, listing options such as 'Instant VM recovery...', 'Restore entire VM...', 'Restore virtual disks...', 'Restore VM files...', 'Restore guest files', 'Restore to Amazon EC2...', 'Restore to Microsoft Azure...', 'Export backup...', and 'Delete from disk'. The 'Restore guest files' option is expanded, showing sub-options for 'Microsoft Windows...' and 'Linux and other...'. The left sidebar shows a navigation tree with 'HOME', 'INVENTORY', and 'BACKUP INFRASTRUCTURE' sections.

JOB NAME	CREATION TIME	RESTORE POINTS	REPOSITORY
ABC Company DB Backup	12/22/2018 10:00 PM		ABC Company
ABC Company Webservers Backup	12/22/2018 10:00 PM		ABC Company
apache02		5	
webserv02		5	
SRV12 Workstation Backup		2	TechCompany
SRV13 Fileserver Backup		3	ABC Company

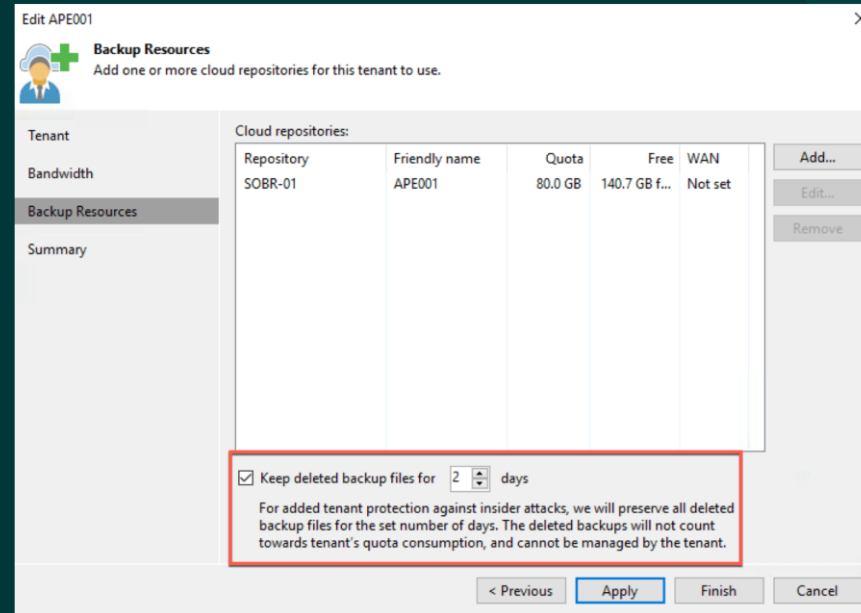


Insider Threat Protection

Insider Threat Protection

Insider Threat Protection is an additional **protection mechanism** for Veeam Cloud Connect backups, able to **guarantee** the **safety of backups** stored in Cloud Connect against mis-deletions or attack.

For example during ransomware attacks to present the victim to avoid paying the ransom by **restoring data** from backup.



Edit APE001

Backup Resources
Add one or more cloud repositories for this tenant to use.

Tenant

Bandwidth

Backup Resources

Summary

Cloud repositories:












Repository	Friendly name	Quota	Free	WAN
SOBR-01	APE001	80.0 GB	140.7 GB f...	Not set

Keep deleted backup files for 2 days

For added tenant protection against insider attacks, we will preserve all deleted backup files for the set number of days. The deleted backups will not count towards tenant's quota consumption, and cannot be managed by the tenant.

< Previous Apply Finish Cancel

Insider Protection

NAME	STATUS	ACTION	DURATI...
 itlabsrv01	 Pending	 Job started at 12/1/2018 3:00:17 AM	
 itlabsrv03	 Pending	 New copy interval started	
 itlabsrv02	 Pending	 Your service provider has implemented backup files protection against deletion...	
		 Building VMs list	00:02
		 Waiting for new restore points	16:19:29

Your service provider has **implemented backup files protection** against deletion by an insider for this cloud repository.

To **protect against advanced attack vectors**, we recommend that you configure your cloud backup jobs to keep **multiple full backups** on disk (as opposed to forever-incremental chain with a single full backup)



Demo

Thank you

veeam



THOMAS
KRENN®

Cloud Backup

„So sichern Sie Ihre Daten einfach und zuverlässig“

TH-MAS
KRENN®

VEEAM



Kurzvorstellung

Cloud-Marktanalyse

3-2-1-Regel

Praxisbeispiel: Veeam Cloud Backup

Kurzvorstellung



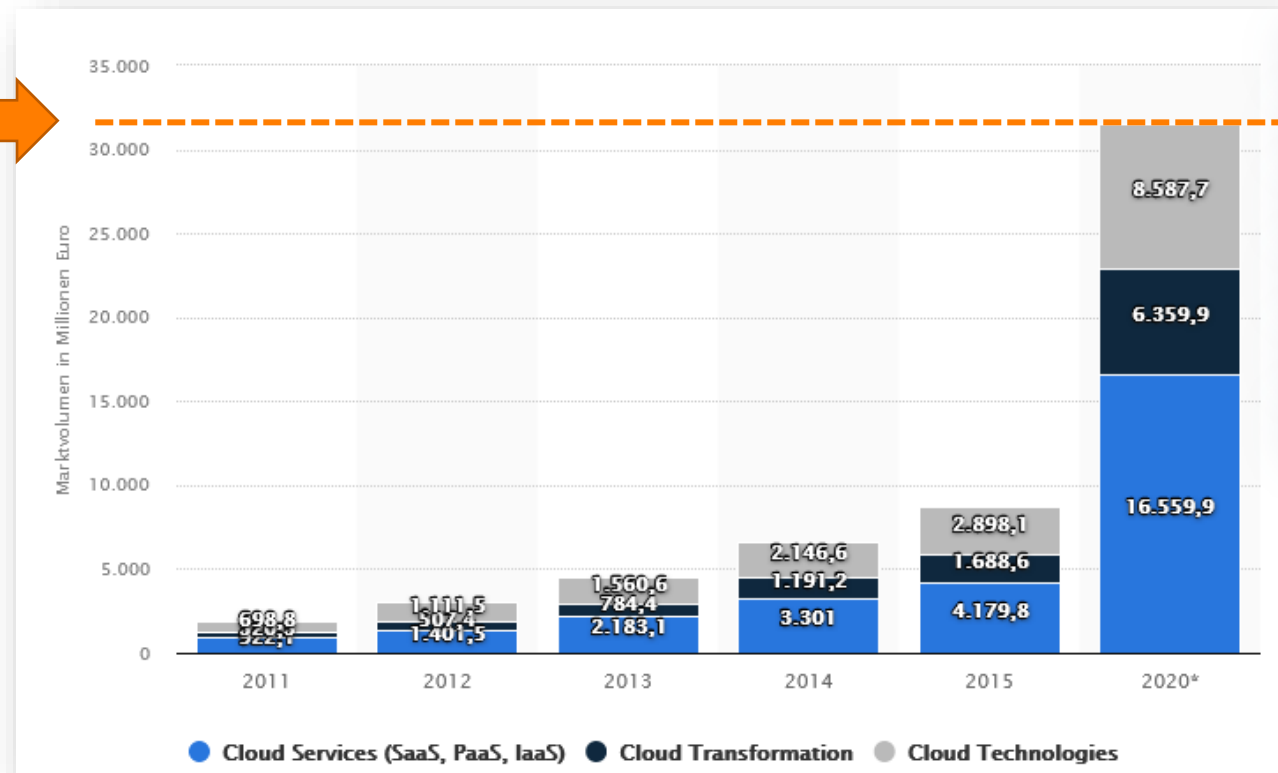
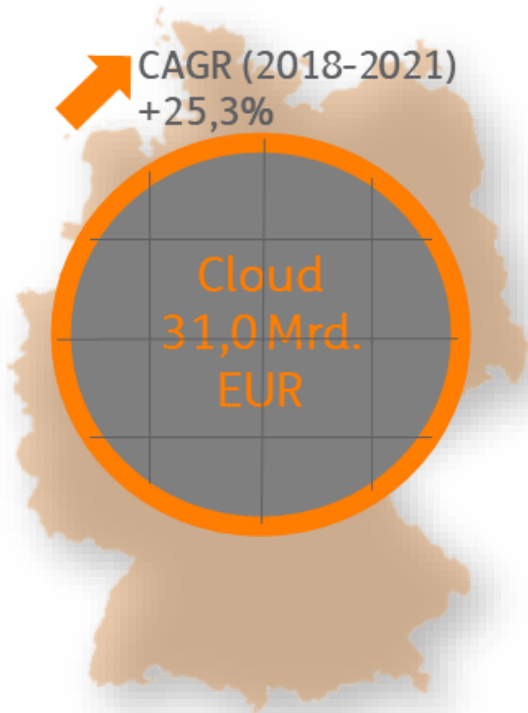
Uli Hurzlmeier

- 33 Jahre
 - B. Eng Technologiemanagement
- Business Developer
- Branchenerfahrung:
 - Industrie, Schwerpunkt:
 - Maschinenbau für die Lebensmittelindustrie

Cloud-Marktanalyse

Marktanalyse

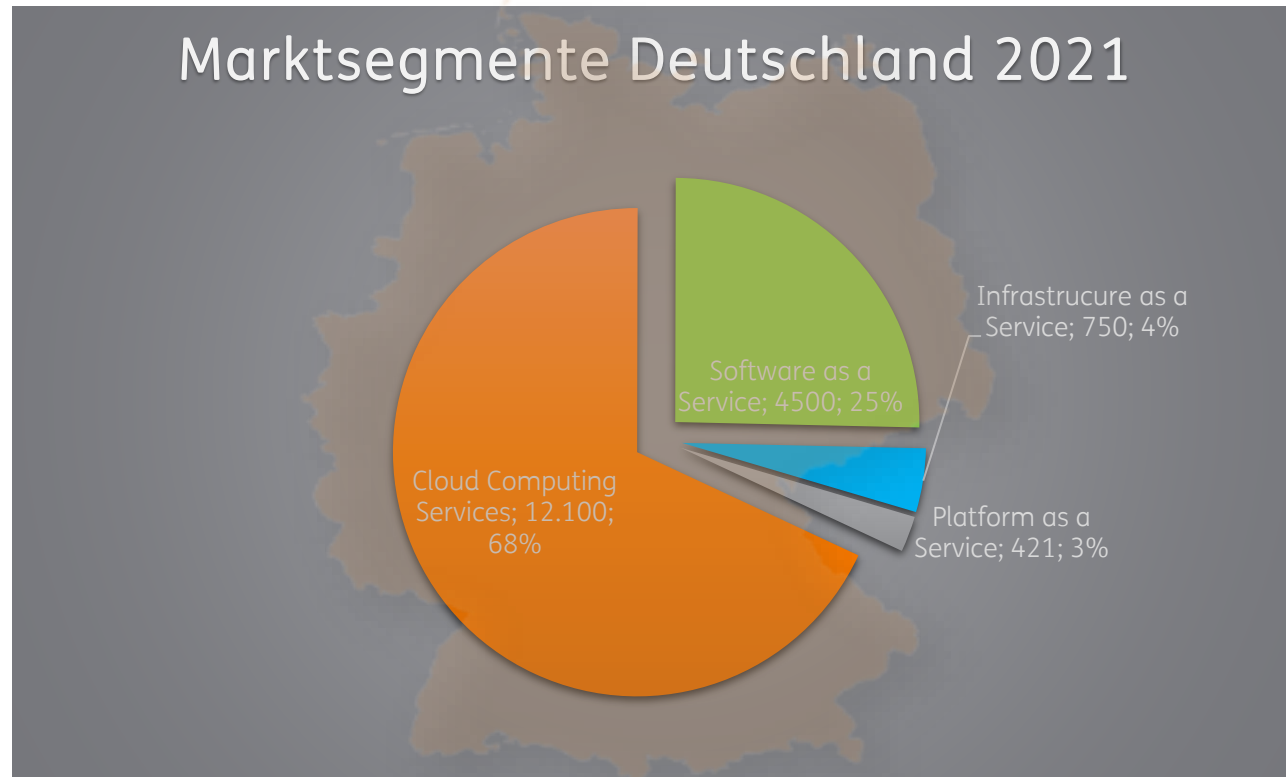
Marktvolumen von Cloud Computing (B2B) in Deutschland nach Segment von 2011 bis 2015 und Prognose für 2020



Quelle: Statista, Abrufdatum: 09.11.2021

Marktanalyse

Cloud - Marktsegmente Deutschland 2021



Wichtige Kennzahlen

MARKTKENNZAHLEN DEUTSCHLAND

Prognose zum Umsatz mit Cloud-Computing-Services in Deutschland 2021

12,1 Mrd. €

Marktvolumen von SaaS in Deutschland

4,5 Mrd. €

Marktvolumen von PaaS in Deutschland

421 Mio. €

Marktvolumen von IaaS in Deutschland

705 Mio. €

Quelle: Statista, Abrufdatum 09.11.2021

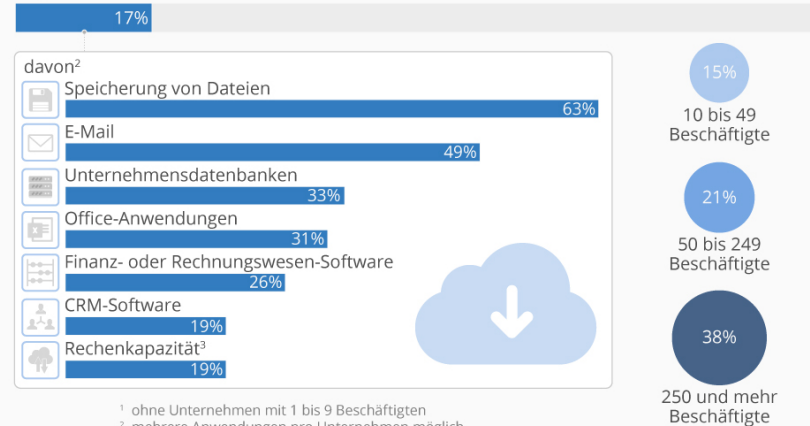
Marktanalyse

Trends

So viele Unternehmen zahlen für die Cloud

Unternehmen¹ in Deutschland, die kostenpflichtige Cloud Services nutzen, 2016

Insgesamt

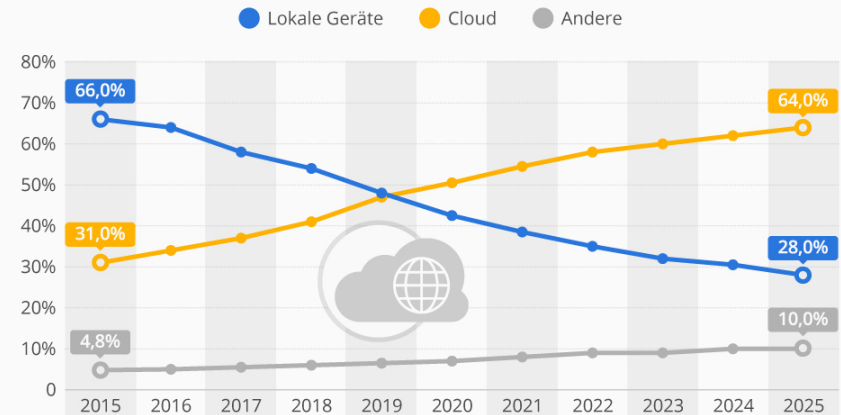


¹ ohne Unternehmen mit 1 bis 9 Beschäftigten
² mehrere Anwendungen pro Unternehmen möglich
³ zur Ausführung unternehmenseigener Software
Quelle: Statistisches Bundesamt

Quelle: Statista, Abrufdatum: 09.11.2021

2020 überholt die Cloud lokale Speichermedien

Anteile technischer Lösungen an der Speicherung des weltweiten Datenaufkommens



Quelle: Statista Digital Economy Compass 2019

Quelle: Statista, Abrufdatum: 09.11.2021

Ausgangssituation

Warum Cloud Backup?



Konformität

- Aufbewahrungsfristen für Daten gesetzlich gefordert (z.B. §147 AO)
- Art und Weise der Datensicherung nicht gesetzlich vorgeschrieben
- DSGVO-Konformität gefordert, speziell bei personenbezogenen Daten



Verfügbarkeit & Sicherheit

- Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr
- Cyberattacken betreffen nahezu 9 von 10 Unternehmen



Wirtschaftlichkeit

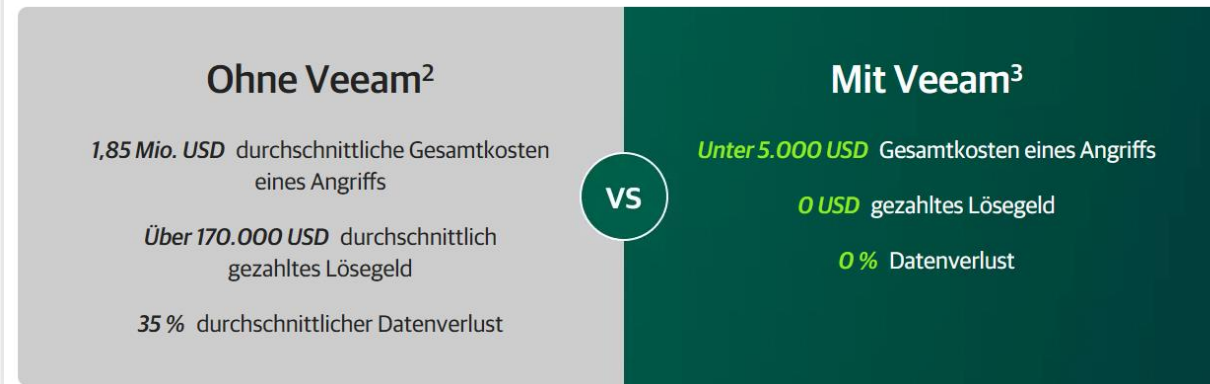
- Ausfall der IT-Infrastruktur oder Datenverlust führen zu erheblichen Einschränkungen im Geschäftsablauf

Ausgangssituation

Zahlen und Fakten

Die wahren Kosten von Ransomware

2021 ist die Anzahl der Ransomware-Angriffe um 93 % angestiegen¹. Bei Ransomware geht es längst nicht mehr um das **Ob**, sondern das **Wann**. Mit Veeam schützen Sie Ihr Unternehmen vor ALLEN Cyberangriffen.



¹ Check Point Software. Mid-Year 2021 Security Report.

² Sophos (April 2021). The State of Ransomware 2021.

³ Veeam (13. August 2020). Ransomware Study Final Analysis.

Backups sind für jedes Unternehmen überlebensnotwendig.

Dennoch sind sie gerade in IT-fernen Branchen oft ein „lästiges Muss“.

Mit der Datensicherung in der Cloud vereinfacht sich jetzt nicht nur der Prozess, die Daten bleiben hochverfügbar, maximal geschützt und können im Ernstfall sofort wieder hergestellt werden.

3-2-1-Regel

3-2-1-Regel

3-2-1 Regel



Definition

- 3 unterschiedliche Kopien, 2 unterschiedliche Medien, 1 externe Kopie
 - Ortsunabhängige Sicherung der Daten
 - Erhalt Ihrer Sicherungskopie selbst bei Naturkatastrophe, Brand o.ä.
 - Beschleunigte Wiederherstellung im Schadensfall oder bei Verlust

Praxisbeispiel

Darum Veeam Cloud Backup

Zusammenfassung

- Einfaches Auslagern Ihrer Backups in das Veeam Cloud-Repository
 - Weniger personeller Aufwand
 - Jederzeit hochverfügbare Daten
- Intuitive Bedienung (Sie haben bereits Veeam im Einsatz – umso einfacher!)
- Maximale Flexibilität, Skalierbarkeit & Kostenkontrolle
 - Sie passen die Größe einfach Ihrer Datenmenge an und bezahlen nur, was Sie auch wirklich brauchen
 - Monatliche Bezahlung – jederzeit kündbar!



**THOMAS
KRENN®**

Vielen Dank für Ihre
Aufmerksamkeit!

