Securing Microsoft O365 Data

CLOUDLAYER

cl8
.com

'OUR CLOUD. YOUR WAY.

Michael Tsistrakis

CLOUDLAYER8 LIMITED
Business Development Manager
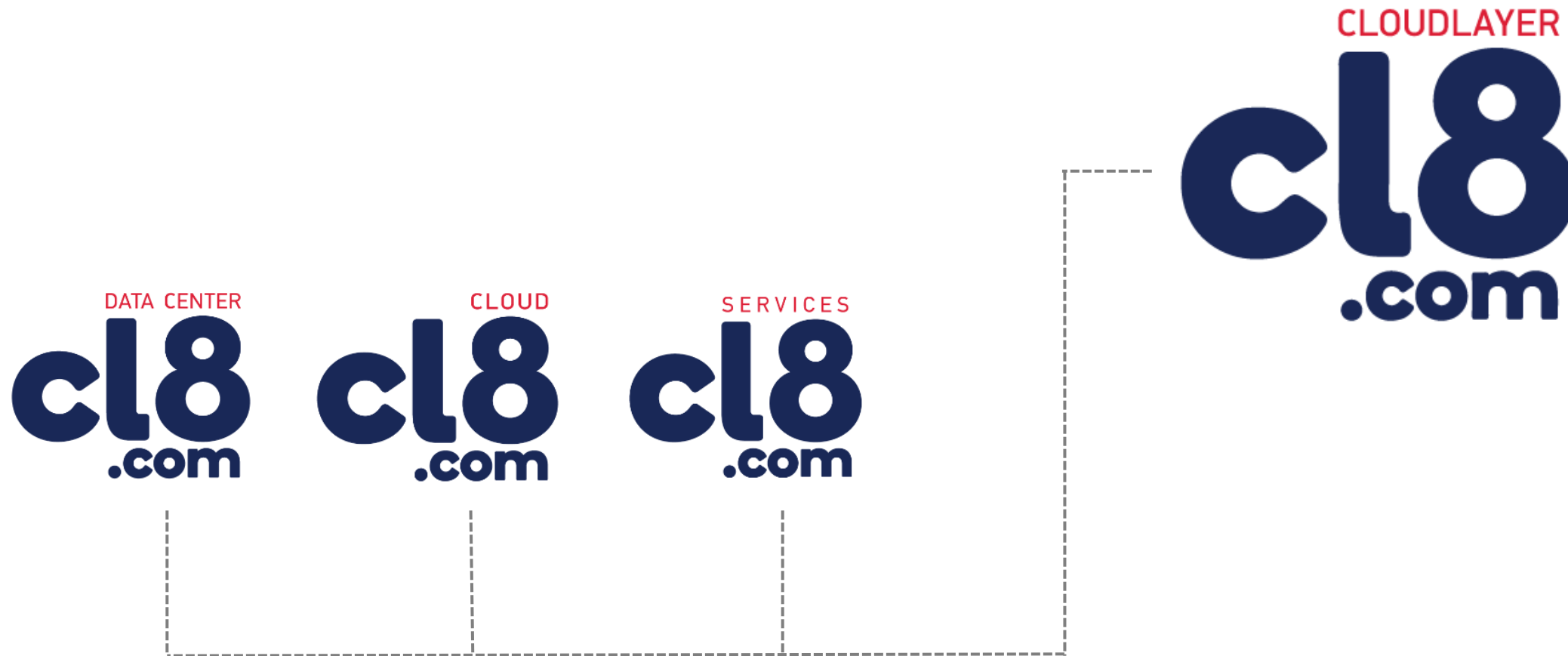
July 2023

A few words about CL8

CL8...

- TIER III Certified Data Center
- Carrier Neutral Multiple ISPs, Multiple Paths
- Always on DDoS Protected services
- CY IX: member of the Cyprus internet network
- NoC 24/7/365 Support, Real people, Real Time
- SLA for provided services, money back guarantee
- Data Center, Cloud & Managed Services
- Team of highly qualified professionals
- Highest Standards and Certifications
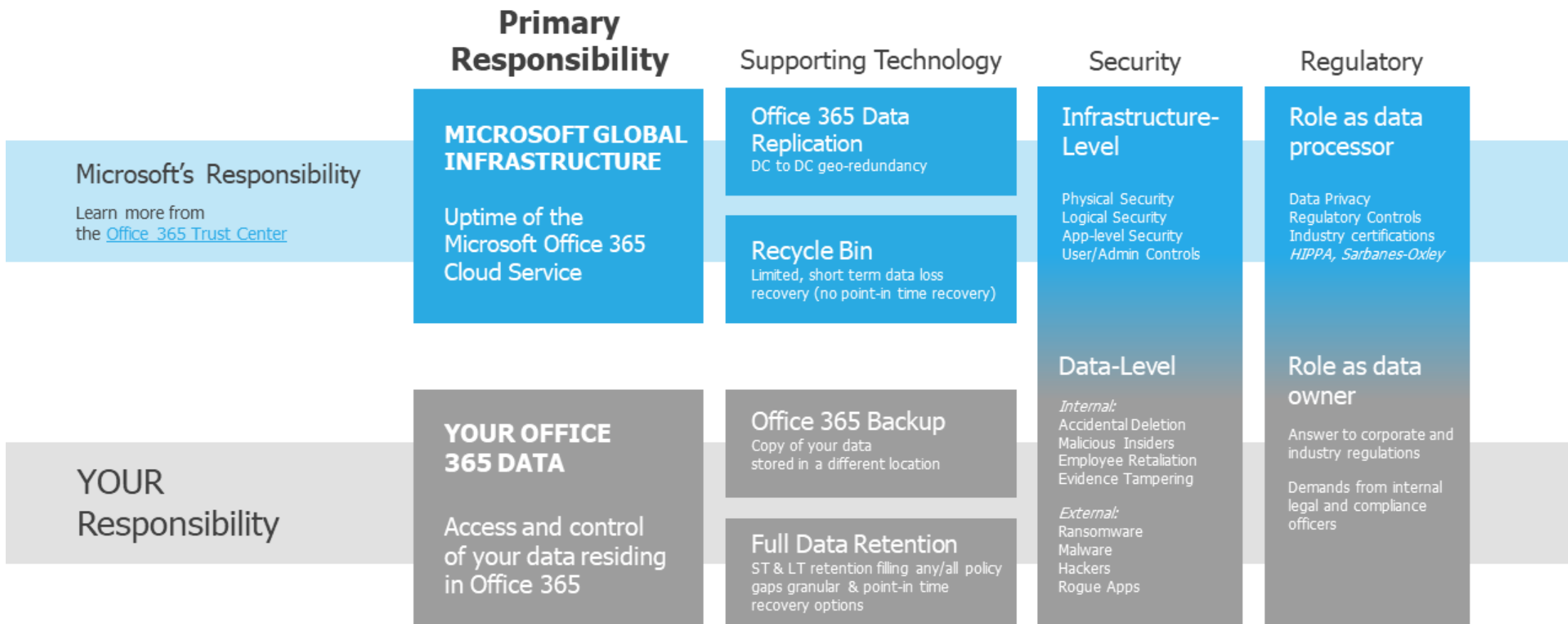- Packaged and Custom Solutions

Certifications

3 Pillars

Securing Microsoft O365 Data

The Office 365 Shared Responsibility Model

	Primary Responsibility	Supporting Technology	Security	Regulatory
Microsoft's Responsibility Learn more from the Office 365 Trust Center	**MICROSOFT GLOBAL INFRASTRUCTURE** Uptime of the Microsoft Office 365 Cloud Service	**Office 365 Data Replication** DC to DC geo-redundancy **Recycle Bin** Limited, short term data loss recovery (no point-in time recovery)	**Infrastructure-Level** Physical Security Logical Security App-level Security User/Admin Controls	**Role as data processor** Data Privacy Regulatory Controls Industry certifications *HIPPA, Sarbanes-Oxley*
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	**Data-Level** *Internal:* Accidental Deletion Malicious Insiders Employee Retaliation Evidence Tampering *External:* Ransomware Malware Hackers Rogue Apps	**Role as data owner** Answer to corporate and industry regulations Demands from internal legal and compliance officers

veeam

Cyberattacks often target Microsoft 365

- **80%** of cyber attacks target Office applications

- **17%** of attacks originated via email and **25%** via malicious link phishing

- **1/3** of data on average is typically unrecoverable after an attack

Distribution of exploits used in attacks by type of application attacked (in %)

Application	%
Microsoft Office	80.09
Browsers	5.84
Android	4.69
Java	3.59
Adobe Flash	3.45
PDF	2.34
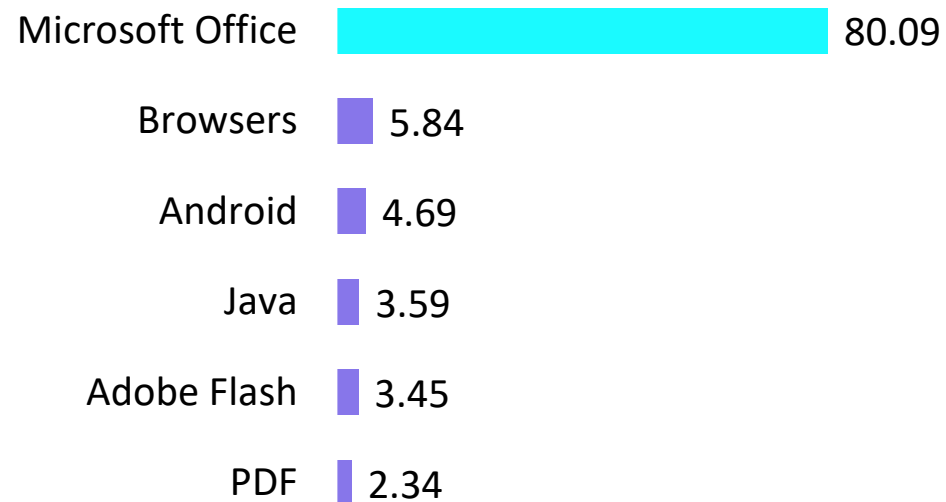
Source: IT threat evolution in Q3 2022
Source: 2022 Data Protection Trends Report, Veeam

Veeam Backup *for Microsoft 365*

Veeam Backup *for Microsoft 365* eliminates the risk of losing access to your Microsoft 365 data, including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams.

Infrastructure Freedom

- Any deployment: on-prem, cloud, BaaS
- Any storage: on-premises, cloud
- Any change: add/change storage, location anytime

Backup control

- Lowest RPO: as low as 5 mins
- Tiered protection: different backup frequencies for different users

Recovery flexibility

- Any recovery: broadest set of recovery options (50+ recovery options)
- Recovery out of M365: to on-premises, via email

Scalable recovery

- Powerful search: search across users, many search filters
- Bulk recovery: restore many users at once to effortlessly recover from disaster

Immutable backup copies

Backup copy immutability benefits

Get peace-of-mind that your Microsoft 365 data is out of reach from attacks

Immutable defense

Ensure that Microsoft 365 data is ransomware-proof – unable to be changed or deleted

Data separation

Establish true data separation with agnostic, immutable backup copies

Recovery confidence

Data can be recovered with ease without any missing or corrupt data

Advanced monitoring and reporting

Advanced monitoring benefits

Get peace-of-mind that your Microsoft 365 data is out of reach from attacks

Full visibility
At-a-glance dashboard view of Microsoft 365 backup performance

Proactive management
Quickly respond to and plan for changes or issues with real-time alerts

Compliance certainty
Ensure backup RPOs are met with intelligent reports

Advanced monitoring and reporting

Delivered through Veeam ONE

Visibility of Veeam Backup *for Microsoft 365* infrastructure components:

- Backup servers
- Backup proxies
- Backup repositories

What's inside:

- 10+ alarms
- Dashboard in Veeam ONE Web Client
- Historical and SLA-based backup reporting
- REST API endpoints
  (backup infrastructure components, jobs, protected objects, alarms)

Increased control with Veeam-powered BaaS
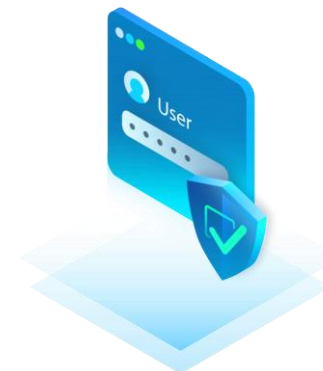
Benefits of Veeam-powered BaaS for Microsoft 365

Backup control
Tenants can create backups and monitor their protected Microsoft 365 data

Tenant autonomy
Organizations can restore their data without having to rely on their service provider

Easy adoption
Leveraging BaaS is made easy with secure onboarding and compliance reporting
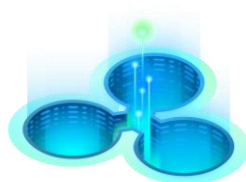
Increased control and self-service capabilities

Fully Self-service

No self-service options

Organization
owned
deployments

Veeam Cloud & Service Providers offer
Backup-as-a-Service for Microsoft 365
with flexible management and self-service
capabilities

Other
as-a-service vendors

Full control   No control

Self-Service Restore Portal Enhancements

Self-Service Restore Portal Enhancements

Self-Service Restore Portal for Microsoft 365 environments empowers customers to restore their own emails, files and more – now with support for Microsoft Teams!

Now customers can choose their individual restore points and restore SharePoint and OneDrive folders.

Service providers can allow access to the restore portal via the Veeam Service Provider Console.

Thank you!