cristie
PROTECTING DATA SINCE 1969

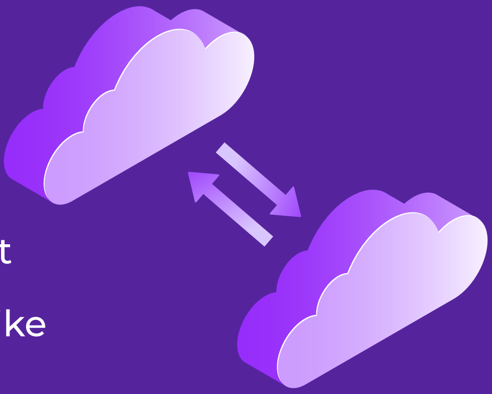
MSPs - Enhance your Multi-Tenant Cloud Services with **Cristie Cloud Protection**

Your Customers Need to Backup their SaaS Data - Because Most SaaS Providers Do Not

Cloud-To-Cloud Backup Is the Only Practical Option for SaaS Data Protection

A recent study revealed that 35% of SaaS users believe their SaaS vendors are responsible for data protection.

Unfortunately, that is not true.
SaaS vendors will protect data for an outage in a data centre environment, but they will not detect threats such as account takeovers and ransomware. Those kinds of attacks will look like the actions of a typical end user.



Crisite Cloud Protection provides vital protection for Microsoft Office 365, Dynamics 365, Google Workspace & Salesforce® with monthly Pay-Per-Use billing and no minimum terms.

Office 365 Google Workspace Microsoft Dynamics 365 salesforce

cristie

PROTECTING DATA SINCE 1969

Cloud users are confusing the availability of the service itself with the recoverability of the data that the service contains.

A recent study polling more than 1,000 IT professionals, backup administrators or business executives, revealed that 40% of respondents did not have third-party backup services to secure their Office 365 data.

Customers must backup their SaaS data. It is their responsibility, even if only from a compliance perspective.

In a recent study only 13% of the businesses surveyed understood that fact.

Contact the Cristie Data team to learn how **Cristie Cloud Protection** provides a SaaS backup solution that will empower your customers to keep business-critical emails, calendars, sites, groups, teams, projects, files, and conversations secure with unlimited automatic backups.

www.cristie.de/cloud-protection

info@cristie.de

cristie
PROTECTING DATA SINCE 1969

Cristie Cloud Protection
Key Features & Benefits

Accident-proof customer SLAs

Meet stringent SLAs with automatic backups up to four times a day and get the flexibility to customize your SLAs for RPO and RTO, instead of relying on Microsoft's default restoration and retention policy.

Customers own their data

Customers maintain full access and control over their backup data, not just what's in Recycle Bins. If backup files are needed for a longer term than the 15-30 days provided by Microsoft, they can be compressed and encrypt on the storage platform of your choice.

Recover on their own terms.

Customers can choose what to restore and where to restore it. Access a backup from weeks ago, or access files during any service disruption: perform in-place or out-of-place restores for granular objects or content, without overwriting valuable data since the last backup, or having to go through Microsoft Support.

Integrate existing security processes.

BYOK, BYOS and BYOA solutions keep your existing security practices operating.

cristie

PROTECTING DATA SINCE 1969

Cristie Cloud Protection

Key Features & Benefits

● Customer-Owned Encryption Keys

Azure KeyVault ensures unique keys for each tenant, owned and managed by each customer to prevent unauthorized access.

● Customer-Owned Data Storage

Data Residency provides hosted options through Azure or through any customer-owned cloud or server storage service.

● Customer-Owned Authentication

Single Sign-on with Office 365 Credentials and Azure AD applications ensures customers retain control of the authentication and authorization of AOS.

● Proactively Detect Ransomware

After the solution detects unusual activity, you receive detailed reports to shorten the investigation and flag the areas of questions. If necessary, you can restore all or specific OneDrive data.