

2023-24 DCIG TOP 5



MICROSOFT 365-SaaS-BACKUP-LÖSUNGEN FÜR MSPs ACRONIS CYBER PROTECT CLOUD TOP-5-LÖSUNGSPROFIL

Von DCIG Principal Data Protection Analyst, Jerome M Wendt

Microsoft 365-SaaS-Backup-Lösungen für MSPs— Acronis Cyber Protect Cloud TOP-5-Lösungsprofil



LÖSUNG

Acronis Cyber Protect Cloud

FIRMA

Acronis
1 Van de Graaff Drive #301
Burlington, MA 01803
(781) 782-9000
acronis.com

UNTERSCHIEDUNGSMERKMALE VON
ACRONIS CYBER PROTECT CLOUD

- Zusätzliche Levels an Cyberschutz für Microsoft Teams.
- Beinhaltet Anti-Ransomware-Software und Dienstleistungen zur Schwachstellenanalyse.
- Kann zur Speicherung von Backups zwischen über 50 Datenzentren auf der ganzen Welt wählen.
- Bietet seine Management-Schnittstelle in unterschiedlichen Sprachen an.
- Abonnementbasiertes, monatliches Lizenzmodell.

GEMEINSAMKEITEN ZWISCHEN ALLEN
MICROSOFT 365-SaaS-BACKUP-LÖSUNGEN
FÜR MSPs

- Schnell und erschwinglich.
- Kostenlose Probezeiten.
- Hohe Verfügbarkeit.
- Keine Installation, Setup oder Wartung.
- Datensicherung in Microsoft Exchange, OneDrive, SharePoint und Teams gehostet.

BEWERTETE LÖSUNGSMERKMALE:

- Anti-Ransomware/Cyber-Resilienz.
- Backup-Verwaltung und Fähigkeiten.
- Abrechnung, Konfiguration und Lizenzierung.
- Wiederherstellung (Recovery und Restores).
- Support.

Die häufig übersehenen 99,9% aller
US-Unternehmen

Technologieanbieter halten stets nach vertikalen Märkten Ausschau, die ihre Produkte bzw. Dienstleistungen benötigen. Sie können sogar Marktnischen mit relativ geringer Bedeutung bedienen, wenn dies gewinnbringend ist. Tatsache ist jedoch, dass die meisten Technologieanbieter notwendigerweise 99,9 Prozent aller US-Unternehmen weitestgehend ignorieren mussten.

Obwohl dies schockierend sein mag, umgehen Technologieanbieter Kleinunternehmen, die Mehrzahl von US-Unternehmen, aus einem einfachen Grund. Diese über 33 Millionen Kleinunternehmen beschäftigen laut US Small Business Administration (SBA) jeweils weniger als 500 Mitarbeiter.¹ Ihre geringe Größe stellt für Technologieanbieter eine taktische Herausforderung dar. Sie haben Schwierigkeiten, Produkte und Dienstleistungen, welche die Anforderungen von Kleinunternehmen erfüllen, kosteneffektiv zu vermarkten und zu liefern.

Cloud-basierte Software-as-a-Service (SaaS) Angebote haben dieses Paradigma geändert. Erhältlich als abonnementbasierte, On-Demand Services, hat ein jedes Kleinunternehmen nun Zugang zu hochkarätigen Technologien zu erschwinglichen Preisen. Dies hat zur Verfügbarkeit von Tausenden SaaS-Angeboten geführt, zwischen welchen Kleinunternehmen wählen können.

Aus all diesen verfügbaren SaaS-Anwendungen haben mehr als 11 Million Kleinunternehmen bereits Microsoft 365 gewählt.² Alle Kleinunternehmen, ungeachtet ihrer Vertikalmärkte, speichern Daten, tauschen Dateien aus, senden E-Mails und halten Video-Konferenzen ab. Microsoft 365 erfüllt diese Anforderungen mit Enterprise Software und Funktionalitäten zu einem Preis, der für Kleinunternehmen erschwinglich ist.

Verantwortungsbewusstsein für in Microsoft 365
gespeicherte Daten

Allerdings erkennen viele kleine Unternehmen, die Microsoft 365 schnell übernehmen, möglicherweise nicht, dass dies neue Herausforderungen für sie schafft. Sie besitzen immer noch die Daten und Benutzerinformationen, die sie in Microsoft 365 erstellen, und müssen diese verwalten. Diese Verantwortung erstreckt sich auf die Sicherung und Wiederherstellung dieser Daten sowie die Verwaltung der resultierenden Backups.

Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Customer	Customer	Customer
	Applications	Shared	Customer	Customer	Customer
	Network controls	Shared	Customer	Customer	Customer
	Operating system	Shared	Customer	Customer	Customer
Responsibility transfers to cloud provider	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Microsoft Customer Shared

Quelle: Microsoft³

Microsoft benutzt Begriffe wie Datenverfügbarkeit und -sicherung, wenn es um die Funktionalitäten von Microsoft 365 geht. Unternehmen sollten diese Hinweise jedoch in erster Linie im Kontext hoher Verfügbarkeit (HA) und Datensicherheit betrachten. Microsoft hostet zum Beispiel Microsoft 365 in seinen hoch verfügbaren Azure Datenzentren. Es sichert diese Datenzentren physisch und setzt Antivirus- und Firewall-Software ein, um die dort aufbewahrten Daten vor Angriffen zu schützen.

Microsoft 365-SaaS-Backup-Lösungen für MSPs— Acronis Cyber Protect Cloud TOP-5-Lösungsprofil

Es wurden Cloud-basierte Microsoft 365-SaaS Backup-Lösungen entwickelt, die speziell auf MSPs zugeschnitten sind.

Microsoft 365 bietet sogar einige beschränkte Datensicherungsfunktionen. Seine Dienstprogramme Gelöschte Objekte und Papierkorb bewahren kürzliche gelöschte Daten auf und ermöglichen die Wiederherstellung (Restores) der gelöschten E-Mails und Dateien.

Diese beiden Dienstprogramme schützen jedoch in Microsoft 365 gespeicherte Daten nicht ganzheitlich. Diese Verantwortung müssen Unternehmen ungeachtet ihrer Größe selbst übernehmen.

Angesichts dieser Herausforderungen haben sich die folgenden drei wesentlichen Trends abgezeichnet:

1. ***Es gibt jetzt Cloud-basierte Microsoft 365-SaaS-Backup-Lösungen.*** Diese Lösungen bieten Backup und Recovery speziell für die SaaS-basierte Version von Microsoft 365.
2. ***Managed Service Provider bzw. MSPs liefern Microsoft 365-SaaS-Backup-Lösungen und bieten das technische Knowhow, das Unternehmen so häufig suchen.*** Diese MSPs bieten die Marketingreichweite, die Anbieter von Microsoft 365-SaaS-Backup-Lösungen benötigen. Häufig bieten diese auch die von Unternehmen benötigte technische Beratung und anfängliche sowie kontinuierliche technische Unterstützung/Support.
3. ***Es wurden Microsoft 365-SaaS Backup-Lösungen entwickelt, die speziell auf MSPs zugeschnitten sind.*** Zusätzlich zur Bereitstellung umfassender Backup-Dienstleistungen für Microsoft 365 beinhalten diese Lösungen Funktionalitäten, welche die besonderen Anforderungen von MSPs erfüllen.

Diese Microsoft 365-SaaS-Backup-Lösungen müssen jedoch zwei Funktionalitäten besitzen, damit MSPs ihren Kunden diese Lösungen anbieten können.

Zum einen muss die Lösung mandantenfähig sein, damit sie diese effektiv verwalten können.

Zum anderen benutzen viele MSPs auch Fernüberwachung & -verwaltung (Remote Monitoring and Management - RMM) bzw. Professional Services Automation (PSA) Tools. Sie benutzen diese Tools zur Verwaltung der Software, die sie ihren Kunden anbieten. Idealerweise kann die Microsoft 365-SaaS-Backup-Lösung auch mit diesen RMM- und PSA-Tools integriert werden. MSPs benutzen diese Tools dann zur zentralen Verwaltung der Microsoft 365 Backups ihrer Kunden und stellen diesen die gelieferten Dienstleistungen in Rechnung.

Stand der Microsoft 365-SaaS-Backup-Lösungen für MSPs

MSPs benutzen und offerieren Microsoft 365-SaaS-Backup-Lösungen aus mehreren Gründen. Insbesondere können MSPs diese Angebote rasch abonnieren. MSPs können dann wiederum dieses Angebot ihren Kunden vorstellen. Nach Anmeldung des Kunden initiiert die Backup-Lösung dann Backups der Daten, die sich in Microsoft 365 befinden.

MSPs müssen an den Microsoft 365-SaaS-Backup-Lösungen keine Wartung durchführen. Die Dienstleister kümmern sich selbst um alle Back-of-House Verwaltungsaufgaben. Dazu gehören die laufenden Fixe, Patches und Updates der SaaS-Backup-Software. Viele dieser Provider bieten auch die Option zur Verwaltung des Cloud-Speichers, auf welchem sich die Backups befinden. Manche beinhalten als Teil ihres Abonnementpreises sogar unbegrenzten Cloud-Speicher.

Das Speichermanagement variiert jedoch nach Produkt. Manche leiten nur die Backups zum Speicher in der Cloud des Anbieters. Andere geben Unternehmen eine Auswahl von Speicherzielen, normalerweise Objektspeicher, inklusive der Nutzung des On-Premise-Speichers eines Unternehmens. In beiden Fällen müssen Unternehmen nach Konfiguration des Speichers sich nur selten über die Verwaltung der Speicherkapazität für Backups Gedanken machen.

Die Optionen, welche Provider von Microsoft 365-SaaS-Backup-Lösungen anbieten, variieren jedoch nach Produkt. Manche leiten nur die Backups zum Speicher in der Cloud des Anbieters. Andere geben MSPs eine Auswahl von Speicherzielen, normalerweise Objektspeicher. Diese Optionen können die Nutzung der On-Premise-Speicherlösung eines MSP beinhalten.

Microsoft 365-SaaS-Backup-Lösungen passen sich dynamisch an die zunehmende oder abnehmende Nutzung von Microsoft 365 durch den Kunden an. Dies trifft auf

Microsoft 365-SaaS-Backup-Lösungen für MSPs— Acronis Cyber Protect Cloud TOP-5-Lösungsprofil

Acronis bietet einen einheitlichen Preis pro Platz, welcher den Schutz von Daten in allen Microsoft 365-Anwendungen (Exchange, OneDrive, SharePoint und Teams) beinhaltet.

Rechner-, Speicher- und sogar Backup-Software-Benutzerlizenzen zu. Sollte zum Beispiel ein MSP mehr Lizenzen für die Microsoft 365-Backup-Lösung benötigen, fügt die Backup-Lösung automatisch weitere Lizenzen hinzu. Sollte die Anzahl der lizenzierten Microsoft 365-Nutzer abnehmen, kann die Backup-Lösung auch die Anzahl der Lizenzen automatisch verringern.

MSPs finden auch Anti-Ransomware, Cyber-Resilienz oder beide Funktionalitäten in vielen dieser Backup-Lösungen. Sie können das Speichern von Backups in unveränderlichen (immutable) Objektspeichern, die Warnung vor vermuteten Ransomware-Angriffen und die Quarantäne von infizierten Dateien in Backups unterstützen.

MSPs werden feststellen, dass alle analysierten SaaS-Backup-Lösungen Baseline-Datensicherungsfunktionen für Microsoft 365 bieten. Sie schützen Daten in den grundlegenden Microsoft 365-Anwendungen, die Unternehmen oft benutzen, wie Exchange, OneDrive und SharePoint.

Weiterhin schützen alle Microsoft 365-SaaS-Backup-Lösungen für MSPs jetzt universell Teams, eine der neueren Microsoft 365-Anwendungen. Im Vergleich dazu wurden im Jahr 2021 Microsoft Teams nur von 50 Prozent der von DCIG analysierten Microsoft 365-SaaS-Backup-Lösungen geschützt.

Alle analysierten Lösungen liefern die grundlegenden Merkmale, die MSPs benötigen, um schnell mit dem Schutz der Microsoft 365-Daten ihrer Kunden zu beginnen:

- **Schnell und erschwinglich.** Abonnementservices für Microsoft 365-SaaS-Backup-Lösungen kosten US\$2-6 pro Nutzer pro Monat mit einem Jahresvertrag. Nachdem ein MSP einen kundenseitigen Microsoft 365-Mandanten mit der SaaS Backup-Lösung verbindet, starten die Backups oft automatisch. Die meisten Lösungen planen standardmäßig anfängliche und wiederkehrende Microsoft 365-Backups mit minimaler bzw. keiner administrativen Intervention.
- **Keine Installation, Setup oder Wartung.** Anbieter hosten ihre Microsoft 365 Backup-Lösung entweder in einer Allzweck- oder einer zweckbestimmten Cloud. Die Lösungsanbieter fixen, patchen, warten und aktualisieren dann ihre Software als Teil ihrer SaaS-Backup-Lösung.
- **Hohe Verfügbarkeit.** Jede SaaS-Backup-Lösung passt sich an Microsoft 365 auf eine wichtige Art und Weise an: sie wird in einer hoch verfügbaren Cloud gehostet. Die Clouds, in welcher jedes Produkt gehostet wird, sind unterschiedlich, obwohl die meisten Provider, die Microsoft 365-SaaS-Backup-Lösungen anbieten, diese in einer zweckbestimmten Cloud hosten. Unabhängig vom Anbieter beinhalten diese häufig ein Service-Level-Agreement (SLA) von 99,5% oder höher.
- **Kostenlose Probezeiten.** MSP-Kunden können während einer kostenlosen Probezeit die Backup- und Wiederherstellungsfunktionen einer Lösung testen. Provider begrenzen die Probezeit normalerweise auf ca. 30 Tage, wobei die Länge der Probezeit eines jeden Providers variiert. Die Probezeit kann Zugriff auf alle Funktionen für bestimmte Nutzer, Zugriff auf manche Funktionen für alle Nutzer oder eine Kombination hiervon beinhalten.

Acronis Cyber Protect Cloud

Bei Abschluss der Prüfung von 14 verfügbaren Microsoft 365-SaaS-Backup-Lösungen für MSPs seitens DCIG, klassifizierte DCIG Acronis Cyber Protect Cloud als eine TOP-5-Lösung. Acronis konzentriert sich hauptsächlich auf die Bereitstellung von Cyber Protect Cloud an Service Provider jeglicher Größe auf der ganzen Welt. Zusätzlich zum Microsoft 365 Backup können MSPs diese Plattform nutzen für:

- Backup und Recovery.
- Disaster Recovery.
- Compliance.
- Cybersecurity (EPP/EDR).
- Endpoint-Management-Funktionalitäten wie Remote Management und Patch-Management.

Acronis benutzt ein abonnementbasiertes, monatliches Lizenzmodell ohne langfristige Verpflichtungen. Es bietet einen einheitlichen Preis pro Platz, welcher den Schutz von Daten in allen Microsoft 365-Anwendungen (Exchange, OneDrive, SharePoint und Teams) beinhaltet.

Microsoft 365-SaaS-Backup-Lösungen für MSPs— Acronis Cyber Protect Cloud TOP-5-Lösungsprofil

Acronis bietet signaturbasierten Schutz und nutzt Bilderkennungsalgorithmen und Machine Learning zur Validierung von Content und Erkennung von böartigen Inhalten in Exchange-Nachrichten.

Acronis hostet Cyber Protect Cloud in mehr als 50 eigenen Datenzentren auf allen Kontinenten weltweit (mit Ausnahme von Antarktika). Jedes dieser Datenzentren hat Direktverbindungen zu Microsoft-Datenzentren, um schnelle Upload- und Download-Geschwindigkeiten zu ermöglichen. MSPs haben im Falle von Datenhoheit auch die Möglichkeit zur Weiterleitung von Backups zu ihrem gewählten Acronis Datenzentrum.

Acronis führt standardmäßig Microsoft 365-Backups sechsmal pro Tag durch. Es speichert diese Daten auf seinem Cloud-Speicher, der unbegrenzte Kapazität zu einem Festpreis beinhaltet. Weiterhin können MSPs Acronis so konfigurieren, dass es in Abhängigkeit von den speziellen Anforderungen seiner Kunden Backups häufiger oder weniger häufig durchführt. Acronis bietet sein Interface auch in zahlreichen Sprachen an. Diese Benutzerschnittstelle ermöglicht es Diensteanbietern mit globaler Geschäftstätigkeit, Personen einzustellen, die Cyber Protect Cloud in ihrer Muttersprache verwalten können.

Weiterhin bietet Acronis Cyber Protect Cloud die folgenden drei Merkmale, welche es weiter von anderen Microsoft 365-SaaS-Backup-Lösungen für MSPs abhebt.

- 1. Anti-Ransomware-Software und Schwachstellenanalyse-Services sind Teil seines Microsoft 365-Backup-Angebotes.** Jeder Acronis MSP Partner und dessen Kunden, die Acronis Cyber Protect Cloud benutzen, erhalten Zugriff auf diese Software und Services. Sie können diese Software und Services ohne zusätzliche Gebühren in beliebig vielen Workloads nutzen.
- 2. Cybersecurity-Software beinhaltet erweiterte E-Mail-Schutzfunktionen.** E-Mail ist die gängigste Art, mittels welcher Ransomware in Unternehmen eindringt. Um dieser Bedrohung entgegenzuwirken, hat Acronis eine Partnerschaft mit Perception Point geschlossen und deren Cybersecurity-Software in sein Microsoft 365-Backup-Angebot integriert. Obwohl Microsoft selbst E-Mails auf Malware und Ransomware analysiert, geht diese Software deutlich weiter. Wie Microsoft scannt auch sie E-Mails in Echtzeit, während diese den Exchange-Server durchlaufen. Acronis bietet jedoch signaturbasierten Schutz und nutzt Bilderkennungsalgorithmen und Machine Learning zur Validierung von Content und Erkennung von böartigen Inhalten in Nachrichten.
- 3. Zusätzliche Cyberschutz-Levels für Microsoft Teams verfügbar.** Die Popularität von Teams hat dieses zu einem neuen Ziel für Hacker zum Einschleusen ihrer Malware und Ransomware in Unternehmen gemacht. Zum Schutz von Teams bietet Acronis einen priorisierten Patching Service. Acronis Cyber Protect Cloud schützt auch Daten und Benutzeraktivität in Teams mittels:
 - Blockieren von Code-Injection-Angriffen.
 - Blockieren von Malware Hooks, die Streaming-Inhalte zu stehlen versuchen.
 - Verhindern von Anfragen zu böartigen Webseiten.
 - Verhindern von Session-ID-Diebstahl. ■

Quellenangaben

1. Frequently Asked Questions About Small Business, März 2023 (sba.gov). Referenziert 01.07.2023.
2. <https://www.microsoft.com/en-us/microsoft-365/blog/2023/05/01/microsoft-365-innovations-across-ai-payments-and-collaboration-tools-help-small-and-medium-businesses-grow/>. Referenziert 01.07.2023.
3. <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>. Referenziert 02.05.2023.

Über DCIG

Die Data Center Intelligence Group (DCIG) befähigt die IT-Branche mit umsetzbaren Analysen. DCIG-Analysten bieten informierte unabhängige Analysen unterschiedlicher Cloud-, Datensicherung- und Datenspeichertechnologien. DCIG entwickelt eigenständig lizenzierten Content in Form der DCIG TOP-5-Berichts- und Lösungsprofile. Bitte besuchen Sie www.dcig.com.



DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552

dcig.com

© 2023 DCIG, LLC. Alle Rechte vorbehalten. Andere Marken in diesem Bericht sind Markenzeichen ihrer jeweiligen Eigentümer. Dieser DCIG-Bericht ist ein Produkt von DCIG, LLC. Alle anderen Marken oder Produkte sind Markenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer und sind als solche zu behandeln. Produktinformationen wurden sowohl von öffentlich zugänglichen Quellen als auch anbieterspezifischen Ressourcen erstellt. Obwohl DCIG versucht zu prüfen, dass diese Produktinformationen korrekt und vollständig sind, kann sich der Support für Funktionen ändern und ist Auslegungssache. Alle in diesem Bericht dargestellten Funktionen repräsentieren die Auffassung von DCIG. DCIG ist nicht haftbar für auftretende Fehler.

Lizenziert für Acronis mit unbefristeten, uneingeschränkten, globalen Vertriebsrechten.

Juli 2023 5