E-Book

datto

SaaS Protection Leitfaden für Käufer

Einführung

Die Akzeptanz von SaaS-Anwendungen hat mit dem Anstieg von Remote-Arbeit aufgrund der globalen Gesundheitspandemie stark zugenommen. Diese Tools sind in der Remote-Arbeitswelt von heute unverzichtbar geworden. Auch bevor die Arbeit von zu Hause aus für viele zur Norm wurde, liegen die Vorteile des einfachen Zugriffs auf Dokumente von jedem Gerät aus ebenso wie die der verbesserten Zusammenarbeit auf der Hand.

Leider glauben viele Unternehmen immer noch, dass durch diese Tools ein Backup überflüssig ist. Das ist schlicht nicht wahr. Backup ist für Daten in SaaS-Apps genauso wichtig wie für Daten, die vor Ort gehostet werden.

In diesem E-Book lernen Sie einige weit verbreitete Mythen und irrige Annahmen zu SaaS kennen, wie Sie mit Kunden über SaaS-Datenverlust und Ausfallzeiten sprechen, worauf Sie bei der Auswahl einer SaaS-Sicherungslösung achten müssen und wie Sie SaaS-Backup zum Aufbau von Margen und zum Wachstum Ihres Unternehmens einsetzen können.

Das könnte Sie auch interessieren:

Infografik

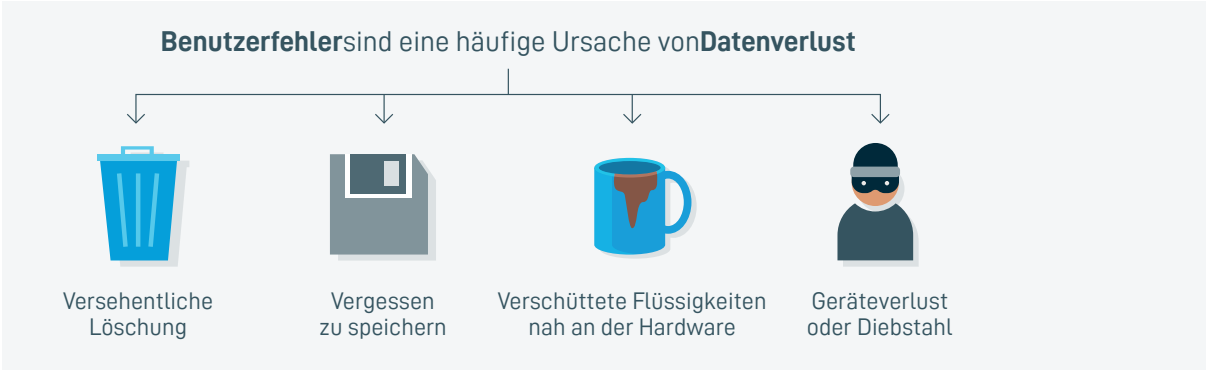
Menschliches Versagen kommt vor: So kann SaaS Backup helfen

ERFAHREN SIE MEHR

Häufige Mythen und irrige Annahmen über SaaS

SaaS-Anwendungen erfordern kein Backup

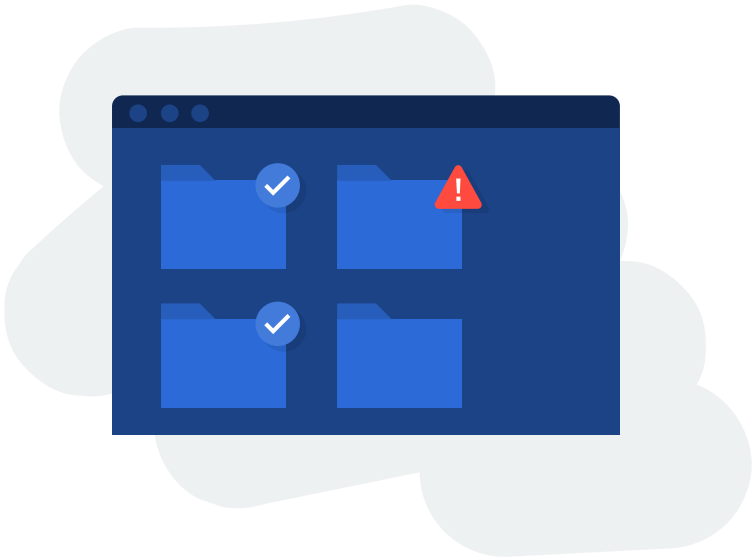
Während SaaS-Anwendungen über eine integrierte Redundanz verfügen, die vor Datenverlust auf ihren Cloud-Servern schützt, schützt dies nicht vor Benutzerfehlern, versehentlichem und böswilligem Löschen oder Ransomware-Angriffen. Während das versehentliche Löschen von Dateien in SaaS-Apps bei weitem die häufigste Form des Datenverlusts ist, kann Ransomware die schädlichste sein. Dies liegt daran, dass Ransomware so konzipiert ist, dass sie sich über Netzwerke und in SaaS-Anwendungen verteilt und Auswirkungen auf viele Benutzer hat.



Ransomware ist nicht nur ein Problem vor Ort. Sie kann sich in SaaS-Anwendungen verbreiten und sie tut es, insbesondere in Microsoft 365. Unternehmen benötigen eine Möglichkeit, Dateien, Ordner, Einstellungen und Berechtigungen im Falle eines Angriffs schnell zurückzusetzen.

File Sync ist ein Ersatz für Backup

File Sync Tools wie Microsoft OneDrive oder Google Drive erstellen zwar eine zweite Kopie von Dateien und Ordnern, sind jedoch kein Ersatz für Backup. File Sync kopiert automatisch Änderungen in synchronisierte Dateien. Wenn also eine Datei oder ein Ordner mit Ransomware infiziert ist, wird die Malware automatisch in alle synchronisierten Versionen dieser Datei kopiert.



File Sync verfügt nicht über die Wiederherstellungsfunktionen einer Backup-Lösung und kann darüber hinaus tatsächlich Ransomware in SaaS-Anwendungen einführen.

File Sync Services bieten zwar einige Wiederherstellungsfunktionen über die Versionierung, sie entsprechen jedoch nicht einer echten SaaS-Backup-Lösung. Dies sind die Gründe:

- **Versionen sind keine unveränderlichen Wiederherstellungspunkte.** Wenn also eine Datei gelöscht wird, werden auch ältere Versionen der Datei gelöscht.
- **Die Versionierung ermöglicht keine zentralisierte Verwaltung von Benutzerdaten.** Mit anderen Worten, Sie haben keine Kontrolle über Backup und Wiederherstellung – das bleibt in den Händen der Endbenutzer.
- **Bei der Versionierung werden keine Wiederherstellungspunkte für Dateien, Ordner, Einstellungen und Benutzer beibehalten.** Wenn Sie nur ein paar Dateien wiederherstellen müssen, ist das keine große Sache. Große Wiederherstellungen sind jedoch ein zeitaufwändiger manueller Vorgang.

File Sync verfügt nicht über die Wiederherstellungsfunktionen einer Backup-Lösung, sondern kann darüber hinaus tatsächlich Ransomware in SaaS-Anwendungen einführen. File Sync und Backup sind keine wettbewerbsfähigen Lösungen, sondern können und sollten nebeneinander verwendet werden. Denken Sie daran: Die Synchronisierung und Freigabe von Dateien dient der Produktivität und das Backup dem Datenschutz und der schnellen Wiederherstellung.

SaaS-Anwendungen sind immer verfügbar

Während SaaS-Apps sehr zuverlässig sind, kann es dennoch zu Ausfällen kommen. Allein im Oktober 2020 hatte Microsoft 365 drei bedeutende Ausfälle, von denen Unternehmen weltweit betroffen waren. Im vergangenen Jahr waren fast eine Milliarde Nutzer von Google Mail, G Suite und YouTube von einem massiven Google-Ausfall betroffen.

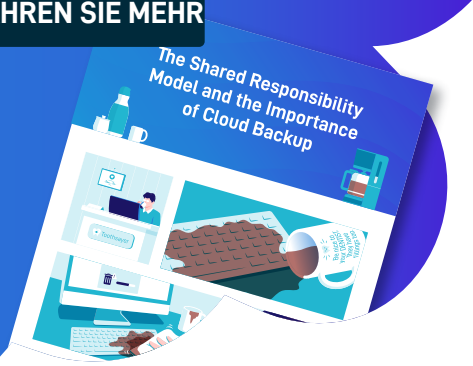
Ausfälle und langsame Wiederherstellungszeiten sind mehr als eine Unannehmlichkeit. Wenn Unternehmen nicht auf wichtige Geschäftsdaten zugreifen können, sinkt die Produktivität und der Umsatz wird beeinträchtigt. Das Erstellen von Backups, die unabhängig von den Cloud-Servern eines SaaS-Anbieters sind, ist die einzige Möglichkeit, im Falle eines Ausfalls den Zugriff auf wichtige Dateien sicherzustellen.

Das könnte Sie auch interessieren:

Infografik

Das Modell der gemeinsamen Verantwortung und die Bedeutung von Cloud-Backup

ERFAHREN SIE MEHR



Microsoft und Google sind für das Backup verantwortlich

SaaS-Anbieter stellen mithilfe von integrierter Redundanz und anderen Hochverfügbarkeitsmaßnahmen sicher, dass sie Ihre Cloud-Daten nicht verlieren. Sie übernehmen jedoch keine Verantwortung für die Wiederherstellung von Daten, wenn Sie diese verlieren. Microsoft nennt dies das Modell der gemeinsamen Verantwortung für den Datenschutz. Aus diesem Grund empfiehlt Microsoft in seiner Benutzervereinbarung SaaS-Backups von Drittanbietern. Im Modell der gemeinsamen Verantwortung:

Geschäftsverantwortung:
Sicherheit in der Cloud

- *Daten-Backup*
- *Geräte (Mobilgeräte und PCs)*
- *Konten und Identifikatoren*

Verantwortung des Anbieters:
Sicherheit der Cloud

- *Physische Infrastruktur*
- *Apps und Betriebssysteme*
- *Netzwerkkontrollen*

Bei dem Modell der gemeinsamen Verantwortung liegt die Verantwortung für den Datenschutz voll und ganz bei Unternehmen, die auf SaaS-Dienste angewiesen sind. SaaS-Anbieter sind dafür verantwortlich, dass ihre Infrastruktur funktioniert, aber Unternehmen sind für die Aufbewahrung und Sicherheit ihrer Daten verantwortlich.

Bewertung von SaaS-Backup-Lösungen

Es gibt eine Vielzahl von SaaS-Backup-Lösungen zu wettbewerbsfähigen Preisen auf dem heutigen Markt. Es gibt jedoch eine Ungleichheit in Bezug darauf, was genau diese Produkte schützen. Wenn Sie also Produkte bewerten, kann dies ein guter Ausgangspunkt sein.

Das könnte Sie auch interessieren:

Umfassender Schutz

Einige SaaS-Sicherungslösungen schützen nur E-Mails, Dateien und Ordner. Es gibt jedoch heutzutage Lösungen, die eine umfassendere Abdeckung bieten. Suchen Sie bei der Auswahl eines SaaS-Backupprodukts nach Lösungen, die Schutz für Kontakte, freigegebene Laufwerke, Tools für die Zusammenarbeit und den Chat sowie Kalender bieten. SaaS-Schutz-Lösungen, die diese Art der Abdeckung bieten, sind weitaus effektiver bei der Aufrechterhaltung der Geschäftskontinuität als weniger robuste Angebote (mehr dazu weiter unten).

RPO/RTO

Das Wiederherstellungspunktziel (RPO) und das Wiederherstellungszeitziel (RTO) sind ebenfalls entscheidende Aspekte. Diese Metriken beziehen sich jeweils auf den Wiederherstellungszeitpunkt und darauf, wie schnell Sie eine Wiederherstellung durchführen können. Wenn es um SaaS-Backups geht, werden diese hauptsächlich von der Häufigkeit der Backups und dem, was speziell geschützt wird, bestimmt. Lösungen, die häufige Backups anbieten, beziehen sich auf RPO, da sie es Ihnen ermöglichen, eine Wiederherstellung auf einen kürzlich zurückliegenden Zeitpunkt vorzunehmen, wodurch Datenverluste minimiert werden. Wie oben erwähnt, werden hierdurch diese Wiederherstellungen schneller und einfacher ausgeführt, da der manuelle Aufwand für die Ausführung von Wiederherstellungen verringert wird. Außerdem ermöglichen sie Benutzern den Zugriff auf Daten im Falle eines SaaS-Ausfalls.

Benutzerfreundlichkeit/Verwaltung

Die Benutzerfreundlichkeit ist für MSPs von entscheidender Bedeutung. Durch die Steigerung der Effizienz können die Margen bei den erbrachten Dienstleistungen erhöht werden. Daher sollte es als unerlässlich angesehen werden, ein Produkt zu finden, das einfach bereitzustellen und zu verwalten ist. Suchen Sie nach SaaS-Backup-Produkten, die speziell für MSPs entwickelt wurden. Dies kann optimiertes Onboarding, native Berichtsfunktionen, intuitive Sitzverwaltung und flexible Aufbewahrungsrichtlinien bedeuten. Ziehen Sie eine Partnerschaft mit Anbietern in Betracht, die Programme anbieten, die nicht für den Weiterverkauf vorgesehen sind, ebenso wie verkaufsbezogene Rabatte und technischen Support rund um die Uhr 365 Tage. Schließlich verbessern Produkte, die in andere Tools integriert werden, auch Ihre Fähigkeit, SaaS-Backup-Services effizient bereitzustellen.

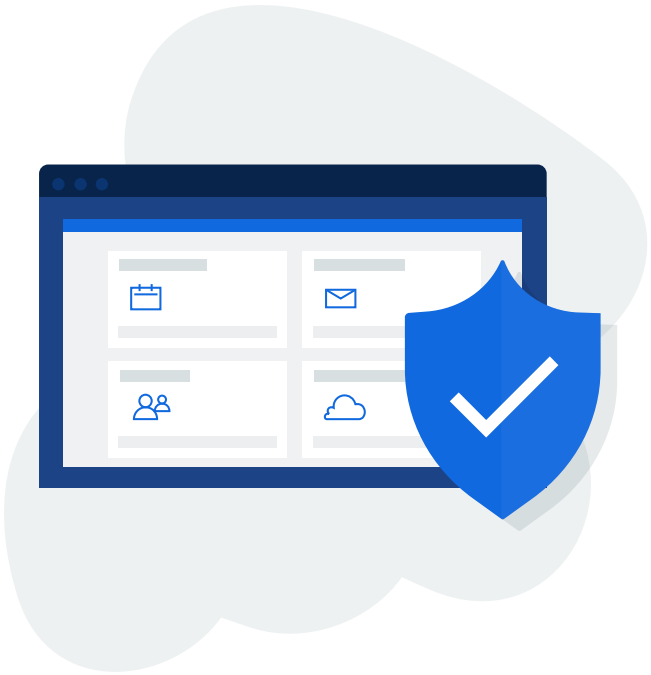
Lösungen, die ein automatisiertes Aufbewahrungsmanagement ermöglichen, um Compliance-Standards zu erfüllen, können den Bedarf an manuellen Eingriffen verringern

Sicherheit/Compliance

Viele MSPs betreuen Kunden in Branchen mit erheblichen Sicherheits- und Compliance-Anforderungen. Daher ist die Auswahl einer SaaS-Schutzlösung, die diese Anforderungen erfüllt, unerlässlich. Suchen Sie nach Produkten, die Daten gemäß den Berichtsstandards der Service Organization Control (SOC 1 / SSAE 16 und SOC 2 Typ II) sichern und die HIPAA- und GDPR-Konformitätsanforderungen der Kunden erfüllen. Lösungen, die ein automatisiertes Aufbewahrungsmanagement ermöglichen, um Compliance-Standards zu erfüllen, können den Bedarf an manuellen Eingriffen verringern. Sie optimieren das Management und stellen sicher, dass Kundendaten für die richtige Zeitdauer gespeichert werden.

Geschäftswachstum

Keine Diskussion über Produktbewertung ist für MSPs vollständig, ohne die Rentabilität zu berücksichtigen. Suchen Sie nach Produkten mit den erforderlichen Eigenschaften und Funktionen zu einem Preis, mit dem Sie Margen für Ihre Services aufbauen können. Ziehen Sie Produkte in Betracht, die Preisvorteile für MSPs bieten, z. B. verkaufsabhängige Rabatte und flexible Lizenzen, für die Sie das bezahlen, was Sie verwenden. Wie oben erwähnt, können Produkte, die die Effizienz steigern, auch die Marge erhöhen und den Umsatz steigern, da sie weniger manuelle Eingriffe erfordern. Möglicherweise möchten Sie den SaaS-Schutz auch zusätzlich zu den bereits bereitgestellten SaaS-Diensten bündeln. Dies hat sich für einige MSPs als effektiv erwiesen. Dies ist nicht unbedingt Teil des Produktbewertungsprozesses, aber es ist erwähnenswert, wenn über das Geschäftswachstum gesprochen wird.



Datto SaaS Protection:

Datto SaaS Protection ist eine Cloud-zu-Cloud-Backup-Lösung, die eine umfassende Sicherung und Wiederherstellung kritischer Cloud-Daten in Microsoft 365 und Google Workspace bietet. Sie wurde speziell für MSPs entwickelt, um die SaaS-Daten ihrer Kunden effizient zu schützen und die Aufbewahrung, Lizenzen und Kosten von Kundendaten zu verwalten.

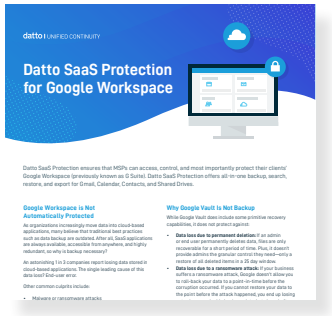
SaaS Protection schützt vor dauerhaftem Datenverlust und ermöglicht es MSPs, mit 3-mal täglichen zeitpunktgenauen Backups die Daten von Kunden nach einem Ransomware-Angriff problemlos wiederherzustellen. Backups werden sicher in der Datto Cloud gespeichert, und Dateien, Ordner, Einstellungen und Berechtigungen für schnelle Wiederherstellungen sind intakt, unabhängig davon, ob Sie ein einzelnes Element oder ein gesamtes Benutzerkonto wiederherstellen müssen.

SaaS Protection bietet Backup, Suche, Wiederherstellung und Export für:

Microsoft 365	Google Workspace
• Exchange	• Gmail
• Tasks	• Google Drive
• OneDrive	• Kalender
• SharePoint	• Kontakte
• Teams	• Gemeinsam genutzte Laufwerke

Wie Sie wissen, geht es bei der Bereitstellung profitabler Managed Services darum, die Effizienz zu steigern und die Rendite der Services zu maximieren. Datto SaaS Protection verbessert die MSP-Effizienz durch optimiertes Onboarding, das neue Kunden schnell einsatzbereit macht. Mit einer einzigen Ansicht erhalten Sie einen vollständigen Überblick über Kunden-Backups und können so die Effizienz weiter steigern.

Das könnte Sie auch interessieren:



Datto SaaS-Schutz für Google Workspace →

Datto SaaS-Schutz für Microsoft 365 →

Datto SaaS Protection bietet außerdem:

- **Einfache Preisgestaltung pro Lizenz:** Stellen Sie Lizenzen für Endkunden bereit und stellen Sie sie nach Bedarf erneut bereit.
- **Aggregierte, volumenbasierte Rabatte:** Die Rabatte basieren auf den Gesamtlizenzen, die für alle Ihre Kunden verkauft wurden.
- **Flexible Abonnementoptionen:** Wählen Sie die beste Lösung für jeden Kunden mit Standard-Monatsverträgen oder ermäßigten längerfristigen Verträgen.
- **Chancen zum Margenaufbau:** Bauen Sie Margen auf und fügen Sie mehrschichtigen Schutz für Ihre Microsoft 365-Kunden hinzu, indem Sie Microsoft 365 und Datto SaaS Protection bündeln.
- **Unbegrenztes NFR-Programm:** Testen Sie das Datto SaaS Protection-Produkt mit Ihren Kunden und fügen Sie mit unserem optimierten Onboarding-Prozess innerhalb von Minuten einen neuen NFR-Kunden hinzu.
- **Marketing- und Vertriebskampagnen von SaaS Protection:** Starten Sie vorgefertigte SaaS Protection-Kampagnen, greifen Sie auf eine Bibliothek mit Co-Branding-Inhalten zu und verwalten Sie Ihre Leads vom potenziellen Kunden bis zum Verkauf.

Datto SaaS-Schutz nach Zahlen:

Milliarden von Backups

Zehntausende von Wiederherstellungen

Hunderttausende von Teams geschützt