Microsoft 365とGoogle Workspaceにバックアップが必要な9つの理由

Acronis

Microsoft 365とGoogle Workspaceのデータを保護するのは、ユーザーの責任

Microsoft 365やGoogle Workspaceのマーケットシェアは拡大し続けていますが、これらのプラットフォームはすぐに使える万能のバックアップとデータ復元ソリューションは含まれないことに注意する必要があります。

ランサムウェアをはじめとするサイバー攻撃が頻発し被害が甚大になるにつれ、MSP（マネージドサービスプロバイダー）と企業はどちらも、システムの計画外停止や壊滅的なデータ損失という現実的なリスクに直面しています。

Microsoft 365やGoogle Workspaceは、思われているよりも脆弱です。これらの便利なクラウドツールには、以下9つの理由の通り優れたバックアップとデータ保護ソリューションが必要となります。

1

偶発的なデータ削除

IT運用管理者のみならず一版のユーザーでも、OneDriveデータ、OneDriveドキュメント、添付ファイルのサイズが大きいEメール等を削除してしまうことがあります。特に、古いデータやもう利用していないデータに起こりがちです。信頼できるバックアップソリューションがなければ操作ミスを復旧することはできず、将来そのデータが必要になった時に深刻な問題になります。

2

重複したファイルの管理ミス

大半の企業は、通常のコラボレーションプロセスの一環で、大量の重複ファイルを作成しています。そのため、古いバージョンや複製したバージョンを削除しようとして、誤って別のファイルを削除してしまうことが起こります。

3

悪意ある操作

まれに不満を抱えた従業員が重要なファイルを破壊したり削除することがあり、それが発見された時には手遅れで復元できない場合があります。

4

フィッシング攻撃とランサムウェア攻撃

サイバー犯罪は巧妙化しており、ビジネスのEメールを模造したフィッシングで、疑うことを知らない従業員をだまします。1回クリックしただけで、データを抜き出されたり、ランサムウェア攻撃の流れでデータを人質に取られてしまいます。

5

ストレージおよび/またはEメールの保持の制約

従業員が退職する際、IT管理者はMicrosoft 365とGoogle Workspaceのデータをバックアップし、そのライセンスを他者に再利用します。しかし、バックアップが常に実行されるとは限らず、多くのデータが失われるきっかけになります。

6

サードパーティアプリケーションの不正な同意許可による攻撃

サードパーティアプリケーションが原因となり、不正な同意許可に基づく攻撃を受け、重要データが窃取される可能性があります。

7

デバイスの紛失や盗難

中堅・中小企業を含む多くの企業では、従業員が個人所有のデバイスを業務用に使用すること（BYOD）を許可しています。コストの削減や従業員の利便性は増しますが、一方デバイスの紛失や盗難に遭うと、取り扱うデータに問題が生じます。

8

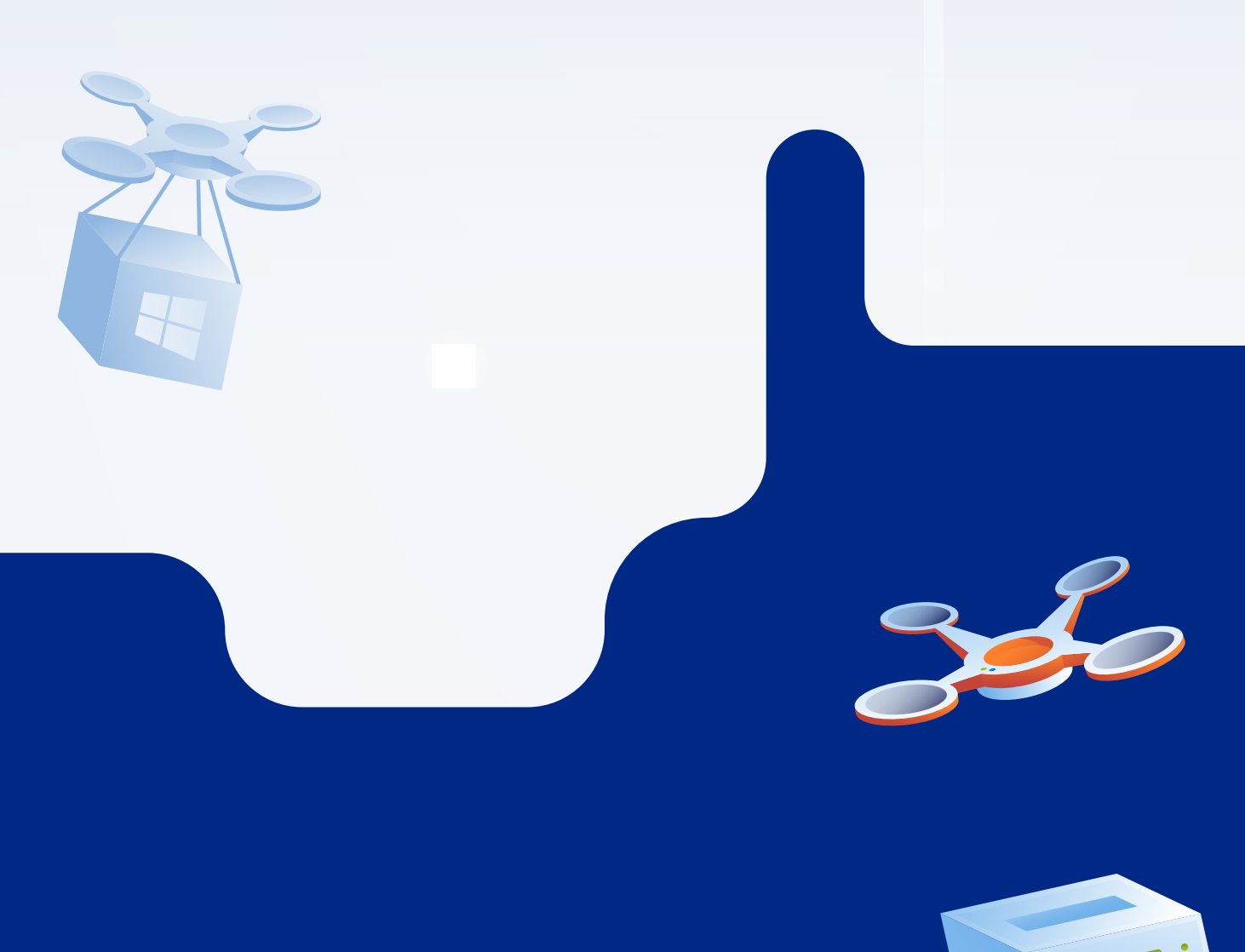
従業員によるデータの上書き

事故は防げません。従業員が重要なデータを上書きするような事故が起こると、基幹業務データを復元する方法がない場合など、企業にとって深刻な問題に発展する可能性があります。

9

限定的バックアップ機能

Microsoft OutlookやGmailや、Microsoft 365とGoogle Workspaceにかかわるデータをバックアップする方法はいくつかありますが、そのプロセスは未だに時間と手間がかかり、多忙なMSPやITプロフェッショナルにとって理想的ではありません。



アクロニスは、Microsoft 365とGoogle Workspaceを簡単に高速で効果的なバックアップとデータ保護を実現するソリューションを提供します。

最新	完全	高速	安全	簡単
Microsoft 365、Google Workspaceなどのクラウドベースのプラットフォームを保護	Microsoft 365、Exchange、Windowsを含む20種類以上のプラットフォームを保護	競合製品よりも約2倍の速さでバックアップ	保存されたデータだけでなく、送信中のデータも暗号化	直感的なダッシュボードで3回クリックするだけでバックアップと管理

アクロニスでMicrosoft 365とGoogle Workspaceの保護をしましょう

acronis.com