



Why standard **SaaS cybersecurity** won't keep your data safe



When software as a service, or SaaS, debuted in earnest sometime in the early 2000s, it seemed to be a cure-all for business technology. Everything your business needed was available online with no software installation or maintenance necessary. Someone else took care of everything for you with SaaS, including cybersecurity.

That was the idea, anyway. SaaS really was a revolution. Huge vendors sprung to life on the back of SaaS technology and the idea that businesses didn't like **messing with installing software** from physical media such as disks. The precursor to SaaS was something called ESD, electronic software distribution (or delivery, depending on the source). But ESD has since become merely the delivery component of SaaS.

The idea behind SaaS was that it would do more than just act as an online delivery service for applications. The last "S" stands for service, and that letter has always been important. SaaS vendors promised to take care of applications for users by managing updates and backing up data—and those value propositions have made the SaaS model very popular. One study shows that organizations **use on average 130 SaaS apps**, a number that might even be a bit conservative.

But SaaS hasn't turned out to be the all-inclusive service some IT professionals might have thought they were buying when the concept was fresher. The same SaaS survey cited above notes that 81% of IT pros say that they are responsible for protecting sensitive data stored in SaaS apps. And they're right, which means the other 19% should beware. Because as great as online apps are, SaaS cybersecurity weaknesses make them risky.

So, despite all the power and convenience of SaaS, your business still needs to oversee and protect your SaaS applications and data. One major SaaS suite in particular, Microsoft 365, demonstrates why.



Microsoft 365 is a test case for bolstering SaaS cybersecurity

There was a time when just about every new employee at a business sat down to a laptop on the first day of work and opened a copy of Microsoft Word stored locally on a computer. Today, that happens less frequently. Microsoft 365 is the company's SaaS office suite and has gained traction since its introduction as Office 365 in 2011, when it began replacing traditional software applications.

Back in 2011, about 200,000 beta testers were putting the product through its paces. Today, more than 3 million **companies worldwide use Microsoft 365**, including 1.2 million in the US. The vast majority of them, 73%, are small, with fewer than 50 employees. More than a third of companies that use the service worldwide have 10 or fewer employees. To be clear, Microsoft 365 is a fantastic option for many small businesses that don't want to deal with traditional software.

But it's not perfect. In fact, Microsoft 365 has flaws that even the vendor itself is aware of. And they're not minor. Businesses that use Microsoft 365 **regularly struggle with security**, according to a recent study. A staggering 92% of respondents whose organizations use Microsoft 365 said they suffered phishing attacks; 86% said the phishing incidents had a negative impact on their businesses. More than half reported suffering financial losses from customer churn after data breaches. Almost half of the incidents that respondents suffered led to employees leaving the company.

The consequences of cyberattacks are familiar to most business owners, but many likely thought they could avoid them by using Microsoft 365. The problem is that Microsoft's SaaS offering is a productivity suite and not a security product. The company knows it, and business owners should, too.

Why Microsoft 365 alone can't ensure cybersecurity

One not-so-subtle hint about the limitations of Microsoft 365 SaaS cybersecurity **comes from the company itself**, right in the user agreement for the service:



We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

Yes, Microsoft directly recommends using third-party, or non-Microsoft, services to guarantee data availability. Why? There are several reasons. The primary one is that Microsoft 365 has known issues. The service simply isn't built to provide cybersecurity and guarantee data availability.

For instance, there are a few basic **cybersecurity risks Microsoft 365 doesn't address**. One is simple human error. Emails or other data that users unintentionally (or even intentionally) delete can disappear forever.

SharePoint, for instance, **permanently erases deleted data** after 93 days. Furthermore, Microsoft 365 might not be able to recover data encrypted or corrupted in a cyberattack. That data could end up being unusable.

And then there is downtime caused by service outages. If Microsoft 365 goes down and a business doesn't have some other backup option in place, the business simply won't be able to access data until service is restored. The duration of downtime could be hours or longer. A cyberattack in December 2022 caused weeks-long outages for some users. A failed update by Microsoft in June 2023 caused hours of downtime.

Rogue apps have found their way into Microsoft 365

So, by the company's own admission, third-party backup is critical for businesses using Microsoft 365. But there are other cybersecurity concerns, as well. One is malicious apps that have found their way into Microsoft 365. Essentially, malware developers figured out how to **trick Microsoft into verifying malicious apps** and released those apps into Microsoft download libraries.

The apps weren't just available; Microsoft also **marked them as safe** for download and use. The apps then launched constant phishing attacks on Microsoft 365 users. Impersonating legitimate companies, malware developers infected users with apps that could:

- Read mail.
- Maintain access to data users allowed the apps to access.
- Read mailbox settings.
- Sign in and read users' profiles.
- Send mail as a user.
- Read calendars.
- Read online meetings.

Microsoft has shut down many of the malicious apps, but the company acknowledges that **the problem continues**. Plus, Microsoft essentially killed off one of its own security applications because it **couldn't keep up with sophisticated cyberattacks**. The app-based cyberattacks demonstrate how important enhanced security is for Microsoft 365.

Email in Microsoft's SaaS suite also has some security issues. Microsoft does offer a secure email gateway, but it's not as robust as what a third party can offer. More than half of cybersecurity leaders whose businesses use Microsoft 365 said **too many phishing attacks** have gotten through their gateways. Nearly all the leaders, 99%, said they were stressed about email security.

Buying a basic Microsoft 365 license gives your business access to a suite that offers fantastic functionality for office productivity. It's the online extension of far and away the most popular productivity suite ever produced. But Microsoft 365—even according to Microsoft—doesn't provide comprehensive backup or cybersecurity. Not even close.

Because SaaS cybersecurity isn't enough, users need to take a holistic approach to security

Microsoft 365 is just one example of a set of SaaS applications that delivers many valuable services...but doesn't cover all the security functionality your business needs. Many others are similar, especially in terms of **not offering the backup and data protection** customers might think they're getting with an online application service.

SaaS users who want to protect their data and make sure it's available need help from a third party. Fortunately, a provider of cloud services can provide cybersecurity and backup offerings that fill the gaps left open in most SaaS applications. Some cloud providers sell licenses to services such as Microsoft 365 that offer the provider's greatly enhanced security and backup capabilities as part of the total license package.

When your business works with a cloud partner, you can be sure that you're adding multiple layers of security to your standard SaaS services.

Cloud-based service providers offer gateways that can prevent phishing emails from getting to your employees. They can keep malicious, malware-infected applications out of your tech stack and virtually eliminate the threat of damage from a cyberattack. And they can do it all for you so you can run your business without worry.

With your data stored in purpose-built, enterprise-level facilities, your information is available whenever you need it, even if your SaaS application experiences an outage. Add all of that to a professional team of experts at your disposal when you have questions or issues, and bringing in a third party to reinforce SaaS cybersecurity for apps just makes sense.

Again, Microsoft itself recommends hiring a third party for data protection. A provider of cloud services offers all the functionality you need with little to no work on your part and a monthly fee that's easy to plan and budget for.

With your data stored in purpose-built, enterprise-level facilities, your information is available whenever you need it, even if your SaaS application experiences an outage.

Rightworks has you covered with enhanced SaaS cybersecurity

Rightworks provides the security cover you need for your SaaS applications. You can buy **Microsoft 365 licenses** with enhanced security provided by Rightworks experts. Cloud-based **managed security services** keep your business-critical data safe on all workstations.

Rightworks security services provide the protection your business needs at a fixed monthly cost that can scale as your business grows. Rightworks protects your SaaS data as well as securing your email and even training your employees to avoid cyberthreats.

You firm or business can trust Rightworks to:

- Protect your data in enterprise-class facilities and provide US-based, 24/7/365 support.
- Back up and protect your data in top-tier data centers for maximum availability.
- Protect your email client with security measures that go beyond what the SaaS apps offer.
- Update security technology without having any impact on your daily business activity.
- Protect the laptops you use to do your job every day.
- Train and test employees so they know how to avoid cybersecurity risks.

The SaaS revolution took software off the laptop and put it in the cloud, but it didn't fully take security with it. Businesses that rely on standard SaaS cybersecurity put themselves at risk if they don't bring in experts to manage security. Rightworks has the experience, facilities and expertise to keep your data safe and available while you run your business with peace of mind.

Want to learn more?
Contact us today at 888.245.0292

 **rightworks**
rightworks.com