

Servium | arcserve®



THE ULTIMATE GUIDE TO SECURING SaaS DATA

Keeping your data secure
in the cloud

















Insight Guide

WHOSE SECURITY IS IT, ANYWAY?

With businesses of every kind turning to cloud, it's critical to clearly delineate who is responsible for what. Your cloud provider takes on a lot of the responsibility for their environment, especially in the case of SaaS, but organisations often aren't fully aware of what they need to be looking out for.

Since the lines of who controls what can be hazy, it's always good to start with the shared responsibility framework, which identifies who takes ownership for what parts of an environment.

SECURITY SHARED RESPONSIBILITY FRAMEWORK

	On-Premises	Infrastructure-as-a-service (IaaS)	Platform-as-a-service (PaaS)	Software-as-a-service (SaaS)
Data	 You	 You	 You	 You
Applications	 You	 You	 You	 CSP
Operating System	 You	 You	 CSP	 CSP
Hardware	 You	 CSP	 CSP	 CSP

Maintain clear boundaries for security ownership

In SaaS agreements, it stands to reason that since it's their environment, security should be the concern of the hyperscaler or cloud provider offering the applications.

That's somewhat true, but not in the way many businesses think.

A public cloud provider is responsible for the security of their cloud, and SaaS app providers need to take accountability for the security of their application as a whole, rather than your environment specifically and in particular the data you retain within it.

For example, if Microsoft 365 is taken offline by bad actors, or cybercriminals exploit a vulnerability in the software to compromise any and all user accounts, then that's an issue for Microsoft to solve.

But at the same time, if a cybercriminal gets access to your Microsoft 365 account by brute forcing your password and subsequently makes off with important data, or impersonates your users, then you're the one who is responsible.

As the shared responsibility diagram above demonstrates, no matter what your agreement is with a cloud provider, data is always your responsibility. However, the confusion around different obligations means that key elements of SaaS applications end up going unsecured - leaving your business (and the critical data that powers it) open to attack.

ABOUT THIS GUIDE

So, your SaaS data is your responsibility. Now what?

Businesses need to be able to secure their SaaS data, building a rigorous SaaS security approach in the process to keep themselves properly protected. This guide starts here.

Accordingly, we've identified four tiers of SaaS security, running from environments which utilise no additional security measures to well-maintained, strategic security postures.

Every tier is typified by a few specific concerns - this guide will run through each, and demonstrate how you can adjust your security posture to meet these challenges and advance your SaaS security.

The end goal is to ensure that your SaaS data (and the business at large) is protected, following the existing best practises for data protection - the 3-2-1 framework:



3 copies of
your data



2 Stored on
different media



1 With 1 copy air gapped
from your live environment

If you're short on time, take a look at our overview below, and skip to the section that most speaks to your business' current approach to cloud security, and the challenges you may be facing. The guide will show you the best next steps from there:



GETTING STARTED

Challenge: Ensuring a closed environment

A journey of a thousand miles starts with a single step. Cybersecurity is no different.

While it may seem obvious, data being left open for cybercriminals to access is worryingly common. According to Verizon's Data Breach Investigations Report,¹ **roughly 10% of breaches** stem from **data that's simply been left visible** to prying eyes. While these oversights are often an honest mistake, it's a precarious situation that any organisation could find itself on the receiving end of.

To take a real-world example of how damaging this can be, the confidential "no-fly" list that the American TSA use was leaked after a hacker found it on a publicly accessible misconfigured AWS server.²

Oversights like this aren't exclusive to IaaS solutions, however. The data that's generated in and by your SaaS applications can often be left publicly available due to similar oversights when it comes to security. For example, an organisation might be allowing anyone with a link to a file sharing platform they use to upload any files they please - potentially allowing a bad actor to deposit ransomware into your environment directly.

As a result, misconfiguration means that even the most advanced security systems can count for nothing - it's like building a castle but forgetting to construct one of the walls.

Solution: Following best practices

It might seem obvious, but following existing best practices is often the easiest way to ensure that you're not leaving your critical SaaS applications and the data they generate open for anyone to access.

In many cases, the hard work here has already been done by your SaaS provider, giving you tools to manage the security and permissions of your applications, as well as control how accessible they are to users outside of your organisation.

From that baseline, it's important to ensure that you also aren't being left exposed by your users. Good password hygiene and user awareness training can help provide a solid start in your journey to superior SaaS security, and ensures that you won't fall at the first hurdle if, for example, an enterprising cybercriminal tries to access your SaaS application with "admin" and "password" as their credentials.

¹ <https://www.verizon.com/business/resources/reports/dbir/>

² <https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair/>

FOUNDATIONAL SaaS SECURITY

Challenge: Establishing data resilience

Many early adopters of cloud - both vendors and customers, saw its potential as a way to backup data.

After all, it's always accessible, and back when on-premises was largely the default operating infrastructure, cloud was always neatly separated from business environments, making following the 3-2-1 framework easy.

That's part of the reason why there are so many backup solutions available to businesses that make use of the public cloud. However, these are services built for the explicit purposes of backing up data and long-term storage and retrieval. There is an argument to say this has contributed to a worrying misjudgement of responsibilities and obligations of the provider when other types of

cloud service are consumed. The reality is that many businesses labour under the belief that all cloud data is backed up by default, with **only 16% of respondents** to one survey even **attempting to back up their SaaS data** as a result of this misunderstanding.³

The underlying assumption is that since a SaaS application can be accessed from anywhere, the data within it isn't at risk in the same way as data on a user's hard drive. After all, if you can download the file onto a new device, then surely it's backed up?

Of course, this isn't actually the case. SaaS data can be just as, if not more vulnerable than on-premises data, and businesses need to take steps to ensure it's not left unsecured.

Solution: Setting up dedicated backups

From this position, the first step needs to be establishing real, dedicated backups using a purpose-built backup solution to ensure SaaS data isn't left at risk.

At this point in your journey to better cyber resilience, there's a lot of options available to you: backing up to on-premises infrastructure, tapes and other offline media, or a cloud-based Backup-as-a-Service solution. All have their strengths and drawbacks and depending on considerations like cost, data volume, and speed will be a better or worse fit for a business.

As we explore later in the guide, the backups ought to be immutable and properly air gapped - meaning that backup files can't be edited and are kept away from live SaaS data as much as possible.

When picking your backup solution, you should keep the 3-2-1 framework discussed earlier in mind - is a backup solution storing data on a different form of media? How many copies does it produce? Where does it store them, and how long for? These are all key questions you should seek answers to before committing to any given solution, and a failure to consider them doesn't just hamper security but can also spell disaster for businesses needing to meet strict compliance frameworks around their data storage.

³ <https://www.statista.com/statistics/995279/worldwide-business-data-backup-usage-by-type/>



Challenge: Ensuring a closed environment

Having established backups of your SaaS data can only go so far, especially if bad actors can still get access to your systems and put both live and backup data at risk. To this end, cybercriminals see users as a valuable entry point into an organisation - if they can get access to legitimate user credentials they can bypass security measures and get into your data.

As a result, legitimate credentials are one of the first things a cybercriminal will look for to exploit a system. Verizon reports that the **use of stolen credentials is the top method cybercriminals employ** when compromising organisations - sitting above even ransomware.¹ Phishing and pretexting - two other methods sitting in Verizon's top 5, also prey on your users to bypass security.

The reason this can be so devastating comes down to poor access management. Especially in fast-moving businesses where documentation and data need to be shared externally on a regular basis, access management falls by the wayside. The result of this is that if cybercriminals get inside a system, they're free to navigate deeper, appearing to all security measures to be a legitimate user. This gives them the ability to interact with your SaaS data, whether that's deploying ransomware to encrypt it, attempting to acquire more credentials for follow-up attacks, or threatening to leak sensitive information unless the business pays them off. So long as they have legitimate credentials, a SaaS application will see them as just another user.

¹ <https://www.verizon.com/business/resources/reports/dbir/>

Solution: Enabling access controls

Access controls and management can take a lot of different forms. Entry-level solutions like multi-factor authentication (MFA) are essentials for any business, requiring users to verify they are who they claim to be before giving them access to important systems.

Of course, MFA isn't the apex of access management - in a number of high-profile cases over the years, cybercriminals have expanded their repertoire when it comes to social engineering strategies, incorporating spoofed MFA prompts to help them bypass controls in the environments they're trying to access. Compared to more conventional attacks, however, these remain incredibly rare.

For more robust access measures, businesses can look towards more advanced solutions that work on the same core idea as MFA - solutions like physical passkeys and biometric identifiers which rely on users having something on their person (or about their person) they can use to validate they are who they say they are. These solutions are much more difficult to bypass - usually requiring real-world criminal activity in order to do so.

These solutions don't need to get in the way of business agility, however. Single sign-on (SSO) solutions allow businesses to kill two birds with one stone, by enabling better access management while making life easier for users.

Importantly, SSO simplifies the monitoring of who has access to your environment, giving organisations a single pane of glass from which data access can be controlled and managed. At the same time, users benefit from a smoother sign-in experience when accessing cloud-based services and key SaaS applications, rather than needing to remember an exhaustive list of login credentials.

ESTABLISHED SaaS SECURITY

Challenge: Improving data resilience

Once you've reached this level of SaaS security maturity, things can quickly become something of a rabbit hole. To prevent yourself from getting lost, it's crucial to take a broader view of your environment as a whole, rather than just adding more protections around the perimeter.

No matter how strong your defences are, breaches are ultimately an unfavourable numbers game. You need to be lucky every time with your cyber defence, while cybercriminals just need to get lucky once. As such, resilience and recovery should be the backbone of your security strategy, rather than just afterthoughts.

We've discussed the importance of establishing backups previously, and while getting these set up is a good start, it's also something that malicious actors have come to expect. Increasingly, cybercriminals target backups as a matter of

priority, compromising them or otherwise taking them offline before moving forward with the rest of an attack.

One of the main ways cybercriminals look to make money is through ransomware, and in this case, taking out backups cuts off the "escape route" that businesses would otherwise try to take. Without a backup, often the only option left to recover your data and return to business as usual is to pay up.

Of course, this doesn't always work. Cybercriminals see a victim who has paid up once as a victim who is liable to pay up again, and so they may keep extorting payments from their target while never actually decrypting their data. As such, businesses need a way to keep their backups safe from cybercriminals, so they can ensure they always have a plan B.

Solution: Immutable backup storage

The reason targeting backups works is because they can be just as vulnerable as your live data, but that doesn't need to be the case.

As mentioned earlier, the best backups utilise immutable storage, which keeps files on a write-once, read-many (WORM) basis.

In effect, this means that once a backup file is created, it can't be tampered with or deleted for a specified length of time, meaning ransomware can't get into backup files and encrypt them, and users can't inadvertently delete backup data.

This ensures your backups are always ready to go should the unthinkable occur, and allows you to sidestep paying extortionate ransoms for data recovery.

As a result, you have a significant boost to your cybersecurity as a whole - once you've ejected an attacker from your systems, there's nothing they can hold over your head, and you're free to return to business as usual.

Challenge: Reducing single-cloud dependency

Throughout this guide, we've touched on the 3-2-1 framework for data protection.

It's widely considered best practise for data security, and for good reason - it accounts for all the major precautions an organisation should take to keep their data safe.

But while businesses are prepared to implement and adhere to a 3-2-1 strategy for on-premises data, it can get a lot more complicated to do so in the cloud.

SaaS applications like Salesforce and Microsoft 365 hold all their data in the cloud, and it's down to you to find a way to apply your 3-2-1 framework to it. That can seem easy enough - there's a wide range of cloud-based backup solutions out there which can ingest data from SaaS apps and back it up to the cloud.

But these often open up a new vulnerability - single-cloud dependency.

This occurs when you've essentially placed all your eggs in one basket. While data might seem like it's air gapped in the sense that it's no longer held solely in a SaaS app, it can often be held in a backup service ultimately harnessing the same cloud architecture.

For example, if your Microsoft 365 data gets backed up to another service that's also based in Microsoft Azure, a bad actor that gets into Azure could conceivably manipulate both live and backup data, and similarly if Azure experiences an outage, you're left without access to both.

Solution: Genuine air gaps

To avoid this, businesses need to ensure their backup data is fully air gapped - whether that means backing up to an entirely separate public cloud, or to an off-site datacentre.

However, neither of these options are easily achievable for many businesses. In the case of the former, this can require a lot of effort and research on the part of the business, as many cloud-based backup solutions obscure the provider they rely on to help head off bad actors.

This gets especially difficult for organisations with a multi-cloud strategy - if SaaS data is coming in from every hyperscaler public cloud, then it's difficult to even identify an environment where backups can go, let alone finding a solution that enables them to occur seamlessly in the background.

At the same time, establishing a dedicated on-premises infrastructure for backups is usually cost-prohibitive for businesses, especially those who have been making extensive use of cloud for a long period of time, and have no real existing on-premises infrastructure - or dedicated expertise for setting one up and pulling SaaS data through for backups.

As such, the best solutions for ensuring genuine air gaps are those which are built to function in the cloud and interface directly with SaaS data as it's generated, backing up said data to separate, dedicated datacentres to ensure isolation from live data.

STRATEGIC SaaS SECURITY

Challenge: Optimising the value of SaaS security solutions

If you've navigated directly to this section from the beginning of the document, then congratulations! You've worked hard to establish a robust and reliable strategy for securing and backing up your SaaS environment, to ensure your business is protected even should the unthinkable occur.

But perhaps you haven't quite reached the end of the line.

Protected, reliable, and regular backups still can't prevent downtime outright, as you need time to restore your data to the live environment. The pause in business operations this creates can inflict significant impacts in terms of lost revenue and missed opportunities, especially for solutions which

store backup data to the cloud - restoring from them is a process limited by download speeds and available bandwidth, and if you're recovering a particularly data-rich system, this might mean your business can't get back to normal for days or even weeks.

Cost also becomes a roadblock. As businesses scale and generate ever more data, the price of storage and protection grows exponentially. It's often difficult for IT leaders to justify, as a security or data protection solution can't add immediate value to a business in the same way that investments in other parts of an IT environment can.

Solution: Arcserve SaaS Backup

Businesses need a cyber resilience solution that can meet these challenges - offering reliable backup of SaaS data in line with the strategies we've laid out, at a predictable cost while overcoming the recovery latency should you suffer a data breach or outage. Arcserve SaaS Backup does all of that, and more.

A simple, per-user subscription model gives businesses access to unlimited backup storage, preventing costs from growing exponentially and making it far easier to scale your cyber resilience.

To mitigate the opportunity costs of downtime, Arcserve SaaS Backup stores 4 immutable copies of data across 2 tier 3 datacentres in the UK - meeting the requirements of the 3-2-1 framework, but also giving users the ability to access data even when the live environment is down. For example, users can access the backup system to read copies of emails and stay ahead of their work, even if their email service isn't currently available.

This allows businesses to avoid missing out, keeping key operations running during the process of restoration, rather than needing to wait for everything to come back online before returning to business as usual.

THE NEXT LEVEL OF SaaS SECURITY

Keep all your data safe with Arcserve

No matter where you are in your SaaS security journey, Arcserve SaaS Backup helps you improve your resilience with next-level protections, and powerful features to keep your data safe and your business moving.

Whether you're planning your first forays into cloud, or are looking for a solution to replace an incumbent that's struggling to meet the needs of your business, the power of Arcserve SaaS Backup, combined with predictable economics, make it an ideal solution.

But Arcserve protection doesn't only apply to SaaS data.

With a wide portfolio of solutions, Arcserve can help you protect your data in any part of your environment, and adapt to meet your IT strategy - whether you're strictly on-premises, a cloud-first business, or looking to adopt a hybrid strategy to get the best of both worlds.

Other Arcserve solutions

Arcserve UDP gives you the ability to back up data from your live environment to any designated location, making it essential for orchestrating your security strategy, while **OneXafe** provides a powerful on-premises solution which stores an immutable archive of your data, whether it's being backed up by UDP or an entirely separate backup technology. If you want to know more about how these three solutions can be combined to keep all your data safe, you can find more information here:



[Servium and Arcserve](#)



ABOUT SERVIUM

We're dedicated Arcserve partners, helping our customers deploy powerful resilience solutions from every corner of the Arcserve portfolio. We have a deep pool of expertise, and work closely with Arcserve to ensure that the solution we deploy is right for your business, and ready to go from day one, meaning you don't run the risk of going unprotected during the changeover process.

We're also well-poised to help you scale and upgrade your solution, as well as develop innovative ways to enhance your security posture - in the cloud, on-premises, and anywhere in between.

If you'd like to learn more about deploying an Arcserve solution to keep your data protected, or simply want to ask us a burning question about your security strategy, we're **ready to talk** whenever you are.

Visit servium.com to learn more.

arcserve®