



Safeguarding SaaS with Cloud-to-Cloud data protection

How Backup-as-a-Service (BaaS) protects
critical SaaS data – with ease

SaaS apps are the new norm

As companies look to increase user productivity, lower expenditures, and simplify how they deploy and maintain solutions, it's no surprise that SaaS app adoption is one of the fastest-growing company initiatives. And while SaaS apps were once considered point or niche solutions, new remote workforce models and digital transformation have pushed these cloud-delivered solutions into every aspect of today's modern businesses. In fact, Gartner estimates SaaS market to reach \$117 billion in 2021.1 From CRMs (like Salesforce), to productivity apps (like Office 365), to critical business applications (like ERPs), organizations rely heavily on SaaS solutions to drive efficiencies, cost savings and performance – which help instill resiliency and avoid disruptions in today's volatile landscape.

Protecting SaaS data is on you

While SaaS applications provide robust capabilities and are cost-effective, they are not all-encompassing – and require dedicated data protection. In fact, third-party coverage is largely considered your data's last line of defense. Without it, you may be susceptible to permanent loss – driving businesses everywhere to reimagine how they stay data compliant, ensure higher business continuity, meet required SLAs, and mitigate emerging data loss threats (like ransomware).



Cybercrime
is up
400%²

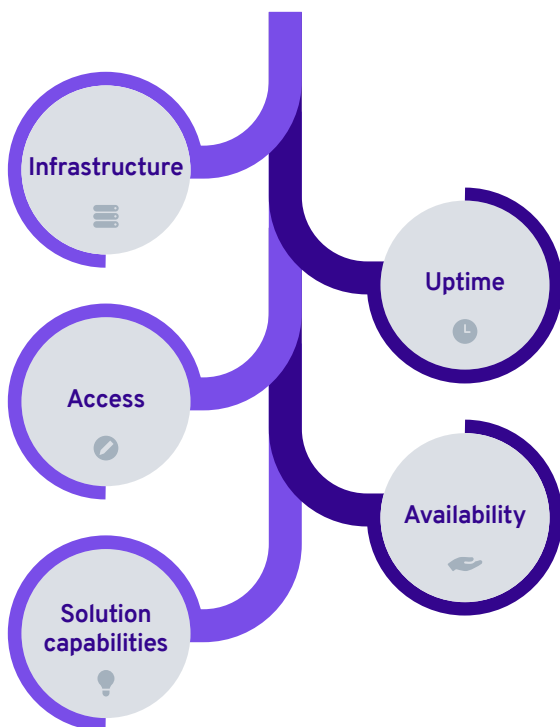
Users and admin
errors lead to
47%³
of SaaS data
loss

63%⁴
of successful
attacks come
from internal
sources

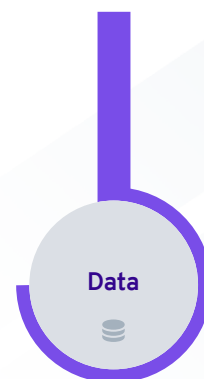
Shared Responsibility Model

Many believe the cloud service providers who administer today's SaaS applications are also responsible for protecting data created and stored within them. However, the majority of cloud service providers (like Microsoft, Salesforce, AWS, and more) follow what is known as the 'shared-responsibility model'. In this model, the cloud service provider is responsible for maintaining the uptime, availability and access of their SaaS solution. The customer, on the other hand, takes responsibility and ownership for protecting their own data entering, housed in, and leaving the SaaS solution. Given this, CIOs must recognize that the responsibility of protecting cloud data lies within their organization.

Cloud Service Provider



Customer



SaaS apps require dedicated protection

While some cloud service providers offer native controls for temporary data replication – they are not comprehensive in nature and do not offer long term retention or rapid controls for recovery. Data experts emphasize the need for a proactive data protection strategy that goes beyond the gaps in native coverage, while cloud service providers themselves recommend that customers implement third-party backups.

Best practices hinge on having a dedicated solution that protects data living within your SaaS applications by:

- ✔ Isolating backup data from source data
- ✔ Preserving data in air-gapped, immutable locations
- ✔ Adhering to retention and recovery SLAs and legislation
- ✔ Delivering extended protection, across active and deleted data
- ✔ Enabling granular, version-level, and flexible recovery options
- ✔ Ensuring speed, scale, and high resiliency

The benefits of BaaS for SaaS

SaaS solutions revolve around simple subscriptions, predictable costs, and no large capital investments – making it an attractive and viable option for organizations today. Backup-as-a-service (BaaS) data protection is no different. BaaS solutions offer enterprise-grade protection with the same benefits and consumption model as existing SaaS solutions, helping companies secure their data, accelerate their journey to the cloud, and drive faster innovation. This cloud-to-cloud model allows businesses of all sizes to simplify data protection without sacrificing features and functionality.

Why Metallic BaaS

With Metallic Backup, you get cost-effective and industry-trust protection, without the complexity. Cloud-to-Cloud data protection that's proven to reduce costs, decrease overhead and eliminate headaches – so you only pay for what you need. You save on:



Network & Compute

No network, hardware and infrastructure expenses. With Metallic you get full-hosted data protection, so you'll never face installation, configuration or large upfront capital investments again.



Admin Time

Eliminate the grunt work. Metallic simplifies data protection, freeing administrators from routine hardware and support maintenance – making backup and recovery a breeze.



Maintenance

Zero software maintenance and licensing. Metallic means we provide automatic updates, releases and in-product support, so you don't have to – helping reduce the burden on IT.



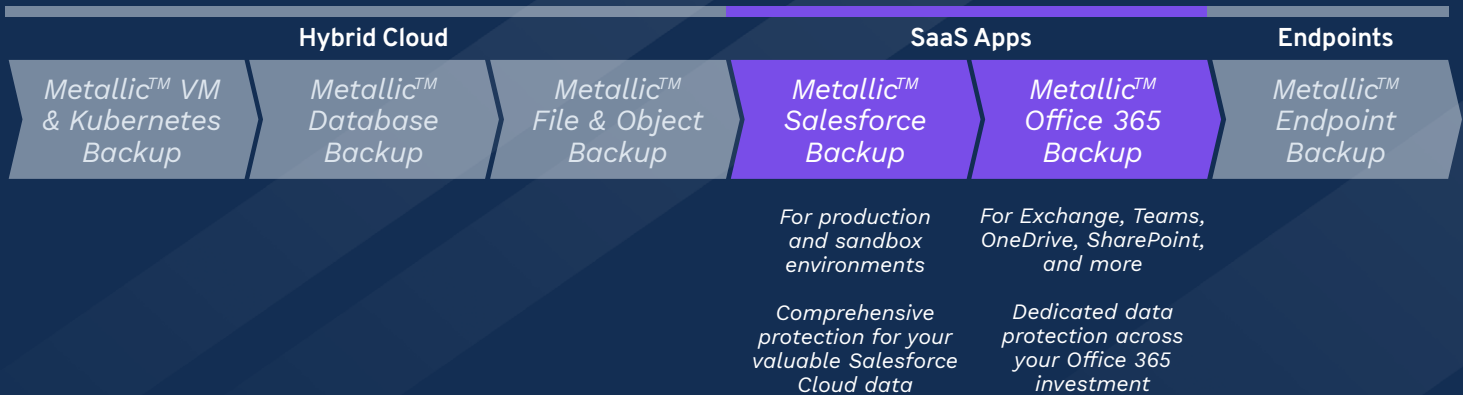
Storage

Ditch the hidden the storage fees. With unlimited Azure storage built into per-user costs, Metallic provides a cost-effective way for your data to grow

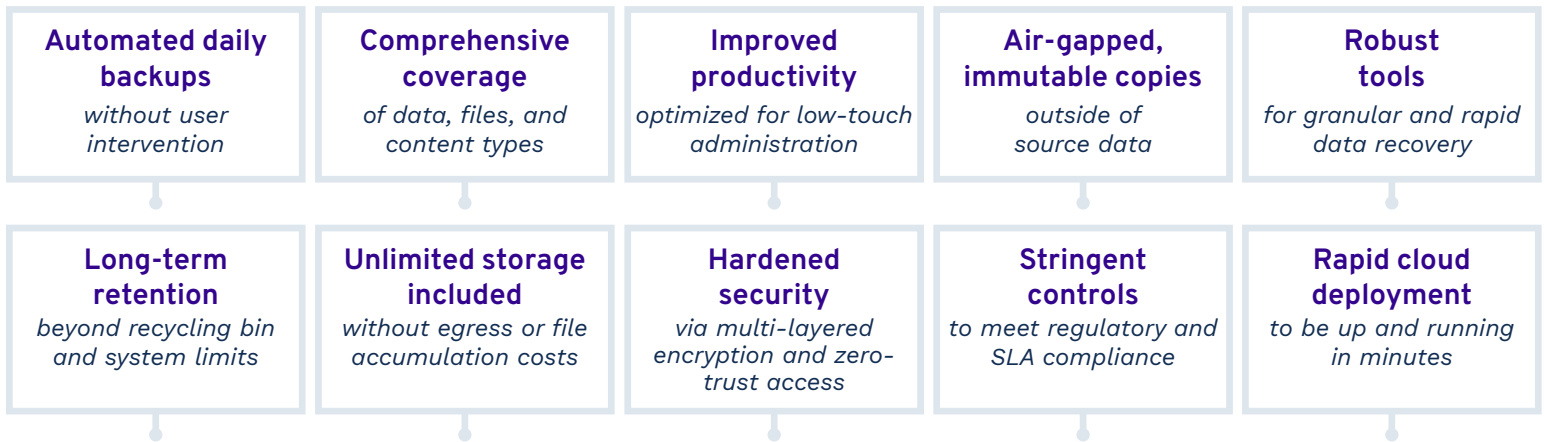
The award-winning Metallic BaaS portfolio

Metallic, built on industry-leading Commvault technologies and powered by Microsoft Azure, delivers trusted backup and recovery with the simplicity of SaaS. With broad-ranging coverage across apps, endpoints, on-prem, and cloud environments - Metallic offers admins and IT professionals comprehensive data protection from deletion, corruption, and malicious attack.

The Metallic Portfolio



Stay protected, stay compliant, and stay recoverable with Metallic BaaS



NEXT STEP



Protecting SaaS data and applications may seem overwhelming, but you don't have to do it alone. Metallic BaaS is here to help you every step of the way.

Checkout [Metallic.io](https://metallic.io) and get started with your free trial today!

Copyright 2021 Commvault Systems, Inc. All rights reserved. Metallic, Metallic and the "M Wave" logo, and the "M Wave" logo are the trademarks or registered trademarks of Commvault Systems, Inc. All third-party brands, product names, service names, trademarks or registered trademarks are the property of and used to identify the products or services of their respective owners.

Sources

- <https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021>
- <https://www.Entrepreneur.Com/article/349509>
- <https://blog.cloudhq.net/1-out-of-3-companies-lose-data-in-saas/#:~:text=Data%20loss%20in%20SaaS&text=The%20vast%20majority%20of%20data,lost%20data%20as%20a%20result>
- <https://purplesec.us/resources/cyber-security-statistics>