



Harnessing SaaS for Hybrid Cloud Resilience

Strategies for Today's CIOs

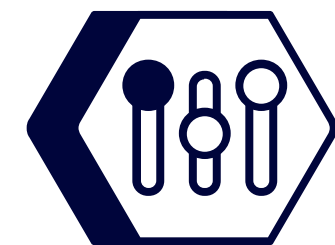
Welcome to the new reality of cyber resilience

Whenever disruption occurs, the longer your organization takes to react to it or adapt to it, the more growth and revenue you'll miss out on. As cyber resilience trends tip toward as-a-service delivery, a SaaS-delivered solution can empower your company's digital transformation. The big question you should always be asking right now is:

Why wait?



The world keeps changing



Your tools and business priorities keep evolving



And the risks keep rising

The disruption of COVID-19 accelerated massive corporate digital transformation, as 60% of the world's corporate data is stored in the cloud.¹ Many companies are now assessing these changes to their infrastructure to determine how they can optimize and better manage their hybrid cloud environment, including the growing need to safeguard data no matter where it lives.

As companies grapple with growing cyber resilience challenges, CIOs need smart and flexible solutions for securing data across hybrid environments. Simultaneously, SaaS-delivered cyber resilience options are expanding.

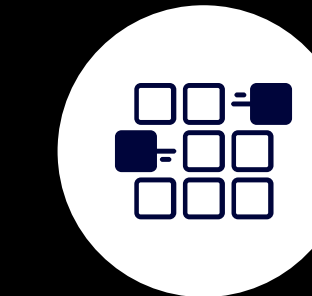
Companies are looking for agile solutions that are:

- Quick to implement
- Minimal-to-no upfront costs
- Simple to manage
- Able to reduce infrastructure footprint

However, to date, limited or inflexible options across vendors may have kept companies from adopting a SaaS solution to safeguard and manage their data.

Companies who want to benefit from cloud-delivered solutions must demand the necessary breadth, flexibility, and security to meet their needs not only today, but as their business continues to evolve. If the past few years are any indication, the pace of change for IT organizations will only increase.

Growing challenges of cyber resilience



Managing data sprawl



Securing data from ransomware attacks



Controlling costs & managing infrastructure



Driving compliance



Privacy & data security requirements

A clear SaaS vision for today's CIOs

When plotting out the best ways to adopt SaaS-delivered cyber resilience, it's essential to consider the impact to your IT and your business strategy.

Hybrid IT is the reality for the foreseeable future

While companies are increasingly moving to cloud, others are moving select applications back on premises, maintaining hybrid environments for the foreseeable future.

A survey of over 1,000 IT decision makers found that **84%** expect the amount of data they store in the public cloud to increase in 2023.²

According to IDC analysts around **70% to 80%** of companies are repatriating at least some data back from the public cloud each year.³



In addition, the digital transformation journey is contributing to enormous data sprawl across cloud and on-premises environments. As companies are caught between realities of cloud and on premises, app modernization imperatives, and SaaS adoption, the data sprawl that ensues can create complexities that make it hard to mitigate the risk of ransomware, ensure

compliance, and protect against data loss. This shift has only accelerated the need for simplified cyber resilience solutions that can handle hybrid operational strategies and help companies close the gap between where they are today, and where they need to be tomorrow.

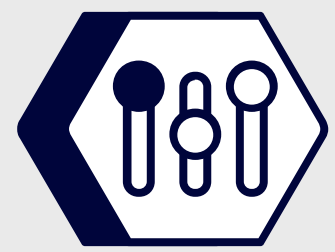
72%
of companies
report using
hybrid cloud
today, with 53% of
workloads running
in public cloud.⁴

SaaS solutions can bridge the resource gap

With the right support for hybrid cloud environments, cyber resilience delivered as a SaaS solution has the capability to bridge an important gap for many companies that don't have the skills, resources, or budget to handle their data backup and recovery needs through

a traditional self-managed software solution. Companies are also preferring to leverage existing staff and resources on transformational activities, rather than managing and maintaining infrastructure related to data backup and recovery.

SaaS-delivered solutions can provide that freedom, and include benefits such as:



Capex to opex

Shifting from a capex to opex operational model frees up resources that would be otherwise dedicated to overseeing onsite infrastructure, lowers capital cost, and reduces budgetary restrictions.



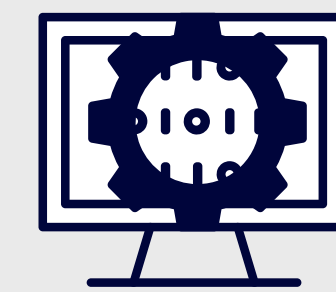
Air-gapped security

Air-gapped copies of cloud data can ease the impact of digital threats such as ransomware and allow for faster, fuller cyber recovery of business-critical data.



Reduced TCO

SaaS-delivered cyber resilience can generate ongoing savings in areas such as Microsoft 365 usage, admin resources, and even staff training.



Simplified management

Instead of dealing with many different vendors or disparate services, a single platform SaaS solution can streamline your cyber resilience and data security, while eliminating the need to manage your own backup infrastructure.

Proactive cyber resilience trumps reactive damage control

The world won't wait for you. Change is happening and is only going to accelerate with each passing day. At the same time, the threats continue to rise, and the cost of data breaches increases.

In 2023
66% of global organizations

have been hit by ransomware⁵

Lack of resources / expertise

remains one of the top challenges for enterprises transitioning to cloud⁴

A single hour of downtime costs the average business more than
\$540,000 USD⁶

How do you combine the cyber resilience solutions you need for any phase of your transformation journey?

Simple.

Partner with a single vendor who offers breadth of coverage today with scale and flexibility for the future.

What's an IT leader to do?

When considering SaaS-delivered cyber resilience to help achieve your digital transformation goals—while mitigating the risks of data sprawl—here are 5 critical building blocks to help you succeed:

#1

Stay SaaS secure

SaaS cyber resilience has become one of the primary approaches for modern enterprises for good reason. Currently, companies use 130 SaaS apps on average.⁷ Productivity in many of those companies is driven by SaaS applications such as Microsoft 365 and Microsoft Teams, or Microsoft Dynamics.

The shared responsibility model for managing SaaS applications, including Microsoft 365, Dynamics 365, and Salesforce, dictates that data backup and recovery is the responsibility of the customer. SaaS applications must have dedicated solutions in place for the long-term to secure data from threat of ransomware attack, internal malicious

actors, accidental deletion, or corruption. And for companies who are running critical productivity and customer engagement applications in the cloud, pairing SaaS-delivered cyber resilience capabilities is a seamless option.

Look for a comprehensive solution like Commvault® Cloud, SaaS-delivered cyber resilience from an industry-leader, to ensure broad coverage within each SaaS application. For instance, when protecting Microsoft 365, look for robust coverage for Microsoft Teams, and not just backup for mailboxes, SharePoint, or OneDrive.

#2

Think hybrid first

As companies take a hybrid approach to technology and infrastructure, IT leaders should look for solutions that allow seamless management of both cloud and on-premises data, without degrading performance. Companies should have the freedom to backup and restore broad data types to the appropriate target—to cloud or on-premises storage—as well as to send secondary backup copies to Azure for long-term data retention and air-gapped ransomware protection as needed. Cloud-based cyber resilience solutions that don't provide on-premises data management options can have customers waiting up to 10 days for a restore.

On-premises and cloud data shouldn't require mutually exclusive cyber resilience and data security solutions. Thanks to Commvault Cloud offering unique storage flexibility, companies can seamlessly back up to cloud or on premises, with single-pane-of-glass management. Customers can control and protect their on-premises data through a simple SaaS-delivered solution, without data ever having to leave on premises.



87% of organizations are multcloud, with 72% of those deploying hybrid cloud.⁴

flexera

#3

Start planning tomorrow's migration today

As your data migrations and backup needs rise, your cyber resilience solution should operate seamlessly across cloud instances and on-premises infrastructure to handle your enterprise-critical workloads. These workloads can include SAP HANA, Microsoft SQL, and Oracle databases, for instance. By anticipating where your data will be processed, you can ensure the

management solutions are already in place to keep it secure whether at-rest or in-flight.

In addition, putting your data protection in the cloud with a SaaS-delivered solution can be an effective early step to a planned migration, setting the table for your cloud transformation.

#4

Keep your app journey secure end-to-end

As you transition from traditional application platforms to containerized approaches such as Kubernetes, your data security must remain a top priority. With stateful enterprise applications moving into containers, the protection needs have changed, shifting to backing up the Kubernetes application and its associated data, images, and cluster control plane.

While high availability can indeed bring back the containers during disaster scenarios, the application cannot recover and be fully operational if the underlying data is corrupted or lost. Securing your Kubernetes data ensures full recovery, rapidly restoring applications with minimal disruption to business. Commvault Cloud also offers SaaS-delivered protection for Kubernetes, supporting all CNCF-certified distributions.

#5

Engage centralized management

Avoid tacking on a bunch of different tools and platforms that create overly complex data management and security interfaces. A solution that operates through a single-pane-of-glass dashboard lets all your workloads be protected while your cyber resilience remains as efficient and comprehensive as possible.

Commvault Cloud provides this critical visibility and simplified workload with the ability to manage any

data, anywhere, all from one console. Integration with Commvault Cloud Autonomous Recovery through a central Command Center means customers can select both SaaS- and self-managed solutions if their strategy requires, and still enjoy industry leadership.

With the addition of Commvault Cloud HyperScale X, companies can store backups locally for speedy recovery of large on-premises data sets.

We are able to have all of our backups in the cloud now, and were even able to leverage our existing Azure storage. With Commvault Cloud, we no longer have to manage and maintain physical hardware which makes us financially and even technically more efficient.

—Jeff Day
Systems Technical Supervisor,
State of Nevada Department
of Transportation*

We're more efficient in all of our backups for Microsoft 365 because it's in a single pane of glass.

—Kristian Smith
Manager of Technical Services
& Support at Linamar**

Your next steps to SaaS cyber resilience

So, why wait?

You see the mounting realities putting pressure on your need to safeguard and manage your data on all fronts.

Ransomware attacks are increasing every day.









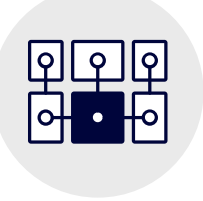



Your online collaboration tools demand compliant data security solutions.

The current remote workforce puts endpoint devices at constant risk for security breaches.

Your business is using cloud-based solutions more every day.

Now's the time to invest in the SaaS-delivered solution that you need to secure all your data immediately—while having the flexibility and scalability to grow with your future data management needs.

The gold standard in SaaS-delivered cyber resilience

| | | | | | |
|---|--|--|---|--|---|
|  VM For Microsoft Hyper-V, VMware, Azure VM, Microsoft Azure, AWS, AVS, VMware Cloud. |  Kubernetes For Kubernetes |  Database For Microsoft SQL, Azure PaaS, Oracle, Amazon AWS, SAP HANA. |  File & Object For Windows Server, Azure Blob & Files, OCI Object Storage, Amazon S3, Linux/UNIX. |  Endpoint For laptops and desktops. |  Air-gapped Storage For isolated cloud storage. |
|  Auto Recovery For VMs |  Microsoft 365 For Exchange, Teams, SharePoint, OneDrive, Project, and more. |  Risk Analysis For M365 |  Microsoft Dynamics 365 For CE applications and Power Platform. |  Salesforce For Salesforce Cloud data. |  Threat Scan For Files |



Commvault is setting itself as the gold standard for Enterprise cyber resilience with a belief that no workload should be left behind; be it at the edge, in the cloud, on premise, or in the data center. That these should all be served in a fast to configure, protect anywhere, single pane data model backed by Commvault and Microsoft as trusted brands.

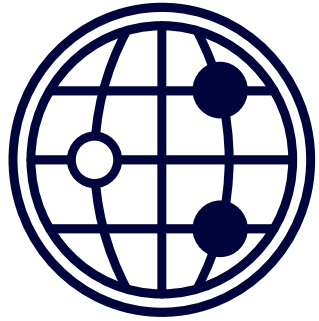



—Ian Moyse, Cloud Matters
Cloud Industry Thought Leader & Social Influencer*

Commvault Cloud + Microsoft Azure

The answer you're seeking

Commvault Cloud, powered by Metallic AI was established to bring next-generation software-as-a-service (SaaS) cyber resilience to the market, delivering Commvault's powerful core technology simply through the cloud. A cloud-native solution built with the best of Azure PaaS and native services, Commvault Cloud delivers unmatched technology together with the durability, scale, and security of Microsoft Azure. Commvault and Azure, are leading in the evolution of the cyber resilience industry—with an enterprise-grade SaaS solution.

Commvault Cloud, with the power of Azure, is:

| | |
|---|---|
|  <p>Available in 30 countries across the globe</p> |  <p>Protecting workloads in everything from SaaS applications and endpoints, to Kubernetes to SAP HANA, on premises or in Azure</p> |
| |  <p>Constantly adding new abilities and features such as Commvault Cloud Compliance, fast and flexible restore of Microsoft Teams data for Microsoft 365 backup, and unique edge management capabilities</p> |
| |  <p>Winning awards such as Best of VMWare, the Gold Stevie in Cloud Storage and Backup, and the #1 spot in SaaS Backup on IT Central Station</p> |

Defining the Gold Standard



The rise in both remote work and potential data risk is driving strong demand for cloud-based data protection solutions—with the continued expansion of Metallic's SaaS Plus portfolio, Commvault has created an impressive backup-as-a-service ecosystem—a comprehensive range of offerings supporting enterprise-wide workloads to the backup target of choice, whether it's on-premises, in the cloud, or to the HyperScale X appliance.

—Vinny Choinski
Enterprise Strategy Group Sr.
Validation analyst

United for a best-practice solution: Commvault Cloud and Microsoft



The recognized leaders

Based on industry-leading technology, Commvault Cloud accolades include 2020 Gold Stevie® Award for Cloud Storage & Backup Solution.

Microsoft provides the gold standard enterprise cloud workloads with more than 95% of Fortune 500 companies using Microsoft Azure.

The power to scale

Scale from 10-10,000+ terabytes or more as the amount of data you have continues to grow with straightforward, tiered pricing. You pay only for what you use.

Global reach and scalability: With datacenters in 60+ regions and 140 countries, Azure provides a global reach with a local presence to reduce the cost, time, and complexity of operating a global infrastructure.

A foundation of experience

More than 100,000 organizations rely on Commvault—so we know what it takes to accelerate digital transformation.

Secure, trusted, and compliant, Microsoft leads the industry with 90+ compliance certifications, backed by 3,500 cybersecurity experts.

Ahead of the innovation curve

In winning the Best of VMworld Award, judges remarked that Commvault Cloud is “cloud-based backup done right for a change.”

Microsoft has added over 1,000 new capabilities recently that help you build the latest advancements in AI, blockchain, Kubernetes, containers, and databases.

Flexibility for backup on your terms

Commvault Cloud has breadth of coverage and flexibility to safeguard everything from endpoints to SaaS applications to enterprise-critical data center workloads and on premises and cloud-based data—all with a simple SaaS solution.

With Azure, you choose. You can build, deploy, scale, and manage servers, services, and applications across a global network of datacenters.

Commvault, and Azure have united to meet companies where their greatest needs are for cyber resilience while also enabling them to overcome the data challenges tomorrow will bring. Through its scope and flexibility, Commvault Cloud is helping customers make the most of their entire data infrastructure while harnessing the benefits of a SaaS-delivered solution and enjoy uncompromising security and peace of mind.

Reach out for your demo today

Sources

1. Data Threat Report Global Edition | Thales | 2022
2. Global Cloud Storage Index | Wasabi | 2023
3. Cloud repatriation and the death of cloud-only | Data Center Dynamics | 2023
4. State of the Cloud Report | Flexera | 2023
5. The State of Ransomware | Sophos | 2023
6. Average Cost of Downtime per Industry | Pingdom | 2023
7. State of SaaSops | BetterCloud | 2023

