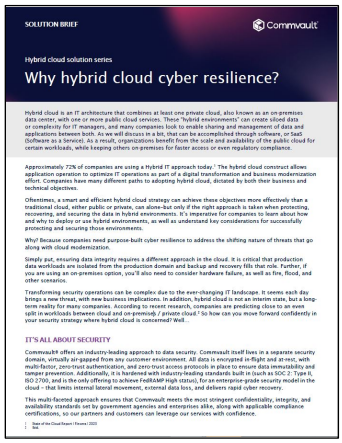

SOLUTION BRIEF

Commvault

Hybrid cloud solution series

Why hybrid cloud cyber resilience?

Hybrid cloud is an IT architecture that combines at least one private cloud, also known as an on-premises data center, with one or more public cloud services. These "hybrid environments" can create siloed data or complexity for IT managers, and many companies look to enable sharing and management of data and applications between both. As we will discuss in a bit, that can be accomplished through software, or SaaS (Software as a Service). As a result, organizations benefit from the scale and availability of the public cloud for certain workloads, while keeping others on-premises for faster access or even regulatory compliance.

Approximately 72% of companies are using a Hybrid IT approach today.[1] The hybrid cloud construct allows application operation to optimize IT operations as part of a digital transformation and business modernization effort. Companies have many different paths to adopting hybrid cloud, dictated by both their business and technical objectives.

Oftentimes, a smart and efficient hybrid cloud strategy can achieve these objectives more effectively than a traditional cloud, either public or private, can alone–but only if the right approach is taken when protecting, recovering, and securing the data in hybrid environments. It's imperative for companies to learn about how and why to deploy or use hybrid environments, as well as understand key considerations for successfully protecting and securing those environments.

Why? Because companies need purpose-built cyber resilience to address the shifting nature of threats that go along with cloud modernization.

Simply put, ensuring data integrity requires a different approach in the cloud. It is critical that production data workloads are isolated from the production domain and backup and recovery fills that role. Further, if you are using an on-premises option, you'll also need to consider hardware failure, as well as fire, flood, and other scenarios.

Transforming security operations can be complex due to the ever-changing IT landscape. It seems each day brings a new threat, with new business implications. In addition, hybrid cloud is not an interim state, but a long-term reality for many companies. According to recent research, companies are predicting close to an even split in workloads between cloud and on-premises / private cloud.[1] So how can you move forward confidently in your security strategy where hybrid cloud is concerned? Well…

IT'S ALL ABOUT SECURITY

Commvault® offers an industry-leading approach to data security. Commvault itself lives in a separate security domain, virtually air-gapped from any customer environment. All data is encrypted in-flight and at-rest, with multi-factor, zero-trust authentication, and zero-trust access protocols in place to ensure data immutability and tamper prevention. Additionally, it is hardened with industry-leading standards built in (such as SOC 2 Type II, ISO 2700, and is the only offering to achieve FedRAMP High status), for an enterprise-grade security model in the cloud – that limits internal lateral movement, external data loss, and delivers rapid cyber recovery.

This multi-faceted approach ensures that Commvault meets the most stringent confidentiality, integrity, and availability standards set by government agencies and enterprises alike, along with applicable compliance certifications, so our partners and customers can leverage our services with confidence.

[1] State of the Cloud Report | Flexera | 2021

Why hybrid cloud cyber resilience?

Thank you for downloading this Commvault Solution Brief.

To learn how to take the next step toward acquiring Commvault's solutions, please check out the following resources and information:

For additional resources:
carah.io/CommvaultResources

For upcoming events:
carah.io/CommvaultEvents

For additional CrowdStrike solutions:
carah.io/CommvaultProducts

For additional Cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Commvault@carahsoft.com
888-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/CommvaultContracts

SOLUTION BRIEF

Hybrid cloud solution series

Why hybrid cloud cyber resilience?

Hybrid cloud is an IT architecture that combines at least one private cloud, also known as an on-premises data center, with one or more public cloud services. These "hybrid environments" can create siloed data or complexity for IT managers, and many companies look to enable sharing and management of data and applications between both. As we will discuss in a bit, that can be accomplished through software, or SaaS (Software as a Service). As a result, organizations benefit from the scale and availability of the public cloud for certain workloads, while keeping others on-premises for faster access or even regulatory compliance.

Approximately 72% of companies are using a Hybrid IT approach today.[1] The hybrid cloud construct allows application operation to optimize IT operations as part of a digital transformation and business modernization effort. Companies have many different paths to adopting hybrid cloud, dictated by both their business and technical objectives.

Oftentimes, a smart and efficient hybrid cloud strategy can achieve these objectives more effectively than a traditional cloud, either public or private, can alone–but only if the right approach is taken when protecting, recovering, and securing the data in hybrid environments. It's imperative for companies to learn about how and why to deploy or use hybrid environments, as well as understand key considerations for successfully protecting and securing those environments.

Why? Because companies need purpose-built cyber resilience to address the shifting nature of threats that go along with cloud modernization.

Simply put, ensuring data integrity requires a different approach in the cloud. It is critical that production data workloads are isolated from the production domain and backup and recovery fills that role. Further, if you are using an on-premises option, you'll also need to consider hardware failure, as well as fire, flood, and other scenarios.

Transforming security operations can be complex due to the ever-changing IT landscape. It seems each day brings a new threat, with new business implications. In addition, hybrid cloud is not an interim state, but a long-term reality for many companies. According to recent research, companies are predicting close to an even split in workloads between cloud and on-premises / private cloud.[2] So how can you move forward confidently in your security strategy where hybrid cloud is concerned? Well…

IT'S ALL ABOUT SECURITY

Commvault® offers an industry-leading approach to data security. Commvault itself lives in a separate security domain, virtually air-gapped from any customer environment. All data is encrypted in-flight and at-rest, with multi-factor, zero-trust authentication, and zero-trust access protocols in place to ensure data immutability and tamper prevention. Additionally, it is hardened with industry-leading standards built in (such as SOC 2: Type II, ISO 2700, and is the only offering to achieve FedRAMP High status), for an enterprise-grade security model in the cloud – that limits internal lateral movement, external data loss, and delivers rapid cyber recovery.

This multi-faceted approach ensures that Commvault meets the most stringent confidentiality, integrity, and availability standards set by government agencies and enterprises alike, along with applicable compliance certifications, so our partners and customers can leverage our services with confidence.

1 State of the Cloud Report | Flexera | 2023
2 Ibid.

COMMVAULT ARCHITECTURE

Commvault is architected for scale and performance with separate control and data planes, with the latter providing features and functionality such as backup job management, data restores, tenant security administration, and more.

The control plane runs in Microsoft Azure and provides a web-based interface for user access. Customer data itself does not flow through the control plane, minimizing network bandwidth requirements.

The data plane encompasses all features and functionality of cyber resilience operations. It ensures that backup data flows can be optimized to secure and manage production data wherever it might reside – on-premises, public cloud, or private cloud.

STORAGE

Commvault has several options for backup storage to help customers meet their RPO and RTO objectives:

Commvault Cloud Air Gap Protect: Fully managed, cloud backup storage. Customers can set policies to place their backup data in specific cloud service provider regions helping meet data residency requirements. Commvault Cloud Air Gap Protect is included in Commvault Cloud Backup & Recovery solutions for Microsoft 365, Dynamics 365, Salesforce, and Endpoints as part of the per user subscription costs.

For hybrid-cloud workloads Commvault offers unique storage target flexibility. Customers can leverage both cloud native storage and local backup copies in concert, for stronger data resiliency and recoverability, including:

· Bring Your Own Cloud Storage: customer cloud, such as Azure, OCI, or AWS
· Commvault Cloud Air Gap Protect: cloud storage target that's fully managed by Commvault
· Bring Your Own On-Premises Storage: customer on-premises server via any disk or NAS device
· Commvault Cloud HyperScale™ X: Commvault appliance used for on-premises backup storage

Figure 3 delineates both primary and secondary storage options for Commvault:

		Secondary Storage							
		Disk	AGP Azure Hot	AGP Azure Cool	AGP OCI Standard	AGP OCI Infrequent	BYOS AZURE	BYOS AWS	BYOS OCI
Primary Storage	Disk	X	✓	✓	✓	✓	✓	✓	✓
	AGP Azure HOT	X	X	✓1	X	X	X	X	X
	AGP OCI Standard	X	X	X	X	✓1	X	X	X
	BYOS AZURE	X	✓2	✓2	X	X	✓2	X	X
	BYOS AWS	X	✓3	✓3	✓3	✓3	X	✓2	✓4
	BYOS OCI	X	X	X	✓2	✓2	X	X	✓2

1 Cross region not allowed
2 Cross regions allowed with warning (By selecting different region for secondary, you will incur inter-region data transfer cost)
3 Cross vendors allowed with warning (By selecting Commvault storage for secondary, you will incur egress charges)
4 Cross vendors allowed with warning (By selecting different cloud provider for secondary, you will incur egress charges)

Figure 3

COMMVAULT SECURITY SOLUTIONS

Bad actors are getting smarter, and bolder. As emerging and sophisticated ransomware attacks pose new threats to businesses, a proactive and well-rounded data security approach has never been more important. Businesses need solutions that both reduces the risk of an attack, while lessening the impact of a successful breach.

That's why Commvault offers security solutions designed to complement your hybrid cloud strategy. How? With a multi-layered, zero-trust security to safeguard endpoints, SaaS applications, and hybrid cloud environments–now and in the future. With Commvault, you get:

- Virtually air-gapped backup copies, isolated from customer environments
- Zero-trust access controls with role-based, SSO, SAML, and multi-authorization protocols
- Real-time insights into at-risk datasets, abnormal behaviors, and suspicious events
- AI-powered anomaly detection, honeypots, and pre-ransomware recovery suggestions
- Rapid cyber recovery, with in-place, out-of-place, item-level, and mass restore options
- Industry-leading best practices built-in, including AE256 encryption, GDPR, ISO27001, and SOC 2 Type 2
- FedRAMP High status, meeting the US government's most stringent data security standards
- Intuitive Commvault Cloud Compliance for legal and regulatory compliance

COMMVAULT CLOUD AIR GAP PROTECT

Ransomware protection is a critical part of an organization's end-to-end security strategy–and necessitates capabilities to detect threats and protect critical copies of data from being compromised. Within any company's strategy, cyber resilience is a last line of defense, and the right path to limiting damage from ransomware attacks is to place the data and infrastructure out of the reach of cybercriminals. Adding air-gapped backup storage infrastructure can make all the difference for quick recoverability.

SaaS-delivered cyber resilience solutions provide a virtual airgap of both backups and restore operations. Backup data copies are stored in isolated, immutable locations–preventing data from being tampered with, altered, or deleted. SaaS-delivered cyber resilience solutions insulate businesses from ransomware attacks that compromise on-premises tools and ensure cyber recovery operations to a clean environment.

Available with both short- and long-term retention options, AGP offers the following benefits to ensure your cloud journey includes exemplary security:

Ransomware and risk reduction

- Virtual air-gapped copy of the data with stringent security protection of Azure cloud
- Encryption and access controls within the Commvault environment for powerful added security to ensure cyber recovery from a ransomware attack

Hybrid cloud adoption

- Beyond a tape library, leverage cloud-based storage and realize the benefits of agile management, limitless scale, and cost savings of cloud
- Easy onramp to cloud for organizations that lack the skills and want to incorporate cloud in their IT strategy

Capacity growth

Meet changing capacity needs on the fly with easy access to cloud

Secondary backup copies

Support the 3, 2, 1 rule: Three copies of the data, two in different locations, and one off-site

Effectively manage cloud costs

Predictable storage costs allow IT to build out long-term forecasting and avoid unexpected bills

COMMVAULT CLOUD THREATWISE

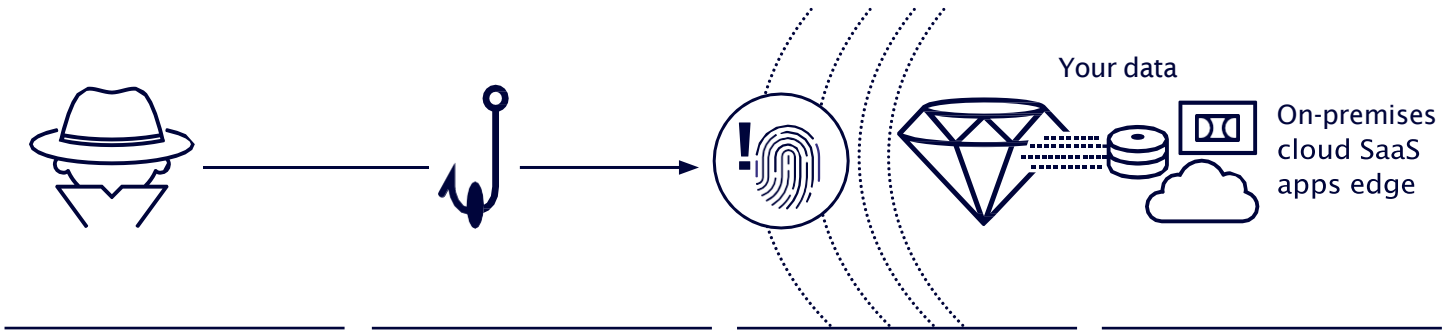
No customer boundary is impenetrable. It's not a matter of if an attacker gets in, but when. As bad actors shift their attention, businesses must also reorient. Companies must reimagine their cyber resiience strategy to focus on proactively responding to threats before their data is compromised, not just recovering from them.

Cyber deception is proven to aid in this effort, equipping businesses with powerful active defense capabilities to secure their data sooner. By disguising itself as legitimate business resources, modern cyber deception solutions engage bad actors the moment an attack begins, in production environments.

By luring bad actors into compromising fake assets, cyber deception provides early warning signals into internal and external threats, exposing unknown and zero-day attacks while empowering businesses to proactively respond to and minimize threats. It is a recognized technology and approach within the defensive MITRE frameworks (MITRE D3FEND and MITRE Engage), demonstrating its efficacy as a countermeasure in the mitigation of cyber risk.

Leveraging patented deception technology, Commvault Cloud ThreatWise changes the game in ransomware protection, combining sophisticated early warning with comprehensive data security. It enables businesses of every size to neutralize silent attacks before they cause harm; detecting and diverting the bad actors which evade conventional security tools and perimeter defenses.

Unlike traditional honeypot technologies, ThreatWise is lightweight, fast and easy–enabling you to dynamically deploy more deceptive assets sooner at a much lower cost. It is purpose-built to directly engage threats–flagging recon, lateral movement, and unwanted privileged access that silently breach defenses (Figure 4). By immediately alerting businesses into attacks in progress, organizations can uncover latent and silent threats traversing environments, before data leakage, encryption, exfiltration, and theft–offering unique multi-layered protection across customer data estates.



1 Deploy fake resources and decoys, indistinguishable to attackers	2 Divert and lure bad actors into engaging false assets	3 Spot threats without false positives or alert fatigue	4 Remediate threats before they reach your data
Flawlessly replicate high value assets	Engage and surface attackers in real-time	Get instant and early visibility into threats	Rapidly scale, to protect your entire surface area

Figure 4

COMMVAULT CLOUD THREATWISE SECURITY IQ FOR THREAT MONITORING

Commvault Cloud ThreatWise Security IQ (Figure 5) provides customers with advanced tools and unprecedented visibility into backup environments. Seamlessly integrated across the entire Commvault portfolio, Security IQ offers a single place for IT admins to quickly bolster security posture, identify risks in real-time, and rapidly recover data. With Security IQ, you can drive better security outcomes by scoring and validating security posture against native controls and parameters, enabling:

- Monitoring potential ransomware activity via unauthorized modifications to configurations, restores, and user logins
- Rolling data back to pre-ransomware states
- Tracking abnormal conditions and behaviors for deeper insight into unwarranted changes on backup data
- Dataset isolation, to recover without reinfection

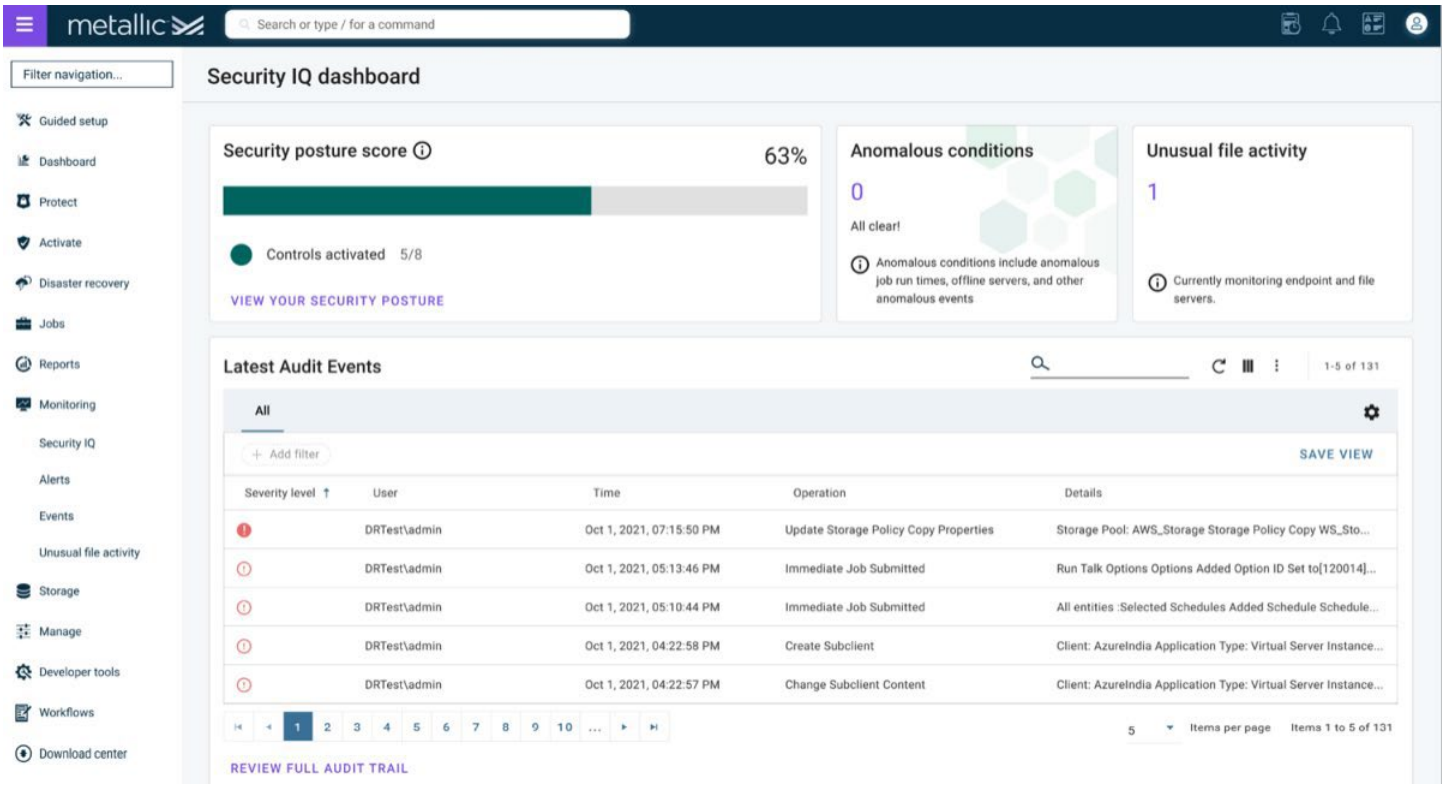


Figure 5

FINAL CONCLUSIONS

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

Stay SaaS protected

SaaS-delivered cyber resilience has become one of the primary approaches for modern enterprises for good reason. The shared responsibility model for managing both hybrid cloud and SaaS applications 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 protect data from the 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 data backup and recovery capabilities is a seamless option. Look for a comprehensive solution like Commvault to ensure broad coverage within each application and workload.

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 cloud platforms for long-term data retention and air-gapped ransomware protection as needed. SaaS-delivered 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 solutions. Thanks to Commvault 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.

Start planning tomorrow's migrations 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 be many and varied.

By anticipating where your data will be processed, you can ensure the cyber resilience solutions are already in place to keep data secure whether at rest or in flight. In addition, putting your data security 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.

Keep your app journey secure end-to-end

As you transition from traditional application platforms to containerized approaches such as Kubernetes, your cyber resilience and data security must remain a top priority. With stateful enterprise applications moving into containers, the security 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 also offers SaaS-delivered cyber resilience for Kubernetes, supporting all CNCF-certified distributions.

Engage centralized management

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

Commvault provides this critical visibility and simplified workload with the ability to manage any data, anywhere, all from one console. Integration with Commvault Cloud Complete Data Protection through a central console means customers can select both SaaS-and self-managed solutions if their strategy requires, and still enjoy industry-leading technology. With HyperScale X, companies can store backups locally for speedy recovery of large on-premises data sets. You get everything you need to modernize your cloud journey from a single vendor.

SUMMARY

As discussed, hybrid cloud security is a complex topic, but it doesn't have to be with Commvault. We know you many have questions about how to secure, defend, and recover your data. We encourage you to **contact your partner** for a personal introduction and discussion to help you get started today!