Enterprise Strategy Group by TechTarget

TECHNICAL SUMMARY

JUNE 2024

A Roadmap to Future-proof Cyber Resilience with Commvault Cloud, Powered by Metallic AI: Elements of a Blueprint

Tony Palmer, Principal Analyst and Practice Director

Read the full Technical Review **HERE**.

Abstract: This Technical Summary of the Technical Review by TechTarget's Enterprise Strategy Group outlines the areas organizations should consider when redefining their approach to cyber resilience, with an end goal of future-proofing their approach and its resulting impact. In the Enterprise Strategy Group Economic Validation "Analyzing the Economic Benefits of Cyber Resilience With Commvault Cloud,"[1] published in November 2023, our analysts interviewed Commvault customers to understand the impact that Commvault Cloud, powered by Metallic AI, can have on an organization's ability to reach IT and business goals. This Technical Summary is designed as a companion to the Economic Validation, providing a framework of criteria to assist organizations in achieving results similar to the significant business and financial impact reported by customers and documented in the Economic Validation.

Building a Blueprint for Cyber Resilience—Key Considerations for an Effective Roadmap

To achieve effective cyber resilience, organizations need to understand their business's needs and their risk tolerance. Requirements shouldn't be based on the capabilities of the tools that businesses already own, but instead on the desired outcomes. Key consideration areas include:

- **Improving business continuity.** The familiar, long-established process of keeping a business up and running after a system outage or natural disaster has been changed by ransomware. In many cases, malicious code malicious code is often embedded in the systems organizations use for recovery, allowing attackers access even after a full recovery. Data security products often back up and protect that same infrastructure code, so at the time of recovery, the malicious code is also restored back into the production environment. In short, ransomware has changed the face of recovery, and recovering malicious code can make things worse. Organizations should implement solutions that ensure clean recovery—including clean data *and* recovery locations.
- **Reducing complexity.** While point-product solutions can protect some workloads and appear easy to deploy, a growing technology stack further fragments operations and siloes data, while requiring additional operational skill sets and infrastructure requirements—all adding to unneeded, burdensome complexity. Organizations should implement a solution that has the ability to span across all data workloads and all types of infrastructure, reducing complexity and simplifying cyber resilience and cybersecurity processes.
- **Eliminating costs.** Complexity drives up the cost of cyber resilience and data protection, which can be hard to justify against increasing budgetary constraints. The complexity that grows with each added point product, tool, or workload can uncover hidden costs. Organizations need a predictable and efficient cost structure when modernizing—a foundation they can use to optimize their entire hybrid cloud environment and reduce overall spending.

[1] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Cyber Resilience with Commvault on Microsoft Azure*, November 2023. All Enterprise Strategy Group research references in this technical summary are from this economic validation.

This Enterprise Strategy Group Technical Summary was commissioned by Microsoft and Commvault and is distributed under license from TechTarget, Inc.

- **Minimizing risk.** Pervasive and autonomous threats take advantage of gaps in the infrastructure. Identifying and eliminating these vulnerabilities is critical to reducing risk. Identifying areas of increased risk and how to reduce it is a key requirement for cyber resilience. Organizations need an upfront assessment of the data and the requirements and insight into how cyber resilience is currently being addressed, with collaboration and communication across teams, from line-of-business owners to application teams to security operations (SecOps) and IT administrators. In this way, organizations can obtain a holistic view of their data ecosystem to create a coherent strategy and prioritize actions.
- **Recovery preparedness.** Organizations also need to assess their preparedness to recover when needed. Periodic, successful testing, which many organizations have found hard to achieve, document, and validate, is essential to a comprehensive and executable cyber resilience strategy and working plan.
- **Enhancing agility.** Hybrid environments introduce security risks to the IT environment. Organizations need to be able to adapt to this change without the compromises caused by the challenges of integrating disparate tools and technologies. Reducing the number of solutions within the environment for cyber resilience will increase an organization's agility. Decoupling the data from the infrastructure it resides on can also significantly enhance agility, creating true data portability while also freeing up resources to focus on innovation and business value-centered initiatives.
- **Removing technical debt.** Technical debt and a continued need for team members to maintain skill sets required to keep both legacy and more recently added point solutions operational forces organizations to prioritize these needs over innovation, stifling efforts to modernize. Technical debt is the consequence of prioritizing keeping deployed systems functional when making IT decisions. This results in the depletion of a portion of ongoing IT budgets, limiting interoperability with new systems. Moving to a comprehensive single cyber resilience platform can significantly reduce technical debt while putting the organization on a path of eliminating the creation of new technical debt.
- **Meeting sustainability goals.** As sustainability becomes a top priority for CIOs and boards over the next few years, organizations need to look to cyber resilience solutions that drive reductions in power consumption. Reducing power consumption in cyber resilience and data protection can offset power consumption in other areas of operations.

Conclusion

Enterprise Strategy Group validated that Commvault Cloud takes what it learns about the environment through embedded AI technology and uses it to help organizations better understand their workloads and create recommendations for adjustments to their cyber resilience approach. Commvault Cloud also provides a roadmap for seamless transformation to SaaS data protection, which can significantly enhance an organization's cyber resilience, data security posture and sustainability results, all while providing a much more predictable cost structure and better TCO when compared with alternative environments.

Read the full Technical Review **HERE**.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com