Enterprise Strategy Group by TechTarget

TECHNICAL REVIEW

FEBRUARY 2024

A Roadmap to Future-proof Cyber Resilience With Commvault Cloud, Powered by Metallic AI

Tony Palmer, Principal Validation Analyst

Abstract

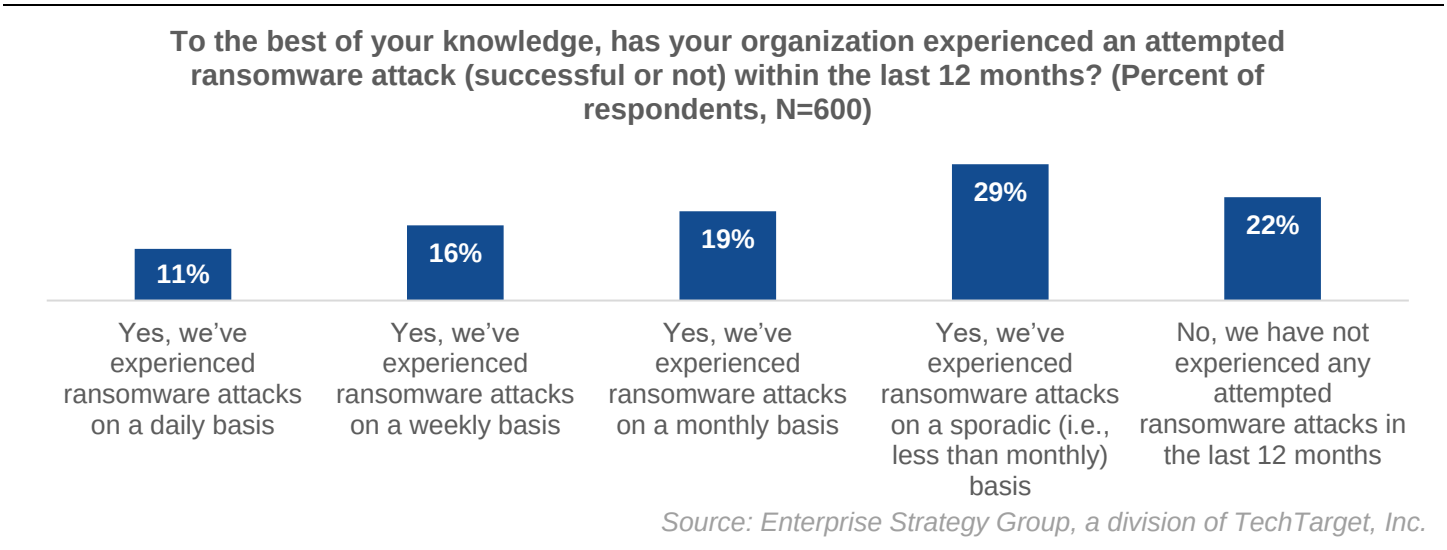
This Technical Review by TechTarget's Enterprise Strategy Group outlines the areas organizations should consider when redefining their approach to cyber resilience, with an end goal of future-proofing their strategy and improving their ability to detect, prevent, and rapidly recover from cyberthreats and attacks.

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 Review 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 documented in the Economic Validation.

The Challenges of Cyber Resilience and Cybersecurity

Organizations are challenged by the fact that effective cyber resilience capabilities become exponentially more complex in distributed hybrid and multi-cloud environments. Enterprise Strategy Group research found that 75% of surveyed organizations reported at least one ransomware attack within the last 12 months (see Figure 1).[2]

Figure 1. Ransomware Attack Frequency Over the Previous Year



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Cyber Resilience With Commvault Cloud*, November 2023.
[2] Source: Enterprise Strategy Group Complete Survey Results, *2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, November 2023.

Attacks damage organizations in many ways, with the cost of an attack going far beyond just the ransom. Data exposure, data loss, and operational disruption all contribute to the financial, compliance, and reputational exposure and damage of ransomware attacks. In the same survey, more than half (56%) of organizations said they paid the ransom in hopes of minimizing disruption and further damage. Of the organizations who paid, 85% reported additional extortion attempts, and more than half of them paid to avoid public data exposure and other consequences.[3]

Improving operational resilience against cyberattacks is critical, as businesses depend more heavily on data for business and mission-critical operations. Paying a ransom in no way guarantees that data will actually be returned, or in a usable state if returned, making a sound strategy and executable plan for cyber resilience an organization's best line of defense.

Cyber resilience is critical, but resilience comes at a cost, and organizations need to consider the real total cost of ownership (TCO) as they reassess and rearchitect their cyber-resilience and data protection strategies.

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 should not be based on the capabilities of the tools that businesses already own, but instead on their 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 can be embedded in the systems organizations use for recovery, allowing attackers access even after a full recovery. Organizations should implement solutions that ensure clean recovery—including clean data *and* recovery locations in order to pursue a robust, adaptable approach to resilience.
- **Minimizing risk—**Pervasive and autonomous threats take advantage of gaps in infrastructure. Identifying and eliminating these vulnerabilities is critical to reducing risk. Identifying areas of increased risk and how to reduce them is a key requirement for cyber resilience. Organizations need an upfront assessment of the data to identify gaps and insight into how cyber resilience is currently being addressed. In this way, organizations can obtain a holistic view of their data ecosystem to create a coherent strategy and prioritize actions.
- **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 complexity. Organizations should look to 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 while improving their cyber resilience, cybersecurity, and data availability.
- **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 can introduce security risks to the IT environment. Organizations need to be able to adapt to this 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 simplify operations and increase an organization's agility. Decoupling the data from the infrastructure it resides

[3] Ibid.

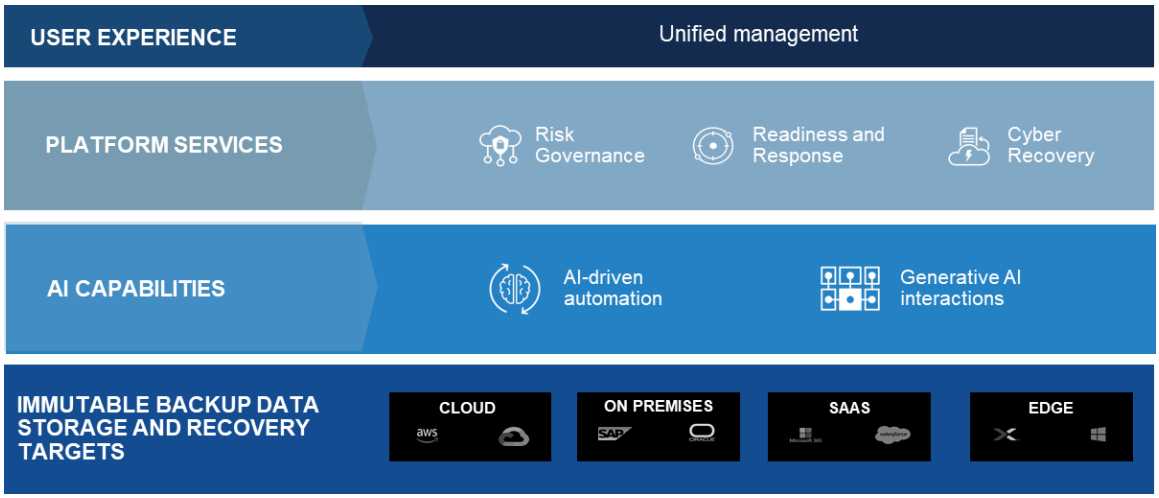
on can also significantly enhance agility, creating true data portability while freeing up resources to focus on business value centered initiatives.

- **Removing technical debt—**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, prolonging the challenge of interoperability with new systems. Moving to a comprehensive, single cyber resilience platform can significantly reduce existing 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.

The Solution: Commvault Cloud Powered by Metallic AI

Commvault developed Commvault Cloud, powered by Metallic AI to deliver enterprise-grade data protection with the simplicity of SaaS as well as tight integrations into the leading data security ecosystem tools in place across today's enterprises. Commvault Cloud is a cornerstone for data protection transformation and delivers a next-generation cloud-based solution, developed specifically for safeguarding data distributed across the hybrid enterprise. As shown in Figure 2, Commvault Cloud provides the protection that has always been the backbone of Commvault, while eliminating much of the complexity that can come with today's multidimensional environments that include elements of on-premises, SaaS, cloud-native, and hybrid environments.

Figure 2. The Commvault Cloud Platform



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group Analysis

This Technical Review by Enterprise Strategy Group explores the benefits that organizations can realize when using Commvault Cloud to integrate cyber resilience, data security, and cybersecurity with data protection across distributed, hybrid cloud environments. We explore how working with Commvault can help organizations design and implement their own roadmap to simplified yet comprehensive cyber resilience.

Reducing Complexity and Costs

Enterprise Strategy Group evaluated how Commvault Cloud reduces bottom-line costs for data protection and cyber resilience. We focused on how Commvault Cloud helps organizations effectively streamline and consolidate operations and tools and how this enables organizations to shift resources closer to the customer to focus on their needs and engage in revenue-producing activities instead of managing multiple back-end tools.

Figure 3. Consolidated Automation and Cyber-resilience Tools and Capabilities

Source: Commvault and Enterprise Strategy Group, a division of TechTarget, Inc.

As shown in Figure 3, Commvault provides multiple integrated capabilities that consolidate the functionality of many individual, often very expensive tools:

- **Unified management—**Users see, secure, and recover data everywhere from a central control plane, providing a single source of truth with a consistent experience for everyone, regardless of the workload and environment.
- **Risk governance—**Users can proactively find and remediate risks to improve data security posture. This includes capabilities to help discover, classify, and protect sensitive data and the ability to detect threats and unusual activity in that data. Commvault Cloud is designed to ensure organizations can securely recover data by identifying the last known clean copies to help avoid any potential reinfection. Additionally, organizations have the information to facilitate efficient compliance and prove this data is unaltered.
- **Readiness and response—**Early warning, automated validation, and continual recovery testing are key elements of readiness and response. Manually planning incident response is complex, and hybrid workloads increase that complexity. Using advanced AI, Commvault Cloud offers intelligent decoys that mimic and behave like legitimate assets to give early warning of threats. With Cleanroom Recovery functionality, organizations benefit from air-gapped cloud storage for data backups, plus the ability to test and prepare for recovery with cloud-ready recovery targets.
- **Cyber recovery—**Commvault Cloud capabilities are engineered to ensure predictable, scalable, and rapid recoveries. Cleanroom Recovery capabilities enable users to not only test and prepare ahead of time, but also ensure safe recovery to a cleanroom—a secure, isolated environment—in the cloud when an incident occurs.
- **Artificial intelligence (AI)—**AI is not new to Commvault. They have incorporated AI, machine learning, natural language processing, and heuristics to help customers accelerate recovery with threat scanning, remediation, intelligent quarantining, and clean recovery validation. Commvault uses AI to drive intelligent automation with:

  - **Advanced threat prediction—**Utilizes real-time predictive threat analysis to find AI-driven ransomware, including detection of shape-shifting AI malware, before it can affect customers' backups and their ability to recover cleanly.
  - **Cloudburst recovery—**Utilizes infrastructure as code and cloud scaling to automate rapid and frictionless recovery of data to any location. Users benefit from portability, as well as a low TCO as a result of the accelerated process.
- **Commvault Cloud Copilot—**Commvault Cloud empowers users with a new AI copilot offered under the name Arlie—short for *autonomous resilience*—which responds to inquiries from users in plain language and can quickly consolidate information and provide actionable responses to help save time. For example, users may be able to use Arlie to verify or validate a clean point of recovery for critical systems or generate requested code in seconds. New AI-enabled capabilities support this type of personal/human interaction within Commvault Cloud.

Organizations have numerous data requirements that have traditionally been very expensive to address. Finding and producing data for e-discovery, implementing controls for stringent compliance frameworks like GDPR, and replicating data for business continuance are just three examples where enterprises would need to spend six to seven figures on separate point solutions. Commvault Cloud can address all these use cases and more in one, unified offering.

Why This Matters

Multiple, diverse backup applications and legacy point solutions increase costs and make it unnecessarily more difficult to control and protect data. Financial models from Enterprise Strategy Group's Economic Validation found that Commvault Cloud, powered by Metallic AI, helps reduce data duplication and data silos, leading to reduced costs and the elimination of technical debt.

Enterprise Strategy Group's Economic Validation showed that Commvault Cloud can provide a much more predictable cost structure when compared to alternative environments. Companies leveraging Commvault's blueprint achieved up to 82% lower administrative costs and a 31% reduction in storage costs with Commvault Cloud.[4]

Minimizing Risk

Commvault Cloud integrates Commvault's SaaS solution (formerly called Metallic) with its software solution, providing a unified control plane designed for ease of use at scale with advanced capabilities. This gives organizations of any size cyber resilience and cyber recovery without the complexity of using numerous protection tools and point solutions from multiple vendors. Data classification capabilities make it possible to prioritize security efforts and reduce the impact of cyber incidents.

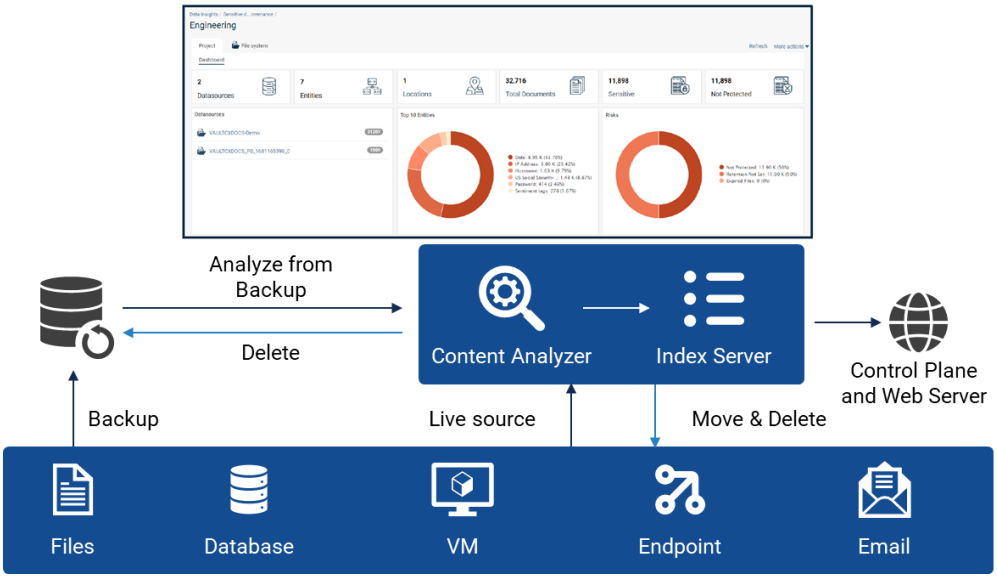
- Certainty of data ownership information minimizes the risk of data exfiltration.
- Reducing redundant data lowers the risk footprint and the overall impact of data breaches.
- User-defined tags aid in quicker remediation and tracking of sensitive information.

SecOps analysts need to know what types of sensitive files are present in the environment, which departments own them, and what risks they pose. This knowledge enables SecOps teams to take proactive remediation actions. The responsibility for providing this intelligence falls on the IT administration team, which needs to share reports of sensitive file locations in the environment to the SecOps team. As shown in Figure 4, Commvault Cloud identifies

[4] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Cyber Resilience With Commvault Cloud*, November 2023.

and classifies sensitive data across on-premises and cloud locations, scanning sensitive data across multiple data types, including images using predefined entities for HIPAA, GDPR, and other compliance frameworks, as well as custom entities for additional personally identifiable information scans.

Figure 4. Commvault Indexing Architecture-Inventory and Risk Analysis



Source: Commvault and Enterprise Strategy Group, a division of TechTarget, Inc.

Commvault Cloud's single-user interface is used to access all analysis and insights. Organizations can monitor for any changes to sensitive data or its access and assess risk based on sensitivity and impact. Administrators and analysts can review file access and privileges, monitor orphan data and files in the environment, and identify redundant, obsolete, and trivial data to identify data sprawl and duplication. Commvault also helps organizations adjust user permissions for sensitive data in bulk and archive sensitive data for compliance regulations. Storage trend reports with tags help drive archiving decisions to further reduce data sprawl.

Commvault Cloud's zero-trust architecture and security controls and protocols have enabled it to earn FedRAMP "High" status—Commvault asserts that this is unique among data protection platforms—which means it has passed extensive testing and review to meet the highest security standards recognized by the U.S. government. In addition to FedRAMP, Commvault Cloud is also Criminal Justice Information Services (CJIS) and Federal Information Processing Standards (FIPS)140-2 compliant.

Why This Matters

Commvault risk analysis enables organizations to identify, analyze, manage, and secure sensitive data in the environment to reduce data breach impact.

Enterprise Strategy Group validated that Commvault risk analysis simplifies how organizations can prioritize security efforts and reduce the impact of security incidents across multiple use cases. Organizations use data ownership information to minimize the risk of data exfiltration, while reducing redundant data shrinks the risk footprint and the overall impact of data breaches, and user-defined tags accelerate remediation and simplify tracking of sensitive information.

Commvault Cloud's broad workload coverage enables organizations to enhance their cyber resilience with a single platform that covers all data and all applications, regardless of where the data resides. Enterprise

Strategy Group's Economic Validation showed Commvault Cloud can significantly reduce data loss that can occur when a cyberattack takes place, increasing the percentage of recoverable data to more than 99%.[5]

Agility

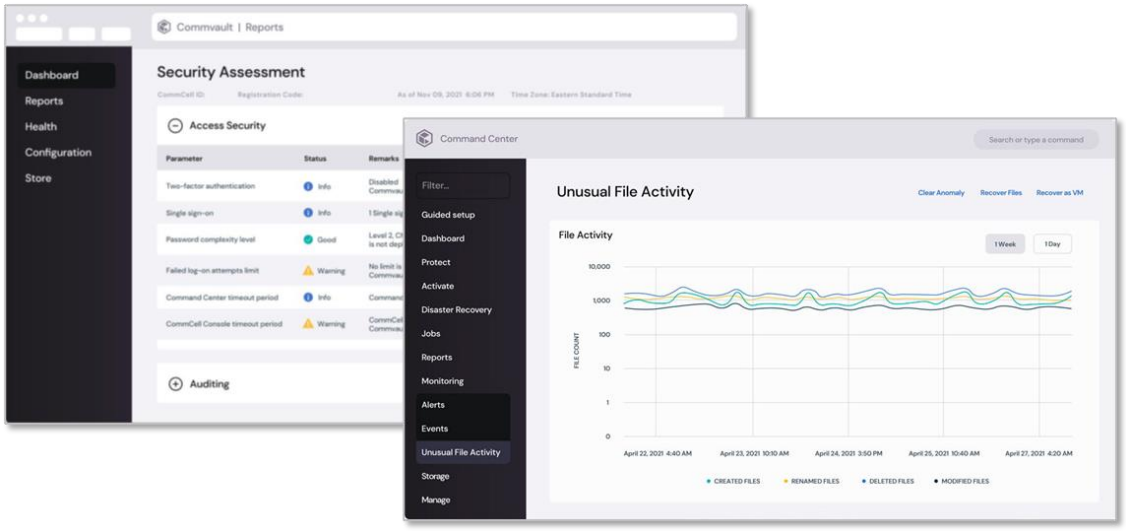
Managing complex environments' data protection and cyber resilience with multiple heterogeneous tools introduces complexity, which increases the likelihood of human error that results in nonrecoverable data. Commvault provides a comprehensive tool—powered by AI—that can provide unified insights, helping organizations monitor and maintain recovery readiness and accelerating the return to normal business operations in the event of incidents and critical outages.

A common foundation for these strategies is the NIST Cybersecurity Framework: standards, guidelines, and best practices to manage cybersecurity-related risk. NIST designed the framework to provide a prioritized, flexible, and cost-effective approach to promote the protection and resilience of IT infrastructure. Commvault Cloud supports the NIST Cybersecurity Framework and also integrates with leading cybersecurity tools, including Microsoft Sentinel, Microsoft Defender, and others, enabling the sharing of intelligence and the ability of Commvault Cloud to act on millions of threat detection signals, while also sharing intelligence back to these tools.

Commvault's data platform employs AI to assess data protection needs in real time, analyzing data growth trends over time, forecasting the required compute resources to meet defined service-level agreements, and making automated decisions to scale compute resources up or down as needed.

The Security Assessment Dashboard (see Figure 5) provides insights and recommendations to quickly build action plans. Recommended controls and settings can be found in the dashboard and easily implemented using interactive actions. Commvault has built a layered antimalware and ransomware strategy into existing security software and policies while reducing management overhead.

Figure 5. Commvault Security Assessment Dashboard and Unusual File Activity Monitoring



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[5] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Cyber Resilience With Commvault Cloud*, November 2023.

From monitoring file system activity and honeypot files to security information and event management integration, to certificate authentication lockdown and actionable alerting, Commvault provides the tools needed to simplify recovery readiness.

Why This Matters

Enterprise Strategy Group found that Commvault Cloud offers an environment in which it is easier to discover, manage, and protect data, regardless of where the data resides. Commvault Cloud runs in the cloud but addresses the importance of protecting on-premises workloads. This flexibility gives organizations the agility to adapt to changing requirements.

Commvault Cloud offers the ability to react to change rapidly, enabling organizations to capitalize on business opportunities, especially when it comes to the integration of data environments and infrastructure, leading to enhanced agility. For organizations that grow through acquisition, the ESG Economic Validation found that organizations that deploy Commvault Cloud for cyber resilience can fully integrate cyber resilience into newly acquired environments in one day, as compared to an average of four to five months to fully enable data protection in the newly acquired environment prior to deploying Commvault Cloud.[6]

Reducing Technical Debt

By removing point solutions that have limited workload coverage, organizations can rapidly eliminate existing technical debt, while avoiding the accumulation of additional technical debt. Commvault Cloud's broad workload coverage brings the ability to eliminate significant amounts of technical debt.

Why This Matters

Enterprise Strategy Group found that Commvault Cloud offers an environment in which organizations can displace numerous data protection solutions and their required hardware and infrastructure, along with the need for specialized skill sets for operations and maintenance. This component of technical debt is often overlooked as compared with the more visible and more easily measured hardware and infrastructure costs.

The Economic Validation found that, on average, companies had more than 15 backup products running in their environment, all of which were ultimately replaced by Commvault Cloud. Not only did deploying Commvault Cloud help reduce staff requirements, resulting in an 82% savings in full-time equivalent hours dedicated to backup processes; deploying Commvault Cloud also resulted in a 31% reduction in storage costs through reduction of the overall data footprint.[7]

Meeting Sustainability Mandates

Nearly all (97%) of organizations with established environmental, social, and governance (ESG) programs told Enterprise Strategy Group that ESG has more than a marginal impact on their organization's strategic planning. Indeed, for nearly six in ten organizations (59%) that had ESG policies and procedures in place, ESG has had a *significant* impact on strategic planning.[8] Organizations with ESG programs think and act differently than those without ESG. Clearly, ESG is a business strategy-level concern. It should come as no surprise that CIOs and CEOs alike are being held accountable to meet critical environmental and sustainability goals.

[6] Ibid.
[7] Ibid.
[8] Source: Enterprise Strategy Group Complete Survey Results, *The Role of ESG Programs in IT Decision Making*, September 2022.

Why This Matters

Enterprise Strategy Group found that Commvault Cloud can help organizations meet and exceed sustainability goals, with the potential of being net carbon negative in data protection by 2030, while offsetting power usage in their core business, further helping to accelerate meeting sustainability goals.

Conclusion

Cyber resilience has always been a challenging activity, and traditional approaches to administering the task have become unsupportable and are limiting business agility while exacerbating the risks of nonrecoverable data loss.

Commvault Cloud is cloud-architected infrastructure, so regardless of where an organization's data resides—on premises, in a private cloud, or in a public cloud—Commvault Cloud enables cost-efficient data resilience and recovery with ease of data portability, enabling businesses to be competitive, agile, and flexible without compromising resiliency.

Enterprise Strategy Group found that Commvault Cloud simplifies an extremely complex task while providing capabilities to replace multiple backup systems. Using a single, unified interface to automate many of the manual tasks associated with backing up and restoring data enables organizations to get a holistic view of the data ecosystem and shifts the focus from troubleshooting daily errors to finding ways to better support business groups, while improving their cyber resilience and data security posture.

According to customers who participated in Enterprise Strategy Group's Economic Validation, Commvault Cloud can provide a much more predictable cost structure and better TCO when compared with alternative environments.[9] When organizations can collapse many different tools with independent interfaces into one, they get a better understanding of their data and how they use it, without the expense of purchasing and maintaining multiple disparate tools. Companies leveraging Commvault's blueprint achieved up to 82% lower administrative costs and a 31% reduction in storage costs with Commvault Cloud, driving reduced complexity, increased data resilience, improved data restorability, and reduced risk.[10] Commvault Cloud has helped almost every customer we interviewed through a total transformation of their data protection. The more workloads for which a customer has made the move to Commvault Cloud, the farther along the customer is toward a complete transformation that brings with it lower costs, increased data agility, and significantly enhanced data security and cyber resilience—along with the parallel benefit of reducing their technical debt and enabling them to better achieve cloud optimization.

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. The more data that is collected and analyzed, the smarter the system gets, and the better the recommendations and decisions it makes, which, in turn, makes IT, security, and data protection teams more agile and responsive to the needs of the business.

Enterprise Strategy Group validated that Commvault Cloud gives organizations a roadmap for seamless transformation to SaaS data protection while significantly enhancing an organization's cyber resilience, data security posture, and sustainability results.

If your organization is looking for a solution that can replace legacy solutions and multiple current tools that are not able to provide cyber resilience and cybersecurity across all workloads with one tool that simplifies data protection, cyber resilience, and cyber-recovery, you should be talking to Commvault about Commvault Cloud.

---

[9] Source: Enterprise Strategy Group Economic Validation, *Analyzing the Economic Benefits of Cyber Resilience With Commvault Cloud*, November 2023
[10] Ibid.

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