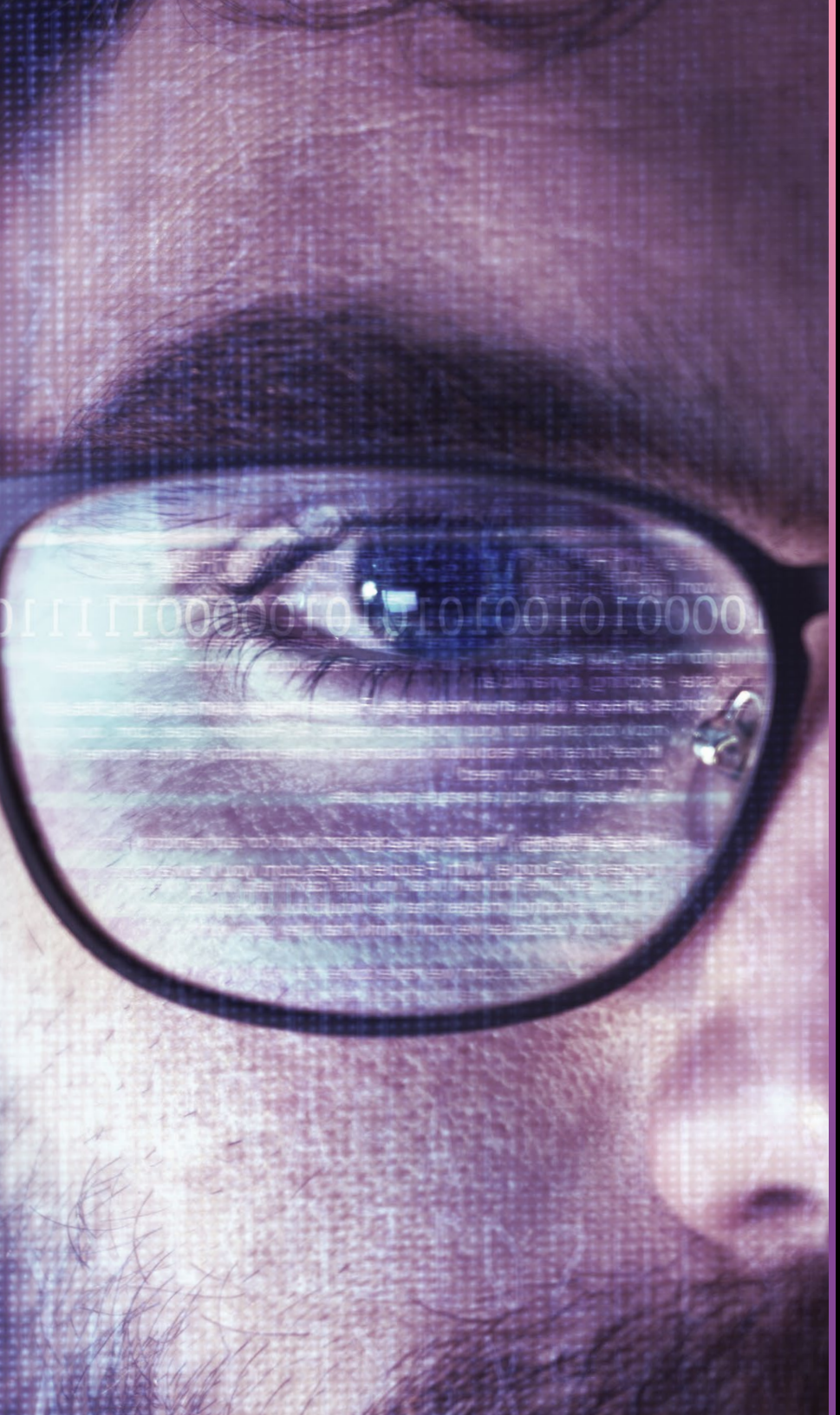

Commvault

eBOOK

Architectural Principles for Cyber Resilience

CONTENTS

DATA IN THE ERA OF CYBER RESILIENCE

Data has become an essential component of modern business operations and strategy.

However, with global data generation on track to surpass industry predictions of 175 zettabytes by 2025[1] effective data protection has become one of the most pressing challenges for organizations across all industries.

The complexity of the issue is compounded by the fact that traditional approaches to safeguarding data are often ill-prepared to handle the sheer volume of information being generated or be able to recover this data quickly enough in the event of a cyber incident.

As we continue to generate and accumulate data at an unprecedented pace, it's crucial to understand the need for solutions that are optimized to work with your existing IT architecture, designed to handle the data load, and minimize the risk of data breaches and cyberattacks.

Commvault®

1 David, R., John, G. and John, R. (2018) The Digitization of the World, from Edge to Core. An IDC White Paper-#US44413318, Sponsored by Seagate. https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

THE RISE OF TELEMETRY DATA AND THE CONSEQUENCES OF DATA LOSS

With the emergence of telemetry data in the modern business landscape, data protection has become more critical than ever before.

This telemetry data plays a pivotal role in driving business applications and decision-making processes. However, with such a large influx of data, the traditional approach was to store it in data lakes, which was considered the go-to solution for storing vast amounts of unrefined data. However, these data lakes often remained unguarded, with the data within them existing without adequate safeguards. This lack of security and protection is a significant concern, especially in today's digital age, where cyber threats like ransomware and data breaches are on the rise.

Organizations are now grappling with the reality that the data amassed in these lakes—which is vital for strategic decision-making—is at risk of being compromised. The potential loss of such critical information can have far-reaching consequences, including significant financial losses and reputational damage.

In the past, replication was considered a reliable disaster recovery measure; however, with the rapid advancements in technology, it is no longer sufficient to only safeguard against data loss. The merging and purging of business-critical data in a storage space-constrained environment makes the loss of such data both catastrophic and irrecoverable. The traditional storage-based replication systems, created during the early days of big data, now struggle under the weight of data they were meant to protect.

Recovering from a cyberattack is more complex than simple data recovery. It involves restoring not only the compromised or lost data but also the systems and applications affected by the attack. This process can be time-consuming and challenging due to the vast amount of data that needs to be recovered. Restoring thousands of terabytes of data over a smaller production network and disks can be impossible, as these disks and networks are designed to handle peak production usage levels much lower than what's required for a full restore at high speed.

When protecting such critical data, the shortcomings of conventional recovery models are becoming increasingly evident. Organizations must adopt more advanced and robust disaster recovery solutions for business continuity and prevent data loss.

UNDERSTANDING YOUR IT NEEDS BEFORE CHOOSING PROTECTION

The data protection strategy must now align with the intricacies of modern IT landscapes. Before you start exploring the vast array of data protection solutions available, a crucial step is comprehensively understanding your existing IT architecture's capacities and limitations. This introspective analysis should include evaluating the existing capabilities, identifying data protection needs, establishing a forensic strategy, articulating expected post-cyber incident outcomes, and identifying potential bottlenecks within the architecture.

Evaluating current capabilities should include assessing the current state of hardware and software and analyzing the existing security protocols and procedures. This will help identify potential vulnerabilities that must be addressed before implementing a data protection strategy.

Defining Needs

Defining data protection needs is another crucial step in this process. This involves identifying the types of data that require protection, the level of protection needed, and the potential risks to the business associated with each type of data.

Forensic Strategy

Establishing a forensic strategy across disparate infrastructure is also essential to data protection. This involves having a plan in place for identifying and responding to cyber incidents, including how to gather evidence, contain the incident, and restore normal operations.

Incident Outcomes

It is equally important to articulate expected post-cyber incident outcomes, which involves defining the desired outcomes in the event of a cyber attack, such as minimizing data loss or downtime.

Architectural Limitations

Finally, identifying potential limitations within the architecture is crucial for optimizing the data protection strategy. This could include analyzing the network infrastructure, software applications, and data storage systems to ensure they can support your organization's recovery needs and are compatible with the data protection solutions claims.

THE DISPERSED ECOSYSTEM OF PROTECTION

Navigating the dispersed and diverse IT ecosystem demands a data protection solution that is not just a one-size-fits-all offering.

While hyperconverged infrastructure (HCI) is often considered an easy-to-deploy solution, it may have limitations that are not considered beyond deployment. Certain limitations of HCI, such as data transfer speeds per node, can considerably impact the effectiveness of a data protection strategy, especially when it comes to robust data recovery.

Considering the challenges that arise after deployment, such as upgrades, patching, adding nodes, cluster sizes, and data loss tolerance is essential. It's crucial not to compromise on data protection needs to achieve simplicity in deployment, as the consequences of data loss and delayed recovery can be catastrophic for any organization. Therefore, evaluating the data protection solution's capabilities is essential to ensure it meets the organization's needs and architecture rather than settling for a one-size-fits-all approach that may not provide adequate protection during or after a cyberattack.

Many HCI solutions require customers to standardize on specific technologies or form factors, resulting in vendor lock-in, increased complexity and costs, inefficient data recovery, cyber resilience and testing challenges, and inadequate support for hybrid workloads. These limitations restrict an organization's agility, increase operational costs, and compromise data protection and recovery capabilities. It is essential to confirm that any evaluated HCI platform allows you to easily migrate data into and out of the platform, allowing for data portability from any platform to any other platform. Storing the data in an agnostic format can improve the ability of organizations to future-proof their cyber resilience strategies.

UNLOCKING THE FULL POTENTIAL OF CYBER RESILIENCE WITH COMMVAULT

At Commvault, our software-driven model allows us to utilize the latest cutting-edge technologies.

Unlike alternatives that rely on appliance-based solutions, we believe that our hardware-agnostic approach is one of our significant advantages. Our solutions are not tied to specific hardware, making them highly adaptive and flexible to various customer environments. This flexibility is critical in meeting our clients' service level agreements (SLAs) as it allows us to tailor our solutions to their individual needs.

However, safeguarding your data from potential threats is not enough; it's also about preparing for what's next. Investing in a flexible and fully functional data protection solution like Commvault is crucial to achieving this level of preparedness.

Taking the time to design the right solution during initial setup is far better than replacing your system in the future when it no longer meets your business's requirements or falls short of your expected outcomes.

With Commvault, you can protect and recover your data from virtually any source, including cloud, virtual, and physical environments. Our solutions offer comprehensive protection against cyber threats, help ensure fast and reliable data recovery, and simplify data protection management across your organization with complete visibility and control over your data.

This enables you to manage your data efficiently and securely, no matter where it resides. It gives you the confidence you need in your data recovery capabilities, even in the face of the most malicious cyberattacks. Commvault also gives you the flexibility to scale your data protection needs as your organization grows, helping safeguard your investment's relevancy for years to come.

The architecture of Commvault Cloud is unique in design with decoupled layers, including the Control Plane, the Data Plane, and the Storage Plane. This structure offers superior protection capabilities compared to appliance-based solutions, as it employs a multi-layered and robust approach to data security. The architecture enables backup data to be stored securely, with operations and backup copies kept in an isolated, virtually air-gapped environment, separate from the source environments. This isolation is crucial in safeguarding against various threats and helps ensure backup copies are recoverable even in the case of accidental deletion or malicious attacks.

HOW DOES COMMVAULT CLOUD DELIVER TRUE, CLOUD CYBER RESILIENCE?

Data Plane Separation

Resilient architecture

Comprehensive Security

Securing more workloads than any other provider

Any-to-Any Portability

Predictable, reliable recovery, from any location to any location

Risk Remediation

Automated risk scanning and remediation across live and backup data

Early Warning

Leverage AI to identify threats, maximize impact and accelerate recovery

Cleanroom Recovery

Recover without the risk

COMPETITIVE COMPARISON

- × Control planes are NOT separate
- × Requires additional products for complete coverage
- × Tied to storage architecture
- × NO Data Security Posture Management
- × Reactive detection limited to backup data
- × Risky business on your own without Cleanroom Recovery

COMPLEXITY VS. BUSINESS VALUE

The topic of complexity vs. business value is critical in today's hybrid landscape.

When safeguarding sensitive data, organizations must weigh the perceived complexities of deploying a robust data protection system against the value it delivers to their business. Simplification is not always the best option if it comes at the cost of capabilities. Commvault understands this and provides a layered defense approach that culminates in agility and recovery speed, which can be the difference between mere survival and sustained success in the face of cyberattacks.

To confront the complexities of data protection in the modern era, businesses must have a holistic understanding of the role of IT architecture. This requires a strategic partnership with agile, intelligent, and robust solutions. The burden of data protection no longer lies with the replication and recovery models of the past. It requires a shift towards solutions as dynamic as the data they protect.

By collectively acknowledging the hidden challenges within data practices and rising to the task with innovative and forward-thinking partnerships, we can protect your organization's lifeblood and provide you with the resilience needed to thrive and focus on what you do best - delivering value to your customers.

ARCHITECTURE ANALYSIS CONSIDERATIONS

The following is a list of essential factors to consider when evaluating your current IT architecture's capabilities, limitations, and data protection needs.

While this list is not exclusive, this introspective analysis will help you identify potential bottlenecks in the architecture and determine if potential solutions can support your organization's resilience needs while being compatible with your existing architecture.

Current Data Protection Environments

- Volume of front-end data (FET) currently being protected
- Number of servers and VMs being protected
- Number of servers utilized to protect sites
- Disk libraries replication type
- Disk libraries storage type
- Production disk hardware storage type

Data Centers and Remote Sites

- Number of data centers
- Number of geographic locations
- Number of disaster recovery sites/locations
- Number of branches and remote offices with protected local hardware
- Bandwidth between the data centers (Gbps)

Recovery Requirements

- Recovery Time Objectives (RTO) - The period within which systems, applications, or functions must be recovered after an outage
  - Time for single VM recovery
  - Time for mass recovery
  - SLAs
  - Application tiers
- The Recovery Point Objective (RPO) - The frequency of time to which systems and data must have a data protection operation run
- Any external factors that could impact your ability to meet desired recovery time or point objectives, e.g., Server, storage, and networking performance
- Desired recovery locale

Step into the era of cyber resilience with Commvault.

Explore how Commvault can help you use modern and innovative data protection strategies to ensure data is secured, defended, and recovered—everywhere. Request a hands-on demo of the Commvault platform today.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®