POINT OF VIEW

Data Protection in a Cloud-Connected World

Environment and workflow are at risk for cyberattack

Data protection has been historically focused on monolithic data sets rather than dynamic data workloads. Backup and disaster recovery plans were often seen as boxes to be checked off, rather than ongoing strategies implemented throughout the entire organization.

EVOLVING SOLUTIONS

Today, data protection has evolved based on the increasing need to limit risks and safeguard a business' greatest asset—its data. Organizations have a heightened focus on consistently securing data in more granular, intelligent ways. In an increasingly mobile, cloud- and internet-connected world, where loss of data integrity can take many forms, organizations are prioritizing how they protect and back up this crown jewel. When leveraged correctly, data unlocks valuable insights, reveals room for growth, and more.

This is why it is critical to develop a data protection strategy designed for your organization's business purpose. As you develop this strategy, it is essential to keep these key questions in mind:

- What environments do your workloads reside on, and what are the resiliency needs for these environments?
- Do you have a strategy in place that protects not just the data, but the workloads dependent on that data; regardless of their design?
- Does your resiliency plan address availability, data protection, reliability and recovery for on-premise, off-premise and hybrid workloads?

Use Case

CLIENT:

Large Manufacturing Company

CHALLENGE:

Mitigate the risk of business disruption and prevent unavailability of critical data due to malicious acts, including ransomware, malicious insiders, and compromised admin accounts

HOW WE HELPED:

- Implemented a software solution that seamlessly integrates with current technology to offer secure and unalterable storage for vital data.
- Utilized an immutable Write Once, Read Many (WORM) compliance solution to secure critical data.
- Ensured protection against malicious acts in both primary and Disaster Recovery systems.

RESULT:

Increased data protection across the client environment, guaranteeing data integrity.

> **Whether your data is on-premise, on a public cloud, fully cloud-native, or part of a hybrid cloud environment, these factors directly influence your data protection strategy.**

Environment Matters

Whether your data is on-premise, on a public cloud, fully cloud-native, or part of a hybrid cloud environment, these factors directly influence your data protection strategy.

For example, if you leverage microservices as part of a cloud-native application approach, your data and services may be spread across multiple clouds and multiple zones. As a result, you must use code (or scripts) to recreate infrastructure and reestablish data connectivity to get the same resilience you might have in a traditional environment. Additionally, the code used to provision your infrastructure must also be protected and available. In short, your environment directly impacts your data protection strategy.

In an increasingly hybrid cloud and cloud-native world, it is paramount to remember to protect not just the data in your environment, but also the data “of” and “about” your environment.

Use Case

CLIENT

A Health and Fitness Technology Company

CHALLENGE:

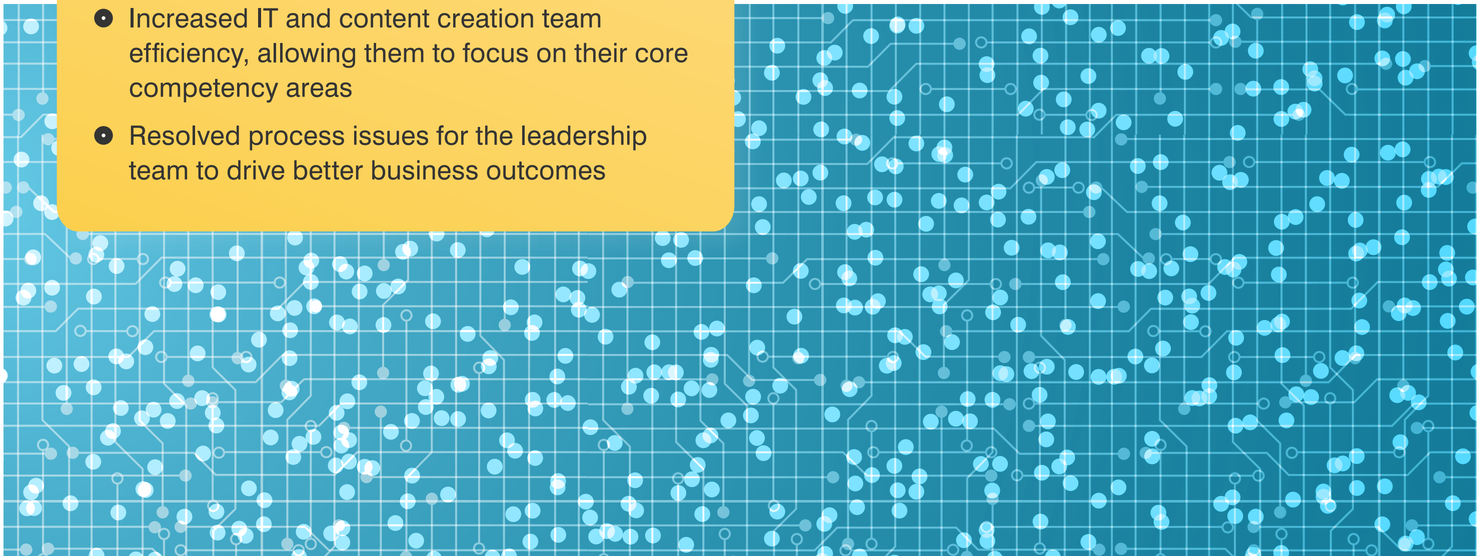
- Ensure a consistent IT experience with standardized processes and streamline communication across a siloed organization
- Enhance productivity within a team that was responsible for content creation but was taking on responsibility for infrastructure administration and data management

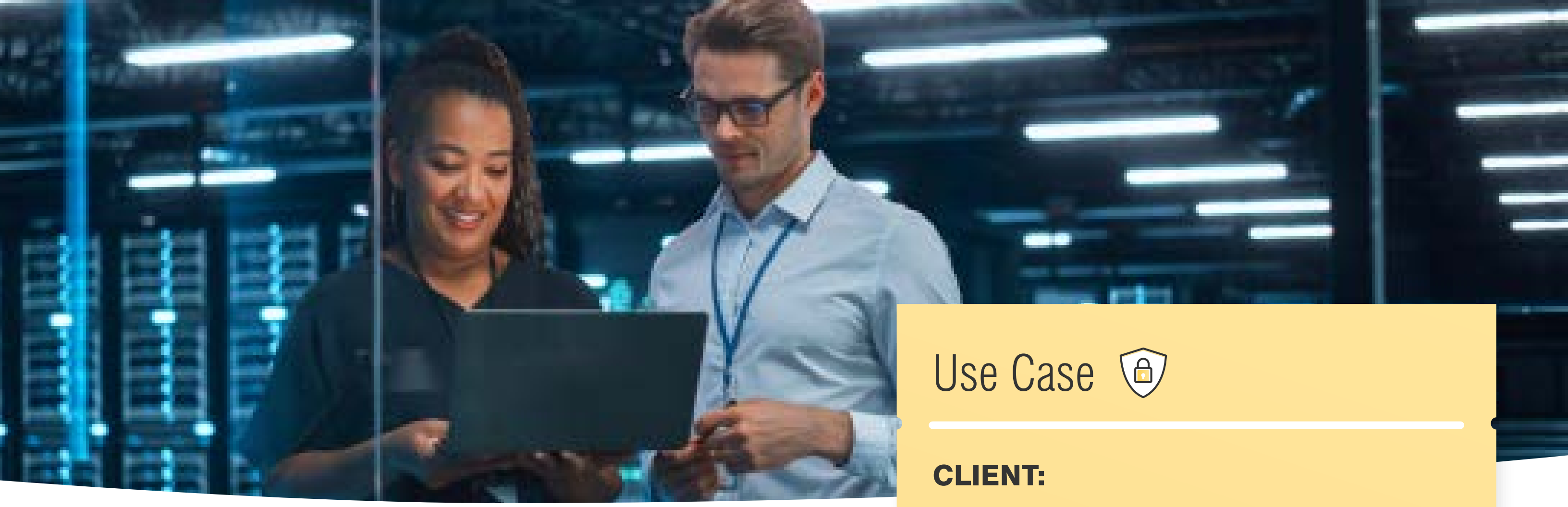
HOW WE HELPED:

Collaborated with stakeholders across the organization to create consensus and improve internal communications around a data protection methodology. This led to an improved budgeting methodology and a new internal communication process for technology projects.

RESULT:

- Ended a reactive approach to handling issues and deficiencies
- Initiated the design of a strategy that allows IT and lines of business to plan at the financial and technical level for issue remediation and organizational growth
- Increased IT and content creation team efficiency, allowing them to focus on their core competency areas
- Resolved process issues for the leadership team to drive better business outcomes





Create an Agnostic Data Protection Workflow

The increasing prevalence of public and hybrid cloud changes the way on-premise infrastructure and workloads function. Public cloud workloads and cloud-native behavior rarely translate perfectly back to traditional monolithic, multi-tiered, on-premise infrastructure.

Rising cloud trends are increasingly driving customers to treat their on-premise infrastructure as private clouds. This provides the agility of a public cloud, and because the cloud can be effectively leveraged in backup and recovery strategies, allows workloads to more gracefully transition between environments.

However, this trend—the integration of on-premise infrastructure and private cloud—calls for developing an agnostic data protection workflow that looks the same on-premise or in the cloud, whether private or public.

An API-enabled automation pipeline can help with this, reducing workflow complexities required to create an effective data protection environment. For example, if you are rolling out a new application, or your data protection needs change, you need a workflow that automatically makes these updates or changes to where your organization's backup lives. Data protection strategies contain too many elements for a single human to track—effectively making automation a necessary component of your plan.

Use Case

CLIENT:

Medical Prosthetic Company

CHALLENGES:

- Need to quickly recover from a cyber incident
- Address resource technical knowledge gaps on back-up and restore
- Ensure organizational readiness in case of a future cyber incident

HOW WE HELPED:

- Immediately assisted our client in recovering from a cyber incident. This involved recovering data, adding to and reconfiguring physical storage, and expanded data protection applications and infrastructure
- Provided guidance and oversight in the development of improved data protection processed and methodologies to decrease vulnerability and improve recovery speed
- Supplemented and trained client IT team on back-up and restore techniques

RESULT:

- Resolved cyber incident outages and assisted with the restoration of all necessary systems and data
- Increased storage capacity and improved storage redundancy
- Enhanced existing infrastructure to improve redundancy, reliability, and overall operational security
- Defined a data back-up and recovery plan with processes for more granular reporting and proactive alerting to speed discovery and decrease impact to business in the event of a future cyber incident

4 Steps to Increase Data Protection and Guard Against Data Breaches

Although ransomware is a hot topic that often captures public attention, there's much more to data protection than guarding against ransomware alone. Data breaches can take many forms—from inadvertent data deletion to unexpected downtime.

Fortunately, there are numerous approaches your organization can use to mitigate data corruption. Here are four steps to help increase data protection and guard your organization against data breaches. These steps work best in combination, creating a comprehensive approach:

1. **Implement strong security policies:** The need for consistent, strong security policies has become more pressing when it comes to keeping track of different environments. As a result, an effective, end-to-end strategy starts with maintaining consistency across security policies.

2. **Consistently create and update data copies:** Backed up data copies allow you to restore data back to a point in time before data integrity loss.

3. **Establish complete traceability and visibility:** Seamless traceability from the controls to the policy to the tools that implement the policy creates an ideal environment in which you can quickly map issues or data integrity problems to the business impact. Data managers should also have complete visibility into the security patterns of users for logging, encrypting users' data and stopping potential outbreaks. This will make it easier to know when a data integrity issue occurred.

4. **Constantly monitor your data environment:** From the firewall to your organization's internal components to data access patterns, everything must be monitored. Automating security helps enable constant monitoring as well.

Addressing Data Protection Misconceptions

It is also important to identify and correct any data protection misconceptions before developing your organization's strategy. Here are a few common ones:

- **Public cloud is automatically safe and secure:** Just like any environment, you must attend to your organization's cloud security strategy. Cloud providers do not have this responsibility—you do. Make sure levels of security are appropriate for your business workloads and understand what your responsibilities are in a cloud provider's shared security model.
- **Data protection is an "all or nothing" undertaking:** In many cases, organizations believe they should either backup and restore absolutely everything or nothing at all. There is a middle ground here. Your organization should do what it can to protect its data and evaluate the cost and complexity against business risks and impacts.
- **Data should only be backed up to guard against disasters:** The fact is, data integrity can be damaged through small breaches and inadvertent data deletion—not just full-on disasters or ransomware breaches.

Action Recommendations

Your data protection strategy will depend on your business needs, your industry, your data environments, the risks you might be exposed to, and more. There is not a "one-size-fits-all" approach that will meet all your needs, but you can follow these steps to develop a data protection strategy that is fit for your business:

Evaluate your data environments and the processes you need to keep this data protected

Automate where possible, and create an environment-agnostic data protection workflow that works on-premise, in the cloud or in a hybrid environment

Ensure you have data protection best practices in place that you monitor and update regularly—from traceability to security policies to data encryption

Create a plan to consistently maintain your data resiliency strategy

EVOLVING
SOLUTIONS

We’re here to help protect your organization’s data.

Let’s get to work.

ESI-010224-X104