Technical Insight Report

Data Protection Modernization

An Imperative for the Digital Age

By Krista Macomber, Senior Analyst

March 2021

Evaluator Group

Enabling you to make the best technology decisions

PREDATAR

Introduction

Enterprise IT teams are at a challenging intersection point. On one hand, they must meet data protection requirements that are more demanding than ever before. Data pools are growing exponentially in volume, yet data ownership has devolved to be unclear and scattershot. New kinds of business-critical resources that reside in hybrid and multi-cloud environments are entering the equation. Additionally, sophisticated cybercrime activity like ransomware attacks must be protected against. At the same time, enterprise IT is contending against legacy data protection solutions that are cumbersome to manage, expensive, and inflexible.

> ***Most large organizations are in a position of needing to simplify, adapt and otherwise drive the most value out of their existing data protection infrastructure.***

To address this problem, enterprises are rethinking their approach to data protection. They are seeking to make their day-to-day lives more efficient by reducing the complexities inherent in legacy infrastructure. They want centralized protection of – and oversight over – their hybrid cloud and multi-cloud environments. Ransomware has necessitated stringent backup schedules and accelerated, proven recovery streams. And finally, cost is always king when it comes to data protection; enterprise IT is seeking to meet these requirements on a budget.

The challenge is that existing data protection solutions and processes cannot just be thrown out. There is substantial risk and cost inherent in migrating off a solution that has protected business critical data for years. Furthermore, even if a new data protection solution is successfully introduced, typically the legacy solution is still kept up and running for a period of time (in many cases, for years), because of the need to support legacy infrastructure and to ensure recoverability of data that it has protected. In other words, there is still a long tail for usage of the legacy solution.

For these reasons, most enterprises and other large organizations are in a position of needing to simplify, adapt and otherwise drive the most value out of their existing data protection infrastructure – a concept known as “modernizing” data protection. This paper will unpack in more detail why data protection implementations need to be modernized to begin with. Given the influx of various vendors’ market messaging on the topic, this paper will also investigate what exactly it means to modernize data protection infrastructure.

> ***One of the key reasons that customers are looking to modernize their data protection infrastructure is to reduce day-to-day management complexity.***

Why Does Data Protection Need to be Modernized?

One of the key reasons that customers are looking to modernize their data protection infrastructure is to reduce day-to-day management complexity. IT teams are always pressured to do more with less, and these days that means overseeing a larger and more complex IT environment with minimal (if any) headcount growth. Against this backdrop, IT teams are shifting to be comprised more of IT generalists as opposed to specialists. This is especially true when it comes to data protection, which historically has required dedicated training as well as specialized product experts.

> ***Legacy solutions were not designed to support modern cloud and container resources [however] Born-in-the-cloud SaaS apps must coexist and interact with traditional databases and storage systems.***

The process of modernizing data protection is also intended to address the fact that the advent of the hybrid multi-cloud is shifting ownership over data, as well as responsibility for data protection functions, to a different group of users that sits outside of the data protection and even the central IT teams. For example, Evaluator Group sees application owners and users not only providing input in areas such as how much data loss and downtime are tolerable – we also see them requiring self-service recovery capabilities.

Data protection also needs to be modernized because legacy solutions were not designed to support modern cloud and container resources. They were designed to support on-premises infrastructure and apps, but not the born-in-the-cloud software-as-a-service (SaaS) apps like G Suite and Salesforce, the cloud-delivered infrastructure-as-a-service (IaaS), and the developer-created container-based applications – that all must coexist, and in most cases interact, with traditional databases and storage systems. Furthermore, legacy offerings do not support having data live across these hybrid and multi-cloud environments. An objective of data protection modernization is to facilitate centralized visibility and control so that protection service level agreements (SLAs) including required recovery points and recovery times are met consistently across these resources.

Visibility and value-add analytics furthermore become table stakes for a modern data protection solution to combat cybercrime. Threats like ransomware necessitate a solid backup strategy that includes the ability to be able to identify the last known good backup, as well as the ability to quickly recover from that backup. They also necessitate capabilities like scanning the backup environment to identify as early as possible that an attack has occurred.

> ***COVID-19 has compounded the already growing need for a more elastic and scalable data protection infrastructure and pricing model.***

Lastly, but far from least importantly, customers are also modernizing their data protection solutions to address the fact that, for a growing number of customers, a fully on-premises deployment model is no longer feasible. COVID-19 has made it necessary to avoid having to go into a data center for maintenance, and it has made remote accessibility a requirement. This has compounded the already growing need for a more elastic and scalable data protection infrastructure, as well as the need to break legacy pricing and procurement models that are notoriously inflexible and expensive. This is not to mention the expensive administrative cost of operating complex legacy data protection solutions.

What Does It Mean to Modernize Data Protection?

Simplicity through Automation and Self-Service

As previously mentioned, cutting operational complexities is a top outcome that customers are looking to achieve with a modern data protection solution. As a result, a fundamental step to modernizing data protection is to automate the execution of backup and recovery jobs and repetitive management functions. Not only does embracing automation drive efficiencies by streamlining daily processes, but it also can potentially improve recovery point objectives (RPOs) and recovery time objectives (RTOs) by allowing backups to occur more frequently, and by accelerating the recovery process. Adding in automated testing of recovery processes is also important to ensure recoverability – as is ensuring data integrity.

> ***A fundamental step to modernizing data protection is to automate the execution of backup and recovery jobs and repetitive management functions.***

To further streamline operations and reducing recovery times, the ability to provide self-service protection and recovery for a variety of data owners is an important characteristic of a modern data protection solution. Of course, access must be controlled through user authentication and role-based permissions then come into play for security.

Visibility and Future Readiness

Modernizing data protection also means adding in support for the modern sources including containerized apps that are being developed on a custom basis to support important business functions as a part of a hybrid cloud ecosystem. As touched upon earlier in this document, these data sources have become critical and require integration with traditional databases and data stores, as well as enterprise-grade protection and data governance. With this in mind, to modernize data protection means increasing visibility across all of the data stores under protection – including on- and off-premises applications and infrastructure, and physical, virtualized and container-based resources.

Achieving holistic visibility and control over fragmented hybrid multi-cloud environment, as well as consistent, timely, and accurate reporting, is a differentiator between modern and legacy data protection.

Tactically speaking, Evaluator Group sees modern data protection solutions adding in dashboarding capabilities for centralized insights across all of the resources under protection, as well as providing audit trails to be able to track ownership over and changes to data. We also see modern data protection solutions including machine learning to analyze backup metadata for compliance and security risks. Achieving holistic visibility and control over fragmented hybrid multi-cloud environment, as well as consistent, timely, and accurate reporting, is a differentiator between modern and legacy data protection.

Especially in today's age of ransomware and heavy data regulation, Evaluator Group consistently hears from customers that a solid backup strategy and proven recoverability are table stakes.

With compliance and security in mind, modern data protection solutions are also breaking down barriers between backup and archive or long-term retention, integrating the ability to tier data to low-cost retention storage that is increasingly frequently hosted in the public cloud. Of course, the ability to apply immutability and write once read many (WORM) designations are becoming points of parity as protection measures. Additionally, many modern data protection solutions have integrated the use of public cloud to open up failover and disaster recovery where otherwise it would be cost prohibitive for customers. Especially in today's age of ransomware and heavy data regulation, Evaluator Group consistently hears from customers that a solid backup strategy and proven recoverability are table stakes. At the same time, it is important to keep in mind that backup and recovery is an element of the broader security strategy that is driven by corporate or organizational security stakeholders.

Cost Efficiency and New Modes of Acquisition

Another important goal of data protection modernization is to drive down the total cost of ownership, especially for data protection infrastructures that were born on-premises, grounded in inflexible capex-based hardware purchases and perpetual software licenses. For a growing number of customers, this means rationalizing or otherwise consolidating their on-premises infrastructure in favor of public cloud-based backup and retention storage as well SaaS-delivered backup software. However, the cloud does not always make sense for a variety of reasons, for instance due to compliance and security concerns. With this in mind, data protection modernization can also entail adopting more variable, consumption-based hardware pricing as well as more flexible, subscription-based software licenses – in order to

provide a cost structure that is more fluid and can be scaled up and down according to protection requirements.

> ***Another important goal of data protection modernization is to drive down the total cost of ownership, especially for data protection infrastructures that were born on-premises, grounded in inflexible capex-based hardware purchases and perpetual software licenses.***

As touched upon earlier in this section, customers are modernizing data protection to reduce expenses related to operating the data protection infrastructure. For some, this means considering a managed approach. In this model, there is flexibility for where the infrastructure and backup software reside (such as on-premises or in the cloud), and the managed service provider (MSP) oversees any necessary deployment, management and maintenance tasks for the customer. Furthermore, many MSPs also handle the execution of protection jobs to RPOs and RTOs designated by the customer (in other words, the customer still sets policies for things like retention times and backup frequency).

Conclusion

Legacy data protection solutions are lacking when it comes to supporting today's complex and demanding enterprise backup requirements, causing customers to consider moving to something that meets longer term goals such as usability by IT generalists and supporting multi-cloud environments. That being said, disentangling from existing backup software is a years-long process. As a result, the practical approach for many enterprises is to modernize what is already in place.

> ***Disentangling from existing backup software is a years-long process. As a result, the practical approach for many enterprises is to modernize what is already in place.***

The concept of modernizing data protection is strategic, but it does carry some gray area due to marketing buzz. In working closely with IT professionals, Evaluator Group has identified a number of actions that customers are commonly taking to modernize legacy data protection implementation. These actions include streamlining operations through automation, increasing visibility into their environment with a centralized dashboard and machine learning, and opting for solutions that can support cloud resources and containers alongside more traditional apps and infrastructures. Finally, we see customers leveraging the cloud where it is feasible, and otherwise increasing the flexibility of their payment and procurement to control their operational and capital expenses.

Next Steps for IT Pros

- Identify administration tasks that are the most cumbersome and time-consuming for the IT team
- Identify gaps in new sources that need protection
- Identify areas of additional visibility that are required
- Consider opportunities to integrate the cloud (e.g. as a backup or DR target)
- Consider opportunities for greater flexibility in pricing and procurement of backup software

About Evaluator Group

Evaluator Group Inc., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.