WHITE PAPER

5 Best Practices CIOs Are Using to Modernize Enterprise Data Protection

SMART.
SECURE.
AUTOMATED.

cobalt IRON®

cobalt IRON®

TABLE OF CONTENTS

Introduction

Most enterprise IT departments today face tremendous challenges in providing adequate protection for all data across the enterprise and in supplying data protection services for mission-critical data in a way that helps to drive profitability. Business and technological obstacles combine to make conventional approaches to enterprise data protection difficult to maintain both successfully and cost-effectively.

Complex IT Infrastructure

The complexity of high-tech IT infrastructure and its continual evolution present significant challenges for IT, which must keep up with new capabilities, models, and usage patterns in handling enterprise data. Whether considering stack convergence, hybrid cloud operations, multi-cloud brokering, edge computing, infrastructure optimization, or distributed and mobile access, the typical IT department faces nontrivial obstacles in maintaining rock-solid enterprise data protection. Along with managing technologies, infrastructure, data reduction requirements, data security, and data protection operations, IT must also address an expanding array of compliance and regulatory requirements.

Growing Volumes of Data and Increasing Reliance on Analytics

The ongoing growth of data creation and storage likewise presents a challenge for IT. Neither the need to capture and store data nor the increase in data being stored is new. In today's business environment, however, the increasing use of machine learning algorithms and other analytical tools to process that data adds further pressure to build and maintain more accessible, more active data archives.

Evolving Business Structures and Operations

Business change is yet another unavoidable challenge IT departments face as they strive to ensure adequate data protection. Growth, downsizing, reorganization, and more stringent data service levels have an impact on an organization's collection and use of data. Mergers and acquisitions introduce new data, new layers of complexity, and even new ways of doing business.

Older generations of data protection solutions often can't address these challenges, and their shortcomings can't be overcome with additional backup licenses or the hiring of more IT staff. Yesterday's solutions are becoming overwhelmingly difficult to maintain, and they are less equipped to harness big data, leverage cloud processing, or deliver end-user experiences to mobile devices.

With these challenges in mind, CIOs are looking beyond investment in features and functionality to an easier consumption of IT services that delivers the desired results. They no longer want to purchase, build, and maintain data protection infrastructure and operations. They want to invest in outcomes — the right outcomes for their business — and they are modernizing their data protection operations to achieve this. Among the best practices being established to modernize enterprise data protection are rapid provisioning, intelligent automation, optimizing to improve service levels, protecting and securing data, and establishing comprehensive visibility and control.

Best Practice No. 1: Rapid Provisioning

Today when an enterprise asks IT to deliver a new solution, the business' leaders expect said solution to be implemented immediately, not after three months of procurement and another three months for fitting out the data center, provisioning the network, implementing storage, laying down a database, and installing and configuring the application. Rapid provisioning is a must. Businesses want enterprise data protection quickly, with minimal effort. Modernized techniques such as cloud services and Software as a Service (SaaS) models can help deliver rapid provisioning. The nature of cloud and SaaS solutions makes it easy to scale up or down to accommodate fluctuations in demand from across the enterprise. In addition, enterprises can pay only for features and capacities they use, and they can also shift from a capex to an opex pricing model if they choose.

> "Cloud is about how you do computing, not where you do computing."
>
> ***Paul Maritz, CEO of VMware***

Fast Provisioning of Infrastructure and Software

Unlike the traditional model of data protection, modern data protection can leverage software that is already installed and configured in the cloud. As a result, the solution provider can provision a server for an instance of that application in a matter of hours, with simple plug-and-play functionality on premises, and make the application ready for use. In addition to reducing the time required for installation and configuration, this model can eliminate issues that often get in the way of conventional software deployment (e.g., mismatched release levels, configuration issues, etc.).

Because the application is hosted in the cloud, the solution provider can more easily automate and accelerate allocation of system resources, deployment of feature sets, and configuration of user permissions. End users are granted access to the cloud-based application through account credentials, a web browser, and connectivity.

This model eliminates the need for extensive on-premises software installation, costly infrastructure for application hosting, and even the need for tedious user configuration. Furthermore, with access to the most up-to-date version of the software, users across different areas of the business can get right to work leveraging the application's most recent features and capabilities.

Cloud, Hybrid, and On-Premises Options

Sophisticated enterprise data protection solutions today often can be implemented in the cloud or in a hybrid solution spanning the cloud and on-premises installations. A hybrid model can allow an enterprise to make an incremental shift to the cloud, maintaining specific elements on premises and gradually evolving to a full cloud deployment over time as it benefits the business. Modern data protection offerings deliver IT services when and where they are needed, in the cloud

or on-premises. As a result, modern solutions can help unify and simplify the IT service experience across a hybrid environment.

Reduced Ongoing Efforts

The willingness of customers to spend time and money to procure and deploy infrastructure now in anticipation of future demands is rapidly evaporating.

> "Cloud computing is empowering; companies leveraging cloud will be able to innovate cheaper and faster."
>
> ***Jamal Mazhar, Founder and CEO, Kaavo***

CIOs are finding rapid provisioning to be a compelling component of modernizing data protection, but there are other benefits as well. The heavy loads of highly skilled infrastructure and operational experts tasked with managing the backup landscape are diminished. Responsibility for hardware and software currency, as well as 24x7x365 support, is shifted to the cloud or SaaS provider. Analytics integrated into the system support automation can simplify day-to-day operation and management. Once implemented, a sophisticated solution can monitor and verify that the backup and replication operations are completed successfully. It can confirm that software updates are applied and hardware failures resolved. It can support data-based capacity planning and provisioning so the business can grow with ease and confidence.

Best Practice No. 2: Intelligent Automation

Intelligent automation is being embraced by enterprises across nearly every industry. KPMG predicts an acceleration of investment in intelligent automation, with overall spending expected to reach $232 billion by 2025 compared with an estimated $12.4 billion today.[1] Why this tremendous growth in deployment of intelligent automation? Because intelligent automation is transforming both business and operating models, regardless of industry or sector.

The purpose of intelligent automation in data protection is to capture and encapsulate best practices, then leverage intelligent analytics to apply automatic updates and deep expert knowledge consistently across the entire landscape.

Data protection providers should always be increasing the level of operational automation, even if just to keep pace. Automation is especially critical when dealing with the challenges of deploying limited expertise to manage an expanding collection of data and the growing complexity of hybrid infrastructure.

Intelligent automation has the potential to transform processes both simple and complex, thereby supporting the enterprise in achieving both its strategic and business goals. With the benefit of intelligent automation, enterprise data protection can enable optimization of critical business areas such as resource and talent utilization while simplifying and improving processes across the business for greater efficiency. Further benefits include more effective use of data to inform business decisions that lead to target outcomes.

For modern data protection solutions, automation is a means to a greater goal: not just speed, efficiency, and cost savings, but the ability to capture data more comprehensively, improve the customer experience, reduce risk, and ultimately enable innovation.

Best Practice No. 3: Optimizing to Improve Service Levels

One of the demands on modern businesses is the need to provide better data service levels at lower costs. Data service levels include performance, capacity, accessibility, and availability characteristics of data. Enterprises often approach demanding data service levels by throwing expensive infrastructure and complex operations at the challenge. Although cloud services can help with fast provisioning as discussed earlier, they can actually cause problems in terms of performance and accessibility if not managed properly. With proper analytics, a modern data protection solution can assist in optimizing infrastructure (including on-premises, cloud, and SaaS resources) and operations (e.g., backups, replications, recoveries, migrations, data lifecycle management, etc.).

Another aspect of optimizing to improve service levels is to categorize and manage different types of business data appropriately. All enterprise data is not equal, and different service levels should be leveraged to manage different types of data. A common method of deploying enterprise data protection has been a one-size-fits-all approach. Engineering gets the same level of data protection as the finance department, which gets the same level of protection as the sales organization, and the services organization, and so on. Every department gets billed accordingly for that IT service. The flexibility of modern data protection offers enterprises alternatives that empower them to cut costs while increasing service levels overall.

Provisioning Appropriately

In today's world, in which cloud and SaaS are prevalent, it is possible — even standard — to charge each organization within the enterprise based upon their usage of the service. Rather than overprovision across the business to ensure that robust data protection is being applied everywhere it is needed, the enterprise can take a more thoughtful and cost-effective approach to meeting data service levels.

Considerations for Modern Data Protection SLAs

- **Performance** - optimize infrastructure and operations to deliver highest performance service levels at lowest costs
- **Scalability** - design with the ability to grow on demand while avoiding major up front investment
- **Security** - focus on readiness, response, and recovery to prevent or reduce impact of any cyber attack
- **Automation** - harness technology to eliminate manual effort and the potential for mistakes
- **Analytics** - use machine intelligence to drive proactive problem avoidance and automated efficiencies

Departments that want or need a platinum level of service will pay more, and get more, than the department that needs only a gold level of service. With different levels of service, the enterprise can align its IT investments to its business needs. By optimizing infrastructure and operations, improved data service levels at tremendous cost savings are possible.

Best Practice No. 4: Protecting and Securing Data

Hacked devices, crashed websites, breached networks, denials of service, copied emails, and other cyber incidents have become commonplace. According to the Online Trust Alliance (OTA), cybersecurity incidents targeting businesses nearly doubled from 82,000 in 2016 to 159,700 in 2017. Because the majority of cyber incidents are never reported, OTA believes the actual number in 2017 could easily have exceeded 350,000. Some attacks, such as ransomware, have increased by 2000% since 2015.

> "1.5 million cyber attacks occur every year, which translates to over 4,000 attacks every day, 170 every hour, or nearly three every minute."
>
> ***CBS News***

No large enterprise can ever be certain that all its corporate data is safe from hacking, breach, corruption, or loss. The continual emergence of new threats, the expanding size of the corporate "attack surface," and the increasing breadth of every company's sensitive data footprint combine to make total data protection and security a tall order.

A modern data protection solution can offer user-friendly protection and restore capabilities that help to prevent — or mitigate the impact of — compromised data. The very architecture of the solution should be designed to provide the utmost security in the face of constantly changing threats.

Readiness, Responsiveness, and Recovery

Avoiding a crisis often comes down to managing a cyber incident properly before, during, and after it unfolds. To this end, a modern enterprise data protection solution should provide a holistic view of the entire datacenter, and incorporate appropriate security features and functionality within its core architecture, not as an add-on feature. A data protection solution with security built in by design is stronger and less expensive than a legacy solution that forces the IT team to plug holes and patch gaps after the threat has become a reality.

Preparation is essential to avoiding exposure, and readiness includes vigilant 24/7 monitoring, proactive problem avoidance, and automated software currency to ensure that enterprise data protection is on alert at all times.

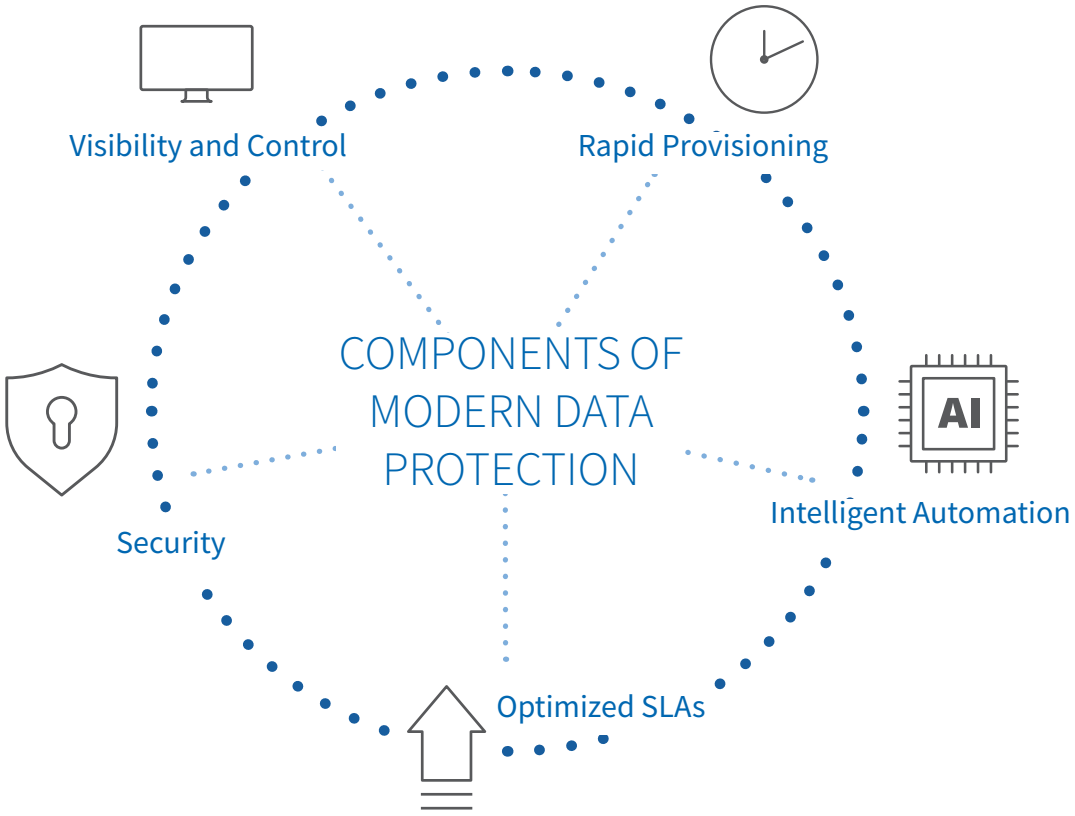
The modern consequences of a major data breach demand responsiveness. Response time to a security incident will be a major factor in determining the extent of damage to the company's data, costs, and reputation. Even if data remains intact, the enterprise still must recover to a known good state, prior to the breach. A modern data protection solution can keep a trusted, protected copy of key data safe so that the enterprise can respond quickly to a breach and immediately begin recovery.

Proper technology response can dramatically limit the negative impact of a cyberattack. Rapid, coordinated execution to resolve incidents minimizes downtime,

data loss, cost, and reputation damage. Quickly returning to normal operations is only the beginning. Rapid restore functions and analytics-driven insights can help to fortify data protection against future attacks.

Managed Data Protection

A data protection service provider with a world-class security solution and a company of experts behind it will offer a host of security features to protect key data.



Security as a Core Competency

Data and system security is a concern of IT departments everywhere. Automated and monitored backups of data, cyber-attack monitoring, secure data protection including encryption in-flight and at rest, system and data integrity verification, locked down authentication controls, redundant instances in secure data centers, and providing air-gapped copies of data are all aspects of a complete data security solution.

Built-in features can include fully human-less backup automation inaccessible to enterprise interference, full encryption schemes, WORM policies, support for air-gapped and isolated landscapes for validation and recovery, and more. These kinds of built-in features not only safeguard data, but also streamline every step of the recovery process.

Best Practice No. 5: Establishing Comprehensive Visibility and Control

Visibility and control of end-to-end data protection operations have become essential to the enterprise because they give executives in IT the ability to demonstrate that what they claim is available to the business is in fact available to the business. Insights into data protection operations can help address data compliance or security requirements, and help determine whether or not the enterprise can grow its business without substantial augmentation of staff or capital equipment costs.

Accurate, Comprehensive Reporting

Anything but a near-real-time level of inspection of claims is becoming unacceptable. Unsubstantiated claims no longer hold water. Rather, enterprises increasingly depend on robust access to the management, administrative, and operational data that supports the claims being made by the business. In the area of data protection, this capability allows the enterprise to give continuous accountability of data to the business. Delivering the ability to recall information and understand why a failure event or data breach occurred, the solution gives the IT team the ability to see what system or function failed. They can assign ownership — internal or external — to the problem and prevent it from happening again. Accurate, comprehensive monitoring and reporting is key to an efficient data protection experience.

Centralized Visibility and Control

Activity measurement and monitoring capabilities are critical to the enterprise's ability to maintain compliance, and modern data protection solutions can provide near-real-time reporting on all aspects of data protection within a single unified control interface.

> By relying on the statistical information rather than a gut feeling, you allow the data to lead you to be in the right place at the right time."
>
> ***James O'Shaughnessy, Investor***

Designed to be operable without complex training or technology skills, such an interface supports execution of operational management tasks such as provisioning new systems, changing schedules, adjusting management policies, and more. Users can extend data protection to new systems, applying global policies and best practices, or inspect the automated processes supporting data protection.

Modern data protection solutions should deliver visibility, reporting, and control in a comprehensive and unified manner enabling businesses to leverage rather than just manage their data. This is yet another reason that IT executives are modernizing enterprise data protection.

Conclusion

Rapid provisioning, intelligent automation, optimizing to improve service levels, protecting and securing data, and establishing comprehensive visibility and control are some of the approaches being pursued by CIOs to modernize and improve enterprise data protection operations. These best practices for data protection can help speed provisioning of data protection solutions, save on operational complexities and costs, optimally leverage infrastructure investments, improve data service levels, better secure corporate data, improve the visibility and management of end-to-end operations, and lower total costs.

Evaluating your data protection infrastructure, operations, and processes against these best practices may provide ideas on steps you can take to improve the robustness and lower the costs of your data protection practices.

1. KPMG, "Ready, set, fail? Avoiding setbacks in the intelligent automation race," https://advisory.kpmg.us/articles/2018/new-study-findings-read-ready-set-fail.html