2020 Modern Backup Buyers' Guide

Cloud adoption is on the rise, with over one-third of companies adding cloud-based infrastructure/services and/or migrating existing workloads to cloud (public, private, or hosted) as a primary strategy for ensuring business objectives and goals. IT decision makers are embracing a multicloud approach to leverage cloud-based services. These services both complement and can stimulate reconsideration of broader data protection strategies to gain greater availability and backup/recovery of data and improved performance of latency-sensitive applications.

With cloud adoption increasing, more companies see the need to modernize their data backup and protection platforms from multiple perspectives: use of cloud as a storage target; protection of data and applications that are hosted in the public cloud; and protection of data consistently across hybrid environments. Eighty percent of decision makers are eager to address the risks related to privacy, cybersecurity, and data integrity, but with IT environments changing so rapidly for most organizations, firms must consider several attributes of any new data protection and backup solution as they look to ensure protection and recoverability of the production platforms and services throughout their environments, including:

› Comprehensive protection.

› Recovery at scale.

› Ease of management.

› Automation and orchestration.

› Data reuse and insights.

› Security.

This guide provides directions into what capabilities to look for within each of these categories and offers questions that IT and business decision makers should ask themselves as they evaluate their companies' specific needs regarding backup and data protection solutions.

FORRESTER®

Comprehensive Protection: Business Continuity, Heterogeneity, And Broad Platform Support

While technology leaders have modernized applications using cloud-native technologies like infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS), they still maintain myriad on-premises technologies and platforms that host an array of critical applications. The heterogeneity of applications and data architectures creates complex data protection requirements that firms must address to protect the business from any crisis.

A comprehensive and heterogeneous strategy should apply not only to what organizations protect (physical, virtual, cloud-hosted) but also to where they protect their data (disk, tape, object-storage). In addition, data protection solutions must deliver a comprehensive approach to backup, snapshots, and replication for entire production data sets while enabling the flexibility to transport those data sets easily between platforms, based on the needs of the business.

Figure 1

34% face difficulties with managing data across multiple cloud environments

34% are not confident they can protect sensitive/private data whether stored on-premises, with a third party, or on the cloud*

Base: 206 ITDMs in the US, the UK, and Germany responsible for data backup and recovery technology decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Veeam, December 2019
*Base: 3,741 security decision makers from companies worldwide
*Source: Forrester Analytics' Global Business Technographics® Security Survey, 2019

Technical & Functional Considerations	Organizational & Operational Considerations
• What new applications does my organization plan to deploy? What data protection needs will each of those have? • How do I protect the heterogenous data sources across my organization? • How do I protect the data stored in various SaaS services that my organization consumes? • What type of data will be stored for each application? What level of protection and recoverability does each need? • How can I improve my network attached storage (NAS) backups and restores?	• How does my organization plan to utilize cloud technologies over the next one to two years? • What are the uptime and retention requirements for all of our applications? • What business risks does my company face as the data spreads across multiple cloud environments? How does my licensing change as we move workloads between platforms and clouds? • Which parts of my organization are or will be dependent on data now residing in cloud-hosted infrastructure or services?

WHAT TO LOOK FOR IN A SOLUTION

Look for a solution that can support on-premises physical and virtualized infrastructure, public cloud infrastructure, and SaaS. As platform-as-a-service (PaaS) platforms grow in mainstream production usage, pursue contemporary data protection vendors that include containers within their strategy and roadmap. In addition, look for the ability to leverage diverse storage platforms for snapshots and replications within the same data protection management framework. Seek data protection tools that support modern workloads, including NAS, distributed file systems, unstructured data, and cloud-based platforms, and that support granular recovery for improved recovery time objective (RTO).

OTHER CONSIDERATIONS

Data volumes — structured and unstructured, cloud-native — are growing rapidly. Infrastructure and operations (I&O) professionals face constant pressure to achieve and maintain a balance of compliance, cost, and speed equation. Consider a combination of storage optimization techniques and new architectures into your list to achieve that balance, including object storage to help reduce the cost; a scale-out architecture to provide a resilient architecture; and public cloud storage targets, which may serve your long-term retention needs.

FORRESTER®

Recovery At Scale:
Reliability Of Backup And Restoration

Organizations must retain copies of their data, despite the exponential growth of backup volumes considering the data type, backup frequency, and data retention needs. Firms must keep the backups and other copies for years, demanding the flexibility and adaptability to manage the underlying storage. Depending on the lifecycle stage, firms may have to place data on disks or public cloud archive storage.

Granularity and speed are important dimensions from both backup and recovery perspectives. Depending on the circumstance, recovery needs span from recovering a few email messages or a single file to an entire data center. In specific examples like ransomware recovery, organizations need to be mindful when developing a retention strategy that ensures immutability of data, as well as assurances that one does not reinfect environments during restorations. Firms must optimize backup tools to reduce the time, cost, and storage requirements yet meet their committed service levels and regulatory requirements. The bottom line of any backup solution is how reliably it can operate under different situations and if its recoveries can meet the needs of the business.

Figure 2

22% report inconsistent service levels across cloud environments

24% are adopting hybrid cloud to take advantage of different service levels/performance on different cloud platforms

26% cite the ability to leverage cloud storage for recovery as a key driver for hybrid cloud adoption

Base: 2,275 infrastructure decision makers from companies worldwide that are implementing or planning to implement hybrid cloud
Source: Forrester Analytics' Global Business Technographics® Infrastructure Survey, 2018

Technical & Functional Considerations	Organizational & Operational Considerations
• What backup optimization options are applicable corresponding to my data sources?	• How do my team's performance expectations vary between cloud and on-prem environments?
• Do my current (cost and storage) optimization techniques still apply with cloud or hybrid deployment?	• What SLAs does my organization currently have in place for data protection?
• Have my backup windows compressed in the past, and how will those shape up in the next two to three years?	• Is my organization not only geared to prevent cyberattacks, but also adequately prepared to recover from ransomware?
• What processes do I have in place to verify that my data is recoverable?	• Can I support a mass recovery from a large-scale data center outage?

WHAT TO LOOK FOR IN A SOLUTION

Find a solution that scales well to deliver data protection and recovery with speed and reliability. Look for a solution that delivers the right optimization techniques for time, cost, and storage. Your solution should be equally adept at both granular and whole-site recovery options, protect restoring data from ransomware and other malware intrusions, and support various recovery modes, including application-centric, user-specific, and file-level recoveries. Search for a solution that can automatically perform background recovery tests to ensure that recovery can happen when you really need it.

OTHER CONSIDERATIONS

Companies are consistently looking for the fastest time and no vendor lock-in to value with any new solution, but that path looks different for each company based on their current environment. A software-centric approach provides flexibility to choose best-in-class components. The emergence of converged backup appliances shows an interest in solutions that combine backup software with hardware, as appliances can have a faster time-to-deployment. Evaluate your current environment and determine the right combination of software and hardware for your organization to support orchestration across all expected environments.
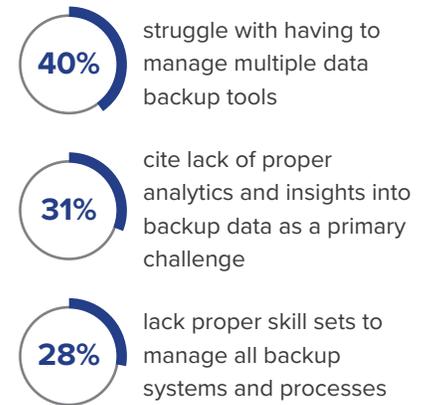
FORRESTER®

Ease Of Management: Day-To-Day Usage And Operations That Provide Operational Analytics And Insights

Today's IT manages various technologies — multiple storage systems, virtualization technologies, databases, and cloud services (IaaS, SaaS) — all of which operate in their own distinct ways and require different methods of protection. Backup tools must integrate with and support this diverse portfolio of data sources and repositories at different levels.

Managing backup operations should not add to the existing complexity with which IT administrators struggle today. Understanding the health, performance, and capacity characteristics of the backup infrastructure is critical for day-to-day operations, capacity planning, and long-term operational strategy. Predictive analytics and aided problem resolution are a must.

IT teams need easier-to-manage backup systems to reduce complexity. Thirty-two percent of technology decision makers believe that improved ease of use would be a primary driver for changing/improving their primary backup solutions.

Figure 3

40% struggle with having to manage multiple data backup tools

31% cite lack of proper analytics and insights into backup data as a primary challenge

28% lack proper skill sets to manage all backup systems and processes

Base: 206 ITDMs in the US, the UK, and Germany responsible for data backup and recovery technology decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Veeam, December 2019

Technical & Functional Considerations	Organizational & Operational Considerations
• How many disparate tools am I using to protect my diverse production data sources? • Do my backup tools operate differently for disparate sources and targets, or do they add to the complexity? • Can my current backup tools provide recommendations based on historical performance or status conditions? • What is my level of visibility into the backup operations? Is that sufficient?	• Do I have the capability, or the requirement, to protect, manage, and report on all assets in a single dashboard? • Do I have dedicated resources, with the proper training, to manage backup systems and operations at scale? • What operational data and reports are available from the backup solution? • Can I effectively use the reports to optimize data protection, backup, and recovery? • Do my backup solution's reports improve my ability to assure regulatory compliance and successfully pass my internal and external audits?

WHAT TO LOOK FOR IN A SOLUTION

Seek out solutions that offer global management and reporting using a unified operational console to produce comprehensive reports across the heterogenous protected assets and distributed data protection infrastructure. Look for solutions that offer out-of-the-box visibility or allow custom creation of operational reports to fit your specific environment. The reports must be intuitive to guide IT professionals and compliance/audit teams to take remediation actions by analyzing the historical achievements.

FORRESTER®

Automation And Orchestration: Integration, Policy-Based Protection, And Workflow-Based Restorations

Businesses are generating far more data than they were just a few years ago. Tolerance to downtime or data loss has drastically reduced. Regulatory requirements and competition have heightened dependence on and stringency for data protection by IT. Application developers are rapidly embracing new technologies that introduce new production platforms for customers service at a pace never seen before. Managing all these changes in a traditional manner — a manual planning and execution of backup tasks — will almost certainly result in protection gaps that leave organizations exposed.

Organizations are witnessing rapid changes in a highly competitive market while users have ever-increasing expectations. To serve those evolving demands, IT teams should look for policy-driven data protection solutions that can affect the changes automatically. IT teams need modern data protection solutions that can integrate with IT orchestration tools such that workflows can execute backup tasks automatically. Fifty-eight percent of respondents surveyed rate automated protection among their top five capabilities that most influence their companies' choice of data protection solutions.

Figure 4

Only 29% of decision makers find it very easy to automate and manage data recovery SLAs across environments

37% report that backup tools don't have policy-based management to automate tasks

34% of decision makers don't find it easy to integrate backup tools with existing systems and processes

Base: 2,275 infrastructure decision makers from companies worldwide who are implementing or planning to implement hybrid cloud
Source: ForresterAnalytics' Global Business Technographics Infrastructure Survey, 2018

Technical & Functional Considerations	Organizational & Operational Considerations
• How much time does my IT staff spend on setting up and managing data protection plans? • What recovery tasks can be orchestrated or scripted? Can the human interaction be reduced to the single decision to "invoke" the recovery plan(s)? • Can my backup tasks be orchestrated by my broader systems management or provisioning workflows? • Can my data protection recovery plan be tested using orchestration for consistency?	• Are we protecting all our data sources? • How does my organization ensure data safeguards within a timely manner? • How effective are the current plans and policies in serving business needs? • How do we know when our plans and policies need adjustment change?

WHAT TO LOOK FOR IN A SOLUTION

Look for a solution that offers built-in automation for routine tasks like backup, test restorations/validations, and recoveries. An automated approach to data protection should report on deviations from protection policies or RTO/RPO deficiencies to ensure compliance with corporate policies of retention and recoverability. These capabilities should be available regardless of the heterogeneity across the production environment(s). Therefore, look for solutions that support the invocation of operational tasks using REST APIs, leverage orchestrated workflows for repetitive tasks and ensuring consistency, and can be governed by policies.
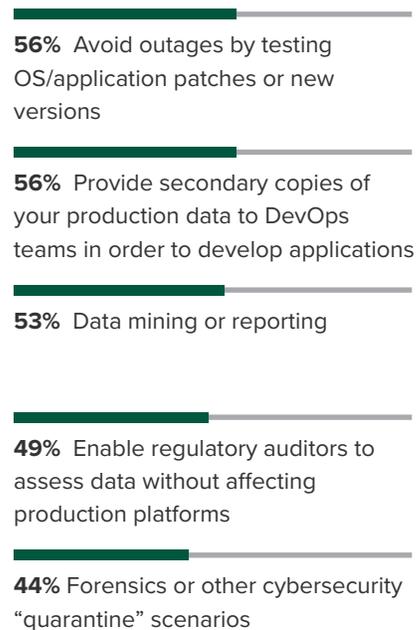
FORRESTER®

Data Reuse And Insights: Use Of Backup Data/Infrastructure For Business Needs In Addition To Recovery Use Cases

Organizations must invest in keeping copies of data for business and regulatory needs. For many, the ROI of a modern backup solution comes not just from the assurance of recoverability but also from the ability to do more by leveraging the data within the backup repositories for any other business use beyond "just" retention or recovery. Application dev-test, IT security, and compliance checks are some of the most sought-after use cases by business teams outside of IT. Fifty-six percent of the respondents report that their organizations reuse backup data for testing OS/application patches or new versions. A similar percentage of respondents report providing secondary copies of the production data to dev-test teams to develop applications, and 53% of the respondents report using backup copies for data mining or reporting purposes.

To enable data reuse, backup tools must be able to carve requested data segments out of backup repositories. They must enable third-party applications to securely request, consume, and manage that test data.

Figure 5

"In what ways does your organization reuse backup data?"

56% Avoid outages by testing OS/application patches or new versions

56% Provide secondary copies of your production data to DevOps teams in order to develop applications

53% Data mining or reporting

49% Enable regulatory auditors to assess data without affecting production platforms

44% Forensics or other cybersecurity "quarantine" scenarios

Base: 206 ITDMs in the US, the UK, and Germany responsible for data backup and recovery technology decisions
Source: A commissioned study conducted by Forrester Consulting on behalf of Veeam, December 2019

Technical & Functional Considerations	Organizational & Operational Considerations

• Which internal teams could utilize secondary access to production data and for what purposes?
 	
  – Compliance audits?
 	
  – Development testing?
 	
  – Patch testing?
 	
  – Cybersecurity?
 	
  – Penetration testing?
 	
• Am I able to satisfy those enablement scenarios today and with what difficulty or regularity?
	• Do I have the processes lined up that will enable reuse of backup data?
	
	• How will I handle and ensure the data security and compliance for these use cases?
	
	• What would it be worth (in ROI) for the other teams in my organization to be able to leverage this dormant data for audits, testing, DevOps, etc.?

WHAT TO LOOK FOR IN A SOLUTION

Explore solutions that offer a standard native interface and/or standard APIs that third-party tools or custom scripts can call to submit the data requests. The solution should be able to carve out specific portions of data. Data security is a must, both for enabling access and preserving the recoverability of data. Look for automated ways to create "sandboxes" or similar testing environments that enable offline and sequestered reuse of quiesced data for secondary purposes.

FORRESTER®

Security:
Integrating Backup And Recovery Within A Comprehensive Cybersecurity Strategy

Ransomware is a global risk firms face in terms of the likelihood of occurrence and impact. Ransomware is known for not only encrypting production data but also wiping out the backup systems and the backup copies, i.e., victims' last line of defense. Organizations must secure the systems and data as part of their cybersecurity strategies. Firms in regulated industries have used air-gapped copies, immutable file systems, and write-once, read-many (WORM) storage repositories to ensure data is unchangeable. IT leaders have been exercising the practice of protecting the data copies by moving them to remote locations that are disconnected from production systems. They now need to ensure the backup systems don't reinject malware by accidentally restoring from infected copies.

Figure 6

81% consider cybersecurity and privacy when developing their technology strategy

50% have strong concerns about security attacks from nonstate actors

29% face security challenges when using multiple cloud platforms*

Base: 3,741 security decision makers
Source: Forrester Analytics' Global Business Technographics® Security Survey, 2019
*Base: 2,515 infrastructure decision makers whose firms are using hybrid cloud strategies
Source: Forrester Analytics' Global Business Technographics® Infrastructure Survey, 2019

Technical & Functional Considerations	Organizational & Operational Considerations
• How will I secure my backup and recovery solution and protect it from being compromised? • How will I secure the backup copies from being compromised or from deletion? • Can I harden the backup solution by adding multimethod authentication for tasks that could destroy the backup copies? • During recovery operation, how can I be sure that ransomware traces are not being (re)injected into the recovered instances?	• How do I work with business and IT security peers to create a mutually agreed upon plan that addresses risks from ransomware? • How often should I test for recoverability? • How will the IT security tools share intelligence with backup tools?

WHAT TO LOOK FOR IN A SOLUTION

Check for backup solutions that inherently provide multidimensional security. One, find what features the backup solution has to secure itself from unauthorized access, rogue elements, and malware attacks. Two, determine how the backup software stores and secures the backup copies. Depending on the application and your data risk profile, find a solution that can save backup data with specific retention requirements on an immutable file system at a defined frequency. A meticulous design using immutable systems will boost data resiliency.[1] You must also look for the multilayer authentication to ensure that a destructive action can't be executed by simply gaining access into the system. This can be a feature native to the tool or achieved through integration with other security tools

FORRESTER®

Conclusion

As organizations increasingly distribute their applications and data across hosted, public, and on-premises systems for their mission- and business-critical systems, they must pay high attention to ensuring the data housed within those systems is protected and properly backed up. This is no small feat as data is constantly in motion between on-prem and cloud systems and between different applications. Increasing data volumes that continue to grow with no signs of slowing down only exacerbate this challenge.

Leaders within IT teams must carefully assess their data protection needs and requirements to ensure they have the right tools and processes to protect and back up all of their data assets. There will always be more data to protect, but your capability to manage data operations and extract insights from current processes to drive improvements is a critical factor to success. As you and your teams consider your future IT architectures in a distributed deployment model that includes multiple cloud services and how you want to protect its data going forward, ask yourself the key questions highlighted in the various sections of this document to understand exactly what your organization needs from a data protection and backup solution.

FORRESTER®

Appendix A: Methodology

In December 2019, Veeam commissioned Forrester Consulting to conduct research regarding companies' current usage and requirements for data backup and protection solutions. The research consisted of two components:

1) Forrester conducted a survey of 206 IT decision makers in the US, the UK, and Germany responsible for data backup and recovery technology decisions, and respondents were asked a series of questions about their current business needs for protection and backup. The survey was double blind, and respondents were offered a small incentive as a thank you for their time.

2) Veeam commissioned the use of Forrester's Business Technographics® surveys to pull insights specific to data protection, data backup, and cloud computing. Surveys used include the Forrester Analytics' Global Business® Technographics Infrastructure Survey, 2018 and 2019; Security Survey, 2019; and Networks And Telecommunications Survey, 2019.

Appendix B: Endnotes

[1] Source: "Four Technologies Combine To Protect You From Ransomware Attacks," Forrester Research, Inc., October 18, 2019.

Project Director:
Chris Taylor,
Senior Market Impact Consultant

Contributing Research:
Forrester's Infrastructure &
Operations research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®