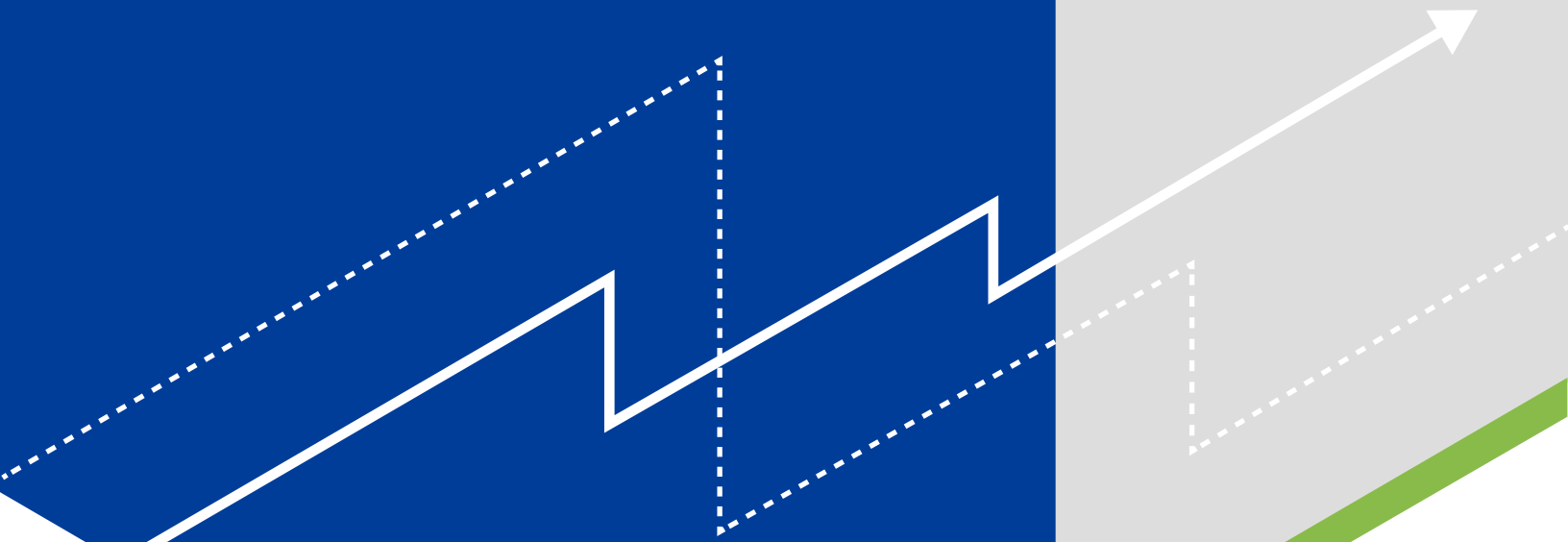
A Forrester Consulting
Thought Leadership Paper
Commissioned By Druva

March 2018

Addressing Data Management Risks For The Public Cloud Era

Leverage Public Cloud To Future-Proof Your Data Protection And Governance



FORRESTER®

Table Of Contents

Project Director:
Heather Vallis, Principal 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®

Backup Architectures

On-premises: Purpose-built software, hardware, tape, or replication off site

Hybrid: On-premises storage for recent backups; cloud for archival

Hosted solution: Backup software hosted in cloud servers, utilizing warm storage

Backup-as-a service: Built from the ground up in cloud, utilizing native services

Executive Summary

A proliferation of business and consumer technologies has led to an explosion of data. Harnessed effectively, this data holds enormous value for organizations looking to generate insights to improve their operations and customers' experiences. But a shifting data landscape has introduced changes in both regulatory data requirements and attack vectors, significantly increasing data risks related to loss, compromise, and non-compliance.

To unlock this data's value while ensuring its proper use, organizations need comprehensive data protection capabilities. But many enterprises store data that is vital to the business across multiple data centers on-premises, at managed data centers, and in the cloud. This can lead to siloed and complex data backup and recovery practices which limit data visibility and make management, governance, and recovery more difficult, if not impossible.

In August 2017, Druva commissioned Forrester Consulting to conduct an online survey of 150 IT decision makers at organizations in the US and Canada to explore this topic. Our study revealed the following:

KEY FINDINGS

- **Current data backup and recovery practices flirt with data loss.** Today's complex and disconnected systems create cracks through which valuable data can be lost: Over 75% of organizations surveyed have experienced a loss to mission- or business-critical data recently. Inadequate backup and recovery practices are exacerbating the problem. Too many organizations are backing up critical data infrequently, and many are using manual backup processes which are prone to errors. Further, a lack of integration between data protection and disaster recovery strategies means running the risk that data lost may not be fully recovered.
- **Organizations turn to cloud backup to relieve infrastructure headaches.** While mission-critical data is predominantly stored on-premises, increased adoption of SaaS applications and other cloud services place more of this data off-premises. Cloud — and now also edge computing — bring great business value but also scatter business data across a wide landscape. Protecting this distributed data is a significant challenge, but cloud-based data backup that reaches across this hybrid landscape can prove attractive, while reducing costs. Roughly one in five organizations turn to cloud-based backup to reduce their storage footprint, while 23% seek to tame escalating costs of on-premises infrastructure.
- **Data protection-as-a-service helps organizations meet security, recovery, and compliance needs.** Data protection increasingly relies on cloud-based systems. A large majority of survey respondents report they are likely to adopt a unified cloud solution that integrates data backup, recovery, and protection; citing improved data security as a top benefit. Additionally, organizations already using backup-as-a-service were more likely to meet the demands for fast data recovery than those using on-premises as their predominant approach.

FORRESTER®

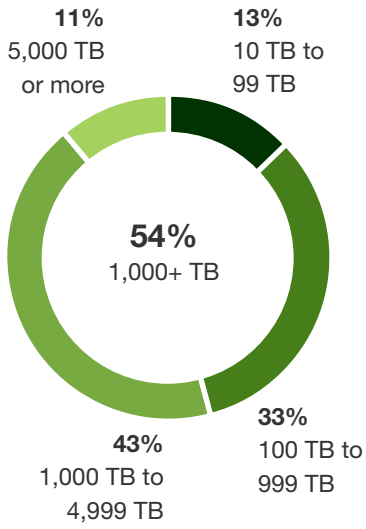
The Digital Revolution Is Accelerating Data Growth

Business and consumer technologies have rapidly advanced in recent years, leading to an explosion of information. Customers, employees, and partners are online, connecting with your organization and each other and generating an ever-increasing amount of data. By industry estimates, 90% of today's digital data was created in the past two years.[1] This data is the lifeblood of every organization — a vital resource that enterprises of all shapes and sizes are seeking to harness to gain competitive advantage and better win, serve, and retain customers. Our study of 150 IT professionals in the US and Canada revealed:

- **Organizations are dealing with vast stores of data.** Over half of the IT professionals surveyed reported their organizations are storing 1,000 TB or more of structured, semi-structured, and unstructured data (see Figure 1). This is particularly prevalent among large enterprises (those with 1,000 or more employees): 65% are dealing with data volumes of this magnitude compared with 41% of smaller organizations.
- **Data volumes have increased significantly.** Virtually every enterprise — whether large or small — is managing an increasing amount of data. Forty-one percent of organizations have seen the amount of data they are storing increase by 50% or more over the past two years. In fact, "exponential data growth" was the No. 1 challenge as cited by respondents around data backup and recovery. Smaller enterprises (those with 100 to 999 employees), in particular, have experienced a sharp uptake, with over half experiencing data growth of 50% or more, compared with 32% of large enterprises.

Figure 1

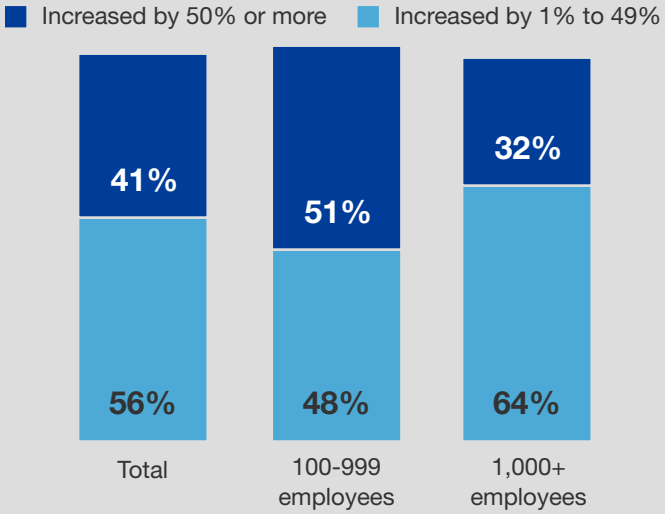
"Using your best estimate, about how much data —including structured, semi-structured and unstructured data — is your organization currently storing?"



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Figure 2

"To what degree has the amount of data your organization is storing changed over the past two years?"



Base: Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Fifty-six percent cite **"exponential data growth"** as a challenge.

FORRESTER®

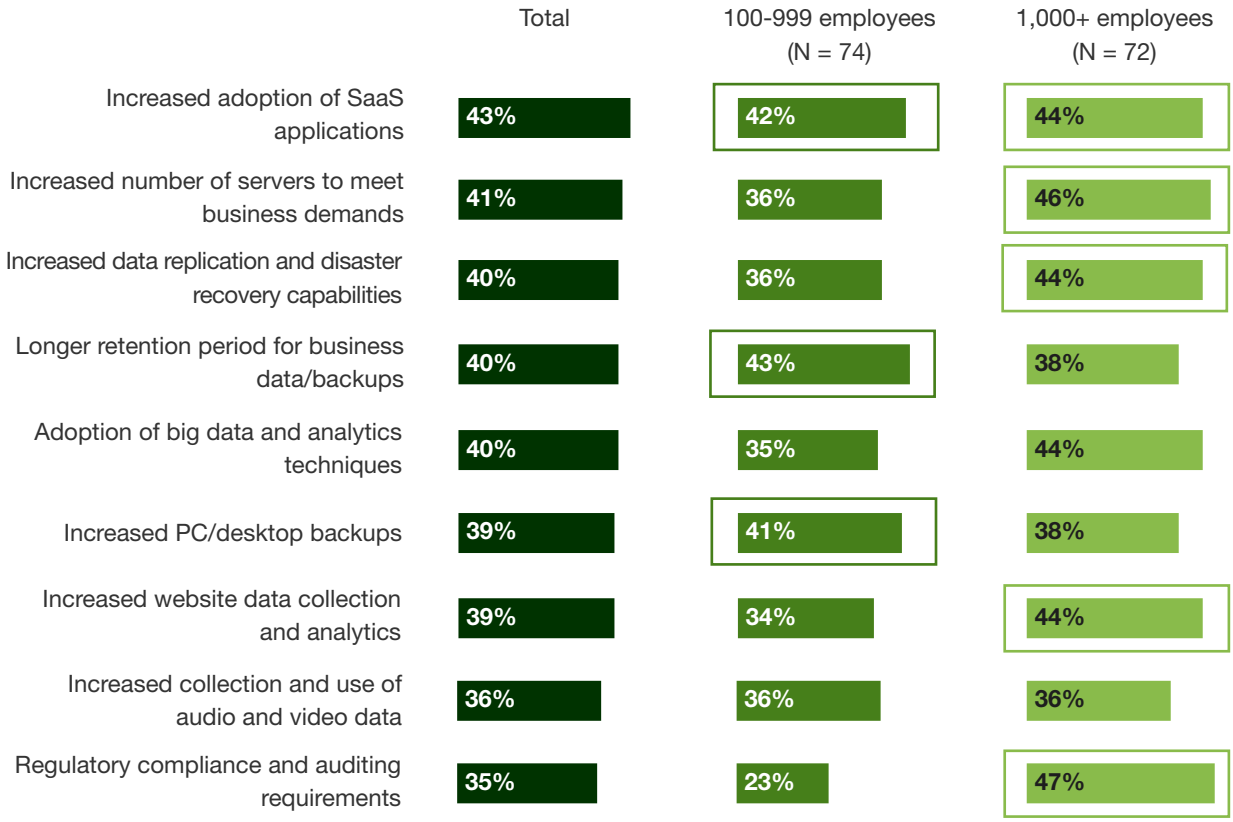
› **The demand for businesses to scale capabilities drives data growth.** Today's organizations rely on data for competitive advantage. They are deploying mobile and SaaS applications to serve customers, employees, and partners in their moment of need; generating more data per transaction. Many are also investing in data warehousing or big data projects to generate just-in-time promotional campaigns. Our study revealed that the growth in data enterprises are storing maps to this increasing demand for capacity and capabilities: Roughly four out of 10 organizations point to a greater number of SaaS applications, an increase in data center capacity, increased collection of website data, and adoption of big data and analytics techniques as key drivers (see Figure 3).

› **Regulatory and compliance requirements equals more data.** Regulatory and compliance pressures are also fueling an uptick in the amount of data being stored, as reported by one-third of respondents. These requirements are, in fact, the No. 1 driver of data growth among large enterprises. Current data retention and privacy regulations mandate storing data for years; for some industries, like healthcare, indefinitely. Additionally, organizations must back up, replicate, and have the capability to recover larger volumes of data. This demand for increased data replication and enhanced disaster recovery capabilities is further driving data growth. Meeting reguatory and compliance requirements for data is no easy task, however — over half of respondents reported their organizations had one or more instances of non-compliance with data retention or data privacy regulations over the past two years.

Increased adoption of SaaS applications is the No. 1 driver of data growth.

Figure 3

"What factors are driving the increase in the amount of data stored by your organization?" (Select all that apply.)



Base: 146 IT professionals at organizations in the US and Canada that have experienced an increase in the amount of data stored over the past two years
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Today's Data Environment Is Getting Increasingly Complex

Enterprises today distribute their business applications — and by extension, their data — across multiple data centers on-premises, at managed data centers, and in the cloud. This results in numerous technology stacks storing data that is vital to the business. While most enterprise data is still stored in physical servers and databases — accounting for an average of 23% and 22% of data stored — as organizations move to the cloud and increasingly embrace enterprise mobility, a considerable amount of data is also residing in virtual machines (19%), endpoints (19%), and SaaS applications (18%).

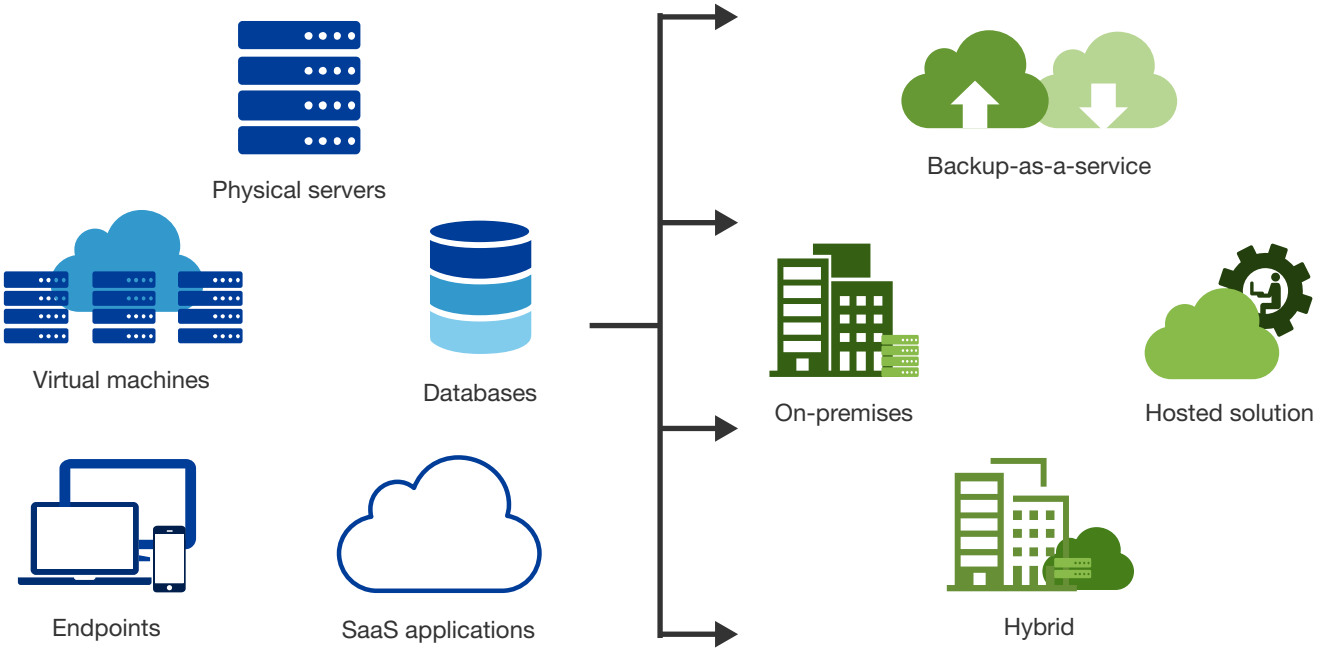
No single solution can address this vast range of technologies, meaning enterprises need more than one tool to cover all data sources and the full data life cycle. The targets for enterprise data are equally as diverse as the sources — organizations have multiple options for backing up data (see Figure 4).

Backup options span technologies and locations, including:

- **On-premises.** The backup solution resides on-premises and pushes data to the on-premises backup infrastructure, with purpose-built software, hardware, tape, or replication offsite.
- **Hybrid.** An on-premises backup solution that pushes the data to on-premises, public cloud, or service provider infrastructure. Hybrid backup uses on-premises storage for recent backups and cloud for archival. Data movement is governed and managed by policies.
- **Hosted.** The backup solution is delivered as a managed service by a managed services provider (MSP) that pushes the data to the MSP environment. The backup software is hosted in cloud servers, utilizing warm storage.
- **Backup-as-a-service.** A backup solution delivered as a managed service by a cloud service provider that pulls on-premises, hosted, or SaaS data and backs it up in a highly available cloud infrastructure. Backup-as-a-service is built from the ground up in cloud, utilizing native services.
- **Edge computing.** An explosion of IoT systems and the associated edge computing infrastructure has not yet been a major issue, but it will be. Most edge data is sent to a central location or summarized and then discarded. More of this data will require inclusion as just another element of the overall resiliency architecture.

Figure 4

Sources and backup options for enterprise data span technologies and locations:



Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

ORGANIZATIONS STILL RELY HEAVILY ON ON-PREMISES BACKUP AND RECOVERY

Although enterprises are reconfiguring their architecture to provide capabilities that extend to this new data landscape, on-premises backup and recovery still plays a significant role, with 50% or more respondents using on-site solutions to backup data residing on endpoints, servers, and in databases; 45% are backing up virtual machines on-premises (see Figure 5). Despite the reliance on on-premises, enterprises do use a varied approach to backup and recovery, using cloud-based targets in addition to traditional approaches. Roughly one-third of organizations tap hybrid or cloud-based solutions for database backup and recovery, while backup-as-a-service is the predominant target for SaaS applications.

Thirty percent cite **backup and recovery systems complexity** as a challenge.

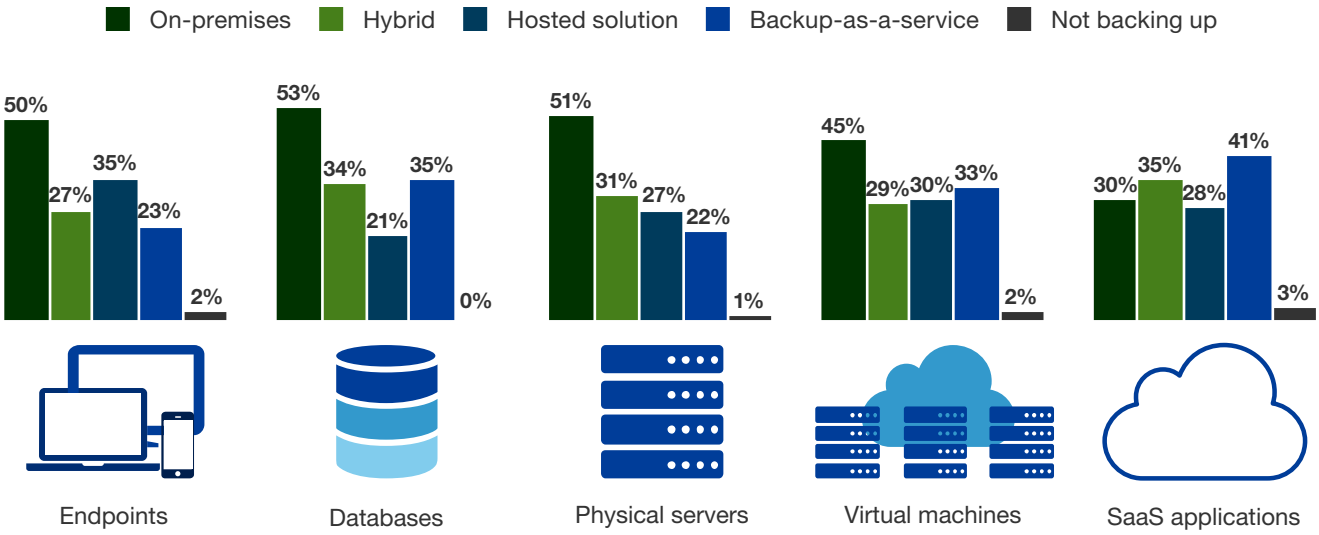
DATA BACKUP AND RECOVERY IS COMPLEX AND SILOED

As organizations move data from a variety of sources to a variety of targets, their data backup and recovery approach is becoming more complex and siloed. Seventy-nine percent of enterprises are using three or more backup and recovery solutions; of that, 26% are using five or more. One solution may not, in fact, cover the entirety of an enterprise's technology landscape — particularly if it's running a highly heterogeneous technology stack. However, using multiple point solutions for different applications, locations, or resiliency models only increases enterprise complexity.[2]

FORRESTER®

Figure 5

"What approaches is your organization using for data backup and recovery in each of the following areas?"
(Select all that apply.)



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

The challenge this presents is not lost on the IT professionals we surveyed: Three out of 10 respondents indicated that their existing backup and recovery systems are too complex. This decentralized approach extends to the way organizations are managing the process: 51% report they have multiple people or teams managing data backup — whether organized by source, line-of-business, or both; 1% take an ad hoc approach, with no one within the organization formally responsible for the task (see Figure 6).

The complexity with which many enterprises are approaching the management and process of data backup and recovery can result in gaps in capabilities and integration challenges, including: limited or no backup of remote or branch offices (37%); legacy systems that are inadequate for archiving needs (29%); lack of integration between distributed data sources (33%); and difficulty integrating legacy systems with new backup solutions (28%).

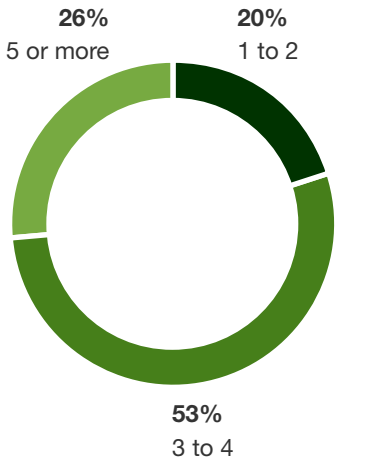
Current Data Backup And Recovery Practices Introduce Risk Of Data Loss

Many organizations are leaving the door open for data loss. Lack of a connected, comprehensive approach to data backup and recovery can result in cracks through which valuable enterprise data can fall. Some complexity is warranted, but too much invites catestrophic failure. Thirty-four percent of the IT professionals surveyed acknowledged that their organization's current distributed environment presented an increased risk of data loss. Further, a lack of integration between data protection and disaster recovery strategies — an issue cited by 24% of IT professionals — means running the risk that data lost may not be fully recovered.

However, given the sheer volume of data generated and stored by organizations today, it's impossible to apply the same degree of protection to all data. Enterprises, therefore, must classify and prioritize applications and the related data based on its value and associated cost to the business, should data be lost.

- **Mission-critical.** Data pertaining to customer-facing, revenue-generating applications. This data needs to be preserved for regulatory compliance. Loss of this data results in significant cost to the business. Forrester estimates that approximately 30% of enterprise data is mission-critical.[3]
- **Business-critical.** Data pertaining to applications that power business processes and drive insights. Loss of this data results in considerable cost to the business. Roughly one-third (34%) of data falls within this category.
- **Noncritical.** Data pertaining to non-customer-facing or revenue-generating applications; internal operations data that support the business. This data requires protection, but its loss may not stall the business. Approximately 36% of enterprise data is classified as noncritical.

Number of data backup and recovery solutions in use:

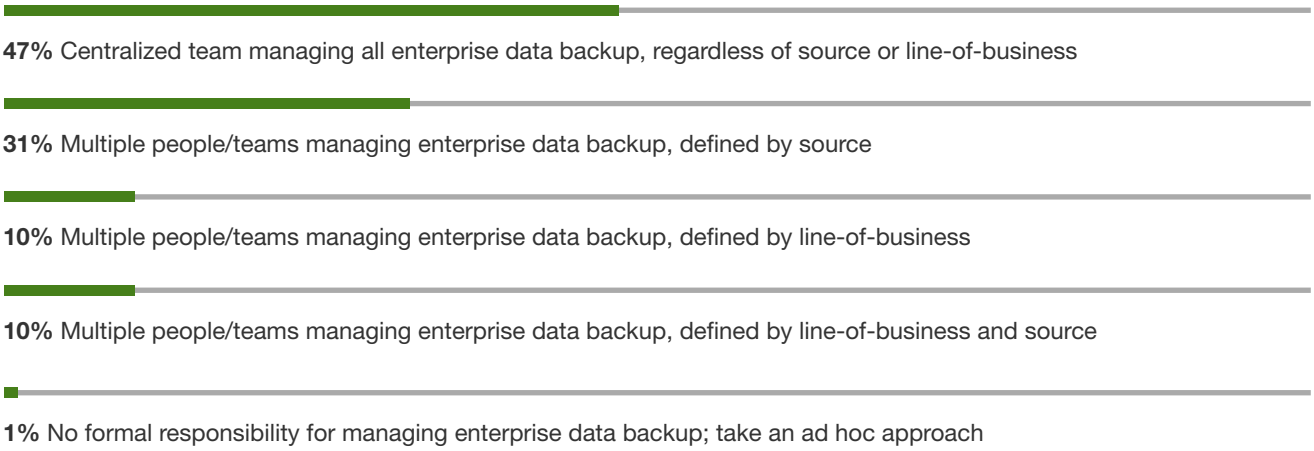


Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Seventy-nine percent of organizations use **three or more** data backup and recovery solutions.

Figure 6

"Which of the following best describes your organization's approach to managing data backup and recovery?"

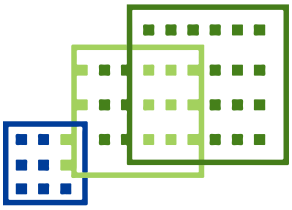


Note: Percentages may not equal 100% due to rounding
Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

MANUAL BACKUP OPERATIONS ARE INADEQUATE

Mission- and business-critical data account for roughly two-thirds of enterprise data and applications, yet our study revealed that many organizations suffer from inadequate backup schedules. Our study found that while most enterprises are regularly backing up their most important data, there is room for improvement: Just 51% of organizations are backing up their mission-critical data every night; 45% are backing up business-critical data with similar frequency (see Figure 7). Shockingly, many organizations are only backing up mission- or business-critical data once a week; even more alarming — some do not have backups scheduled.

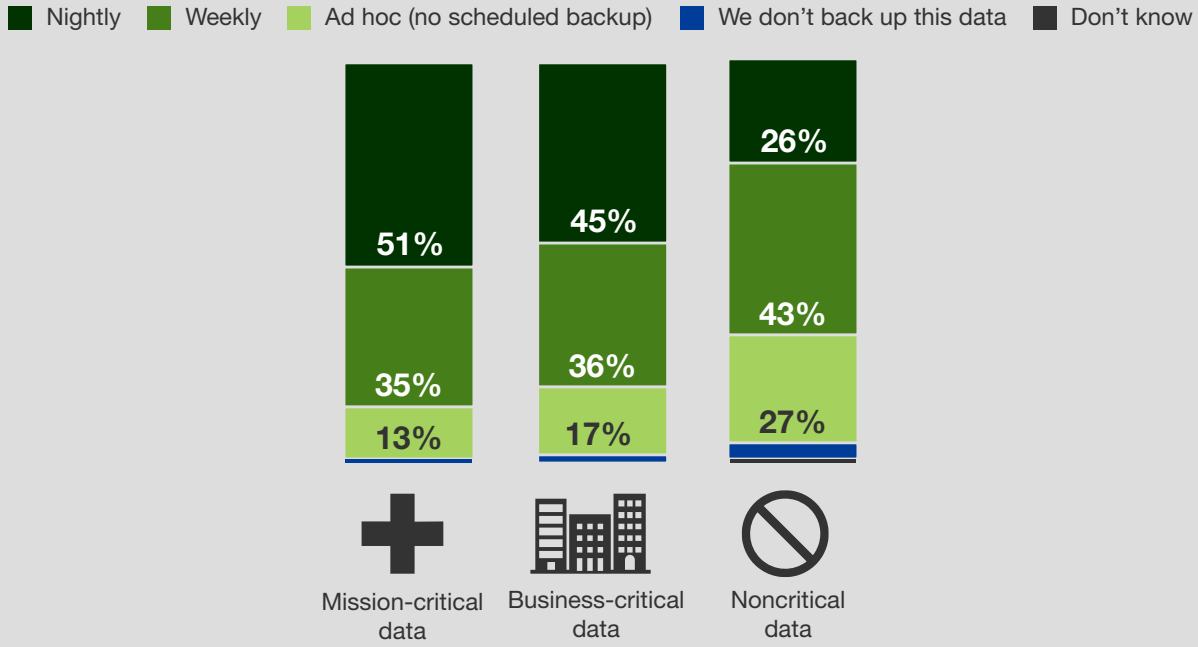
Compounding the issue, a surprisingly high number of organizations still manually backup their most important enterprise data: Over half of those surveyed use manual backup — either solely, or in combination with automated processes — to back up mission- and business-critical data (see Figure 8). A recent joint Forrester/Disaster Recovery Journal study found that organizations are still backing up mission- (21%) and business-critical (31%) data locally to tape and then transporting those tapes to a recovery site. Manual backup processes are by no means fail-safe — our study found that 34% of IT professionals have encountered errors caused by manual data backup, while 41% reported a high incidence of failures in tape backups. These shortcomings only increase the risk that valuable data will be lost.



Over half of organizations use **manual processes** to back up their most-important data.

Figure 7

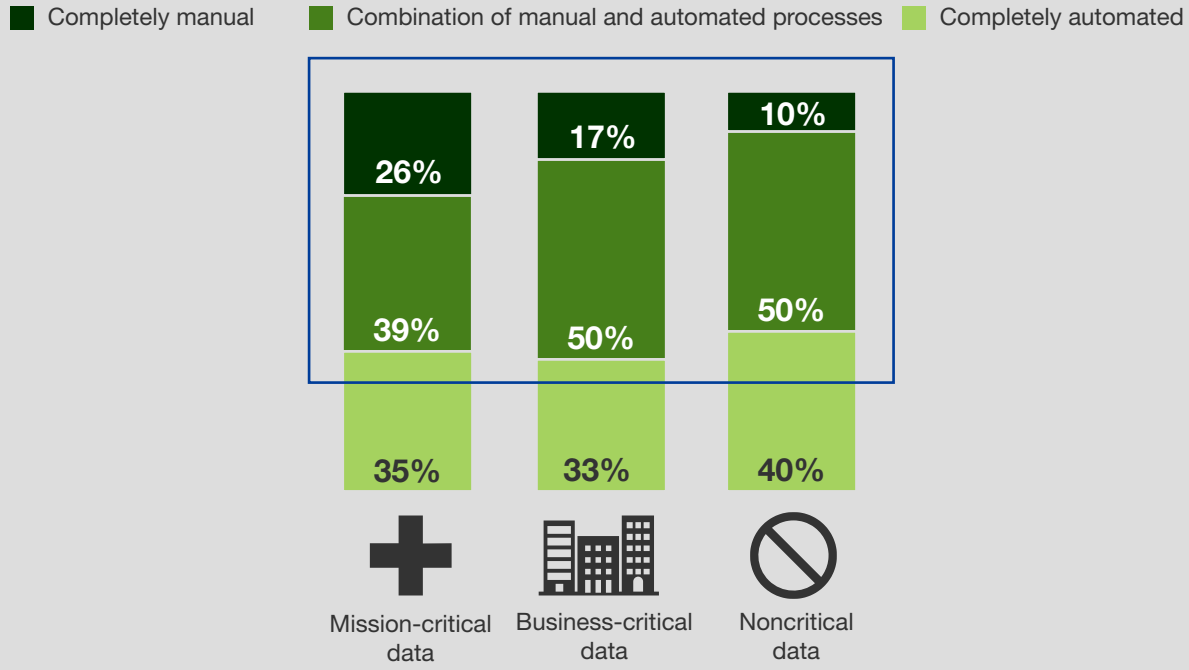
"How often do you backup your organization's mission-critical, business-critical, and noncritical data?"



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Figure 8

"Are the backup processes for this data automated or manual?"



Base: Variable; IT professionals at organizations in the US and Canada that are backing up enterprise data
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

FORRESTER®

Many Firms Struggle With Data Protection And Governance

Data is the lifeblood of any organization. If critical data is lost or corrupted, customer experience can suffer tremendously, and business operations can come to a standstill. No matter how confident you may be in your data backup strategy, no organization is immune to data loss. Our study revealed that loss of critical data is a common occurrence: Over three-quarters of the organizations surveyed have lost mission- or business-critical data over the past two years. Forty-three percent reported three or more incidents of loss of critical data; an unfortunate 14% experienced greater than five incidents of data loss.

Firms lose data for many reasons, inclusive of systems failures, service outages, power failures, malicious insiders, user error, and hacktivists. Hacktivists, in particular, have been grabbing headlines. Ransomware — a form of malware that exploits the human element, the widespread dependence on electronic data, and the high probability that targeted victims do not back up their data at all or reliably — has been on the rise in recent years.[4] In fact, of those respondents experiencing one or more incidents of mission- or business-critical data loss, 50% pointed to ransomware as the culprit. Unfortunately, few could fully recover data lost in the attack — just 26% recovered 100% of their data (see Figure 9). Indeed, "insufficient recovery" is a challenge for organizations, cited by 38% of those surveyed.

Enterprises require round-the-clock, always-on operations across all locations to remain competitive. In fact, loss tolerance is near zero for critical business applications.[5] Today's IT organizations are not only dealing with stemming the tide of data loss, they are also under the gun to quickly restore data. Fifty-six percent of those surveyed report that there is greater demand for quicker restores. Yet IT professionals are struggling to meet these demands: Just two-fifths are consistently meeting SLAs for mission- (39%) or business-critical (40%) data (see Figure 10). It's not enough to meet SLAs some or most of the time. Anything less than all the time — particularly when it comes to mission- or business-critical data — is unacceptable.

Backup and recovery strategies **must adapt to new business demands.**

Forty-three percent of organizations have experienced **three or more incidents of data loss** over the past two years.

Thirty-eight percent of IT professionals cite **"insufficient recovery"** as a challenge.

Figure 9

"To what extent were you able to recover the mission- and/or business-critical data lost as a result of a ransomware attack?"

26% 100% of data was recovered

33% 75% to 99% of data was recovered

35% 50% to 74% of data was recovered

5% Less than 50% of data was recovered

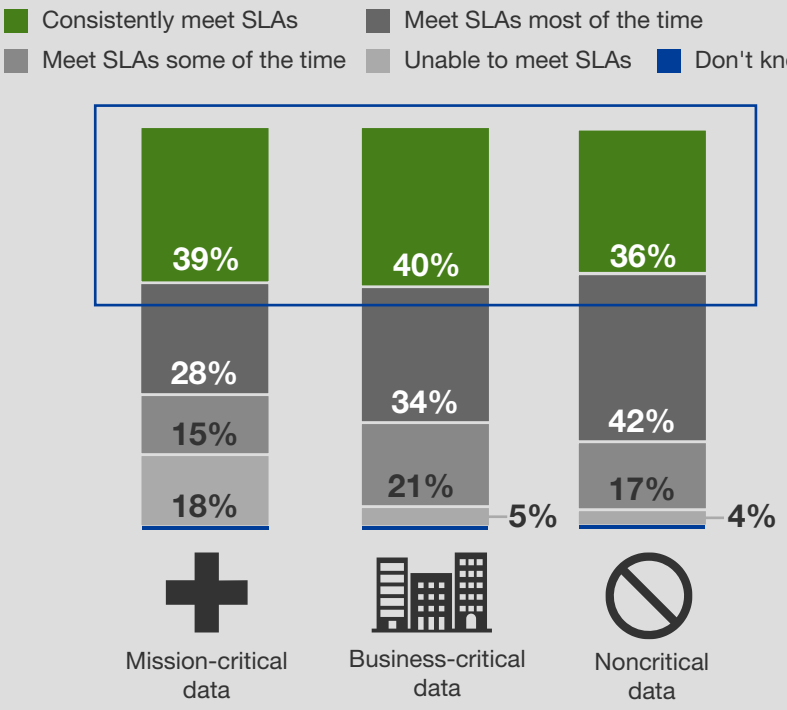
0% We were not able to recover lost data

Note: Percentages may not equal 100% due to rounding
Base: 57 IT professionals at organizations in the US and Canada that have lost mission- or business-critical data within the past 24 months due to a ransomware attack
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Fifty percent of mission- or business-critical data loss was the result of a **ransomware attack.**

Figure 10

"How well are you meeting data protection SLAs (recovery time objectives (RTO) and recovery point objectives (RPO)) for mission-critical, business-critical, and noncritical data?"



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Just **two-fifths** of organizations are **consistently meeting SLAs** for mission- and business-critical data.

FORRESTER®

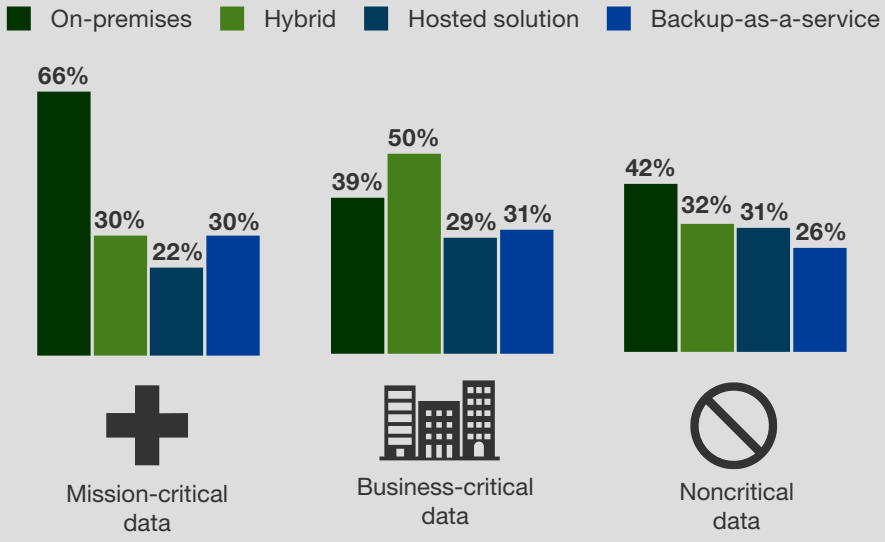
Organizations Embrace Cloud For Business-Critical Data

On-premises approaches have been the mainstay for decades, so most traditional workloads (including mission-critical systems that have been mission-critical for almost as long) fit this model. Our survey found that 66% of organizations back up mission-critical data on-premises — the predominant target for this data compared with hybrid, hosted, or backup-as-a-service solutions (see Figure 11). Established systems have inertia, so they don't shift to cloud or hybrid models easily. Additionally, these systems are seldom supported by new-age cloud or hybrid technologies: Systems like mainframes and proprietary technologies are just not supported in the cloud. The real issue is "data gravity," which mandates that the backup technology be in close physical proximity to the mission-critical data being backed up. Laws of physics dictate this because moving lots of data over long distances takes time, and when it comes to mission-critical data, time can literally mean money.

This data gravity also explains why 50% of respondent organizations are using a hybrid approach to back up business-critical data. Systems of engagement, like web and mobile apps, directly touch customers and partners. Newer and more likely to reside in public cloud services, their data is both on-premises and in the cloud, a by-product of the distributed architecture of more modern software. While used to a lesser extent, organizations are also using hosted and cloud-based solutions to back up business-critical data.

Figure 11

"What approach or approaches are you using to back up this data?" (Select all that apply.)



Base: Variable; IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

FORRESTER®

ORGANIZATIONS ARE TURNING TO CLOUD TO MITIGATE DATA CHALLENGES

SaaS adoption is growing across all industries and enterprises of every size. Forrester predicts that the SaaS market will grow to $157 billion in 2020.[6] This rapid growth in SaaS usage results in proportional growth in the movement of business data from on-premises to the cloud instances. As organizations increasingly adopt SaaS applications, they are discovering that data protection for these apps cannot be assumed — many SaaS vendors leave this in the customers' hands. It comes as little surprise, therefore, that the need for data protection for SaaS applications topped the list of reasons organizations we surveyed are using the cloud for backup and recovery of business-critical data (see Figure 12). Use of the cloud for disaster recovery has been increasing slowly, but steadily, over the past few years. The most recent Forrester/ Disaster Recovery Journal survey revealed that 18% of firms are using the cloud in some way as a recovery site — an increase from 15% in 2013 and 4% in 2010.[7]

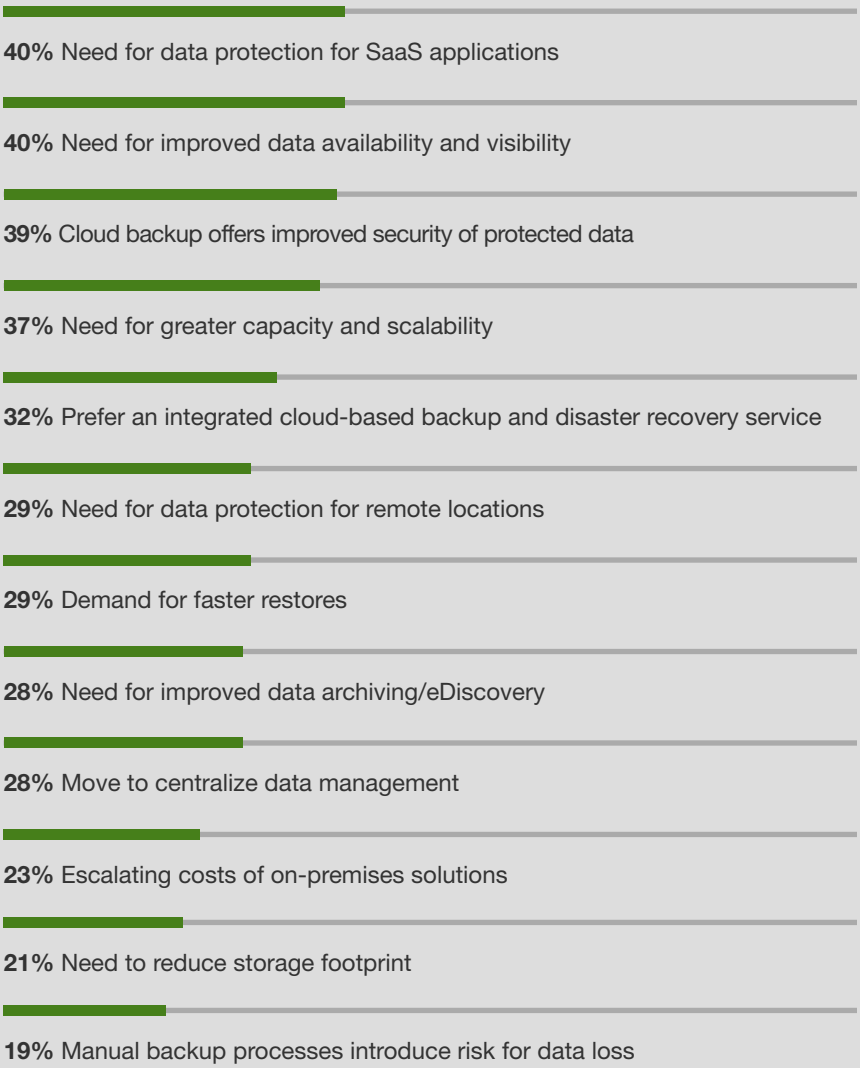
Our study revealed other key drivers of cloud backup and recovery, including:

- **Improved data availability and visibility.** Backing up business-critical data to the cloud helps organizations overcome the challenges that come with distributed, siloed architectures. Lack of data visibility can result in costly compliance and regulatory data risks. Our study found that 40% of organizations turn to backup and recovery in the cloud for better data availability and visibility.
- **More capacity and agile scalability.** Roughly four out of 10 respondents say their organizations use cloud backup and recovery for business-critical data due to the need for more capacity and scalability. Leading cloud services have virtually unlimited storage and compute capacity for backup and this capacity can automatically and immediately expand and contract as needed. As data volumes continue to increase, the flexibility of the cloud provides what on-premises backup can't.
- **Inherent design for dependability.** With on-premises storage infrastructure, a power outage or hardware failure could spell disaster — restoring operations could take hours or days, and any data that had been backed up and then removed may be lost forever. Customer experience can suffer enormously. In cloud, the environment's configuration itself is data that is replicated and designed to be dependable, so the entire system can resume operation quickly. It comes as little surprise, therefore, that nearly one-third of the IT pros surveyed cited the demand for faster restores as a driver for their organizations' use of the cloud for backup and recovery.
- **Lower infrastructure costs.** Nearly one-quarter of organizations turn to the cloud for backup and recovery due to escalating costs of on-premises solutions. Classic on-premises storage and backup comes with some fundamental expenses, including hardware costs, costly management, license fees for purpose-built software; as well as hidden costs like bandwidth, ongoing maintenance, electricity, and equipment replacement. The US Energy Information Administration

estimates that the cost to operate a single server for one year is $731 — for the electricity alone.[8] Cloud backup and recovery infrastructure is managed at scale with costs that are more predictable, transparent, less complex, and based on consumption. And as enterprises are challenged to control infrastructure costs in the face of explosive data growth, over one-fifth turn to cloud backup to help reduce their storage footprint.

Figure 12

"What factors drove your organization's decision to use the cloud for backup and recovery of business-critical data?" (Select all that apply.)

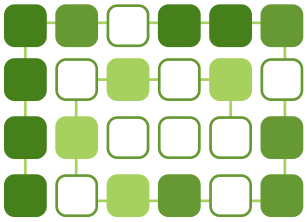


Base: 119 IT professionals at organizations in the US and Canada that use the cloud for backup and recovery of business-critical data
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

FORRESTER®

Wanted: Simplified, Unified Data Management

Given the challenges with managing and protecting enterprise data, IT professionals want a data protection solution that does it all. As previously discussed, organizations are using multiple solutions for data backup and protection. As a result, IT pros must navigate multiple consoles, making managing data protection incredibly difficult. According to the study respondents, the ideal solution would not only have the capabilities they need to better protect data, meet the tighter SLA windows the business demands, and ensure compliance; it would also reduce the complexity of managing and protecting data stored in all sources through a single plane of glass (see Figure 13).



Eighty percent would be very or extremely likely to adopt **an integrated data-protection-as-a-service solution.**

DATA PROTECTION-AS-A-SERVICE IMPROVES THE SCOPE OF BACKUP AND RECOVERY

Because data gravity dictates data protection strategies, an optimum protection solution will cover your data where it lives — but with a centralized point of interactions and control. Such a federated architecture is complex, but good solution design and packaging will hide this complxity. Those who use the system should percieve a simple approach to a complex solution. The heart of this mode of data protection is built on the cloud and delivered through a SaaS model, enabling the provision of data policy management, visibility, accessibility, and recoverability across multiple data sources —on-premises, SaaS, and cloud workloads — all through a centralized control plane. Ninety-two percent of study respondents indicated the ability to centrally manage and protect data across all sources was one of the most important capabilities they seek when evaluating data protection solutions.

Our survey showed strong indicators that organizations are receptive to unified data protection in a cloud-based delivery model. When asked the likelihood they would adopt a data protection-as-a-service solution inclusive of all the capabilities they deemed important (i.e., one including the capabilities in Figure 13), 80% said they would be very or extremely likely to adopt it.

The centralized data management available in a unified data protection-as-a-service solution enables organizations to better meet data security, recovery, and compliance needs. Study respondents identified key benefits, including:

› **Better data security.** Security concerns have historically been a top barrier to cloud adoption, often used by hesitant data storage and recovery teams to slow cloud deployments. Forrester believes, however, that cloud security is both a major strength and driver of cloud adoption, providing superior security to that of the average enterprise.[9] Indeed, the IT professionals we surveyed identified improved data security as the No. 1 benefit of using a unified data protection-as-a-service solution, cited by 47% (see Figure 14). Protection from malware — a key security concern today — was noted by 87% of respondents as a somewhat or very important data protection capability.

Figure 13

"How important are the following capabilities when evaluating data protection solutions?"

Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

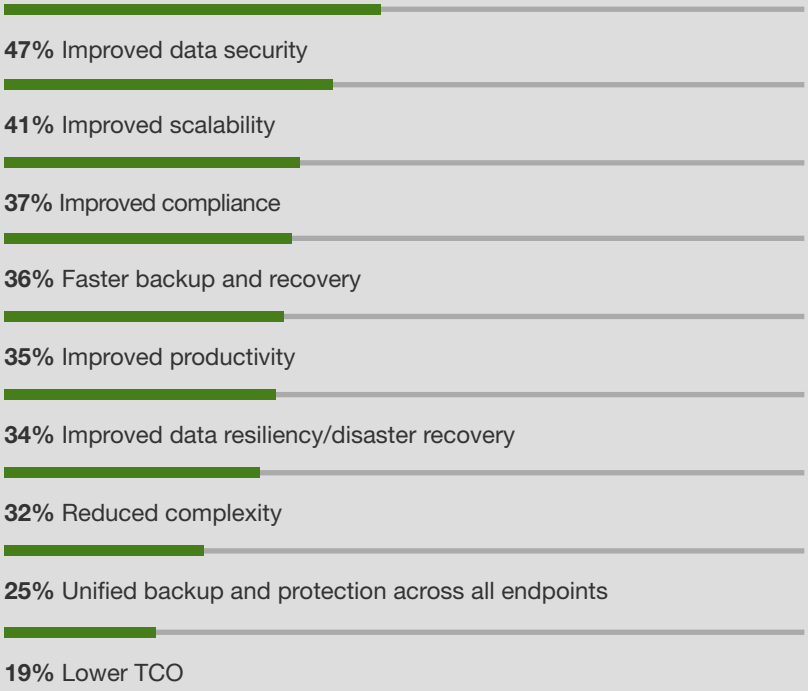
FORRESTER®

› **Reduced complexity.** Integrating myriad technologies to protect and make data continuously available is a struggle for many organizations. Data protection-as-a-service — through the use of a single control plane — provides unified data backup and protection across all sources, a benefit cited by 25% of respondents. Having the ability to centrally manage today's distributed data environments eliminates the need for IT pros to juggle multiple consoles, cited by 92% as an important data protection feature. A unified interface also provides improved visibility into end-user data; and makes it easier to define, manage, and automate policies across all sources and locations.

› **Enhanced scalability to meet the demands of today's data environment.** On-premises backup and data protection cannot keep up with the explosion of data most organizations are facing today, since storage space and computing availability are limited by hardware constraints. With cloud-based solutions, the cloud scales up and down when capacity requirements change, easily adapting to changing business needs. Identified by 85% of respondents as a highly desirable data protection capability, it was also selected as a key benefit of using data protection-as-a-service by 41%.

Figure 14

"What benefits have you realized, or could you potentially realize, by using a data protection-as-a-service solution with these capabilities?"
(Select all that apply.)



Base: 148 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Fifty-seven percent of IT pros at organizations using **backup-as-a-service** reported they were consistently meeting SLAs compared with **45%** mainly using **on-premises solutions.**

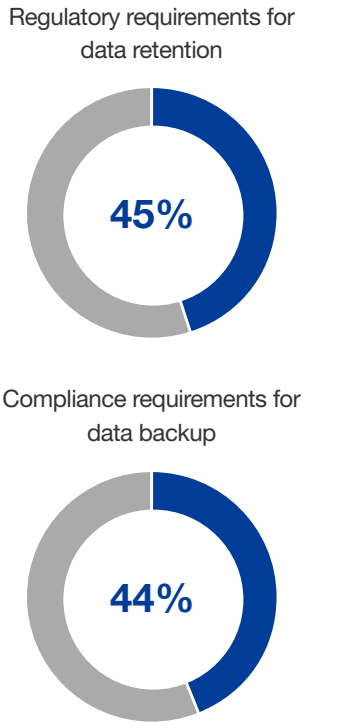
FORRESTER®

- **Improved compliance.** The distributed nature of modern enterprise computing environments means that data can be stored anywhere, limiting data visibility. At the same time, enterprises are under pressure to ensure data backup and recovery practices meet regulatory and compliance requirements — something roughly four out of 10 organizations struggle to attain (see Figure 15). Centralized controls for federated search, audit, monitoring, and legal hold management can enable better data governance and help enterprises identify and remediate data risks before they rise to crisis level. Over one-third of respondents said a data protection-as-a-service solution inclusive of these capabilities would improve their compliance posture. More than half (53%) of organizations see compliance as very important to their resiliency needs. As compliance pressures increase with initiatives like GDPR, this number will increase.
- **Better ability to recover from data loss.** As discussed, many organizations struggle with insufficient data recovery. It comes as little surprise, therefore, that "data resiliency/disaster recovery" was the No. 1 capability IT pros seek in a data protection solution. Our study found that the use of cloud-based backup improves recovery outcomes. Recognizing that no single data protection solution will meet all enterprise data backup and recovery needs, those organizations in the study using backup-as-a-service were more likely to meet the demands for fast data recovery: 57% reported they were consistently meeting SLAs, compared with those predominately using on-premises solutions (45%). Data protection-as-a-service uses various methods to ensure SLAs are achieved without requiring heavy investments in additional infrastructure. And while these approaches could include some on-premises presence to achieve RTO requirements, the system isn't dependent on that. Data protection-as-a-service is purpose-built to take advantage of the storage, compute, and efficiency capabilities of the public cloud.

Unified data protection remains difficult, but it places the burden of simplifying the solution on the vendors. They can — and should — simplify everything for you. Your data is everywhere and it all needs to be protected through the same system. Public cloud has proven to be the best platform for a consolidated interface to this highly distributed system. Seek flexibility, speed, simplicity, and seamless integration in your data protection solutions. Solutions like data protection-as-a-service, data management-as-a-service (DMaaS), DR-as-a-service (DRaaS), and cloud data replication, all help to ensure the dependability of your data. Data integrity is of utmost importance to the business because your customers depend on you to protect your technology — and them.

Figure 15

"What challenges does your organization face relating to data backup and recovery?"
(Select all that apply)



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

Key Recommendations

While cloud services should never be viewed as a panacea, the cloud model offers notable benefits for enterprise data protection. Forrester's in-depth survey of 150 IT professionals on data backup and protection strategies yielded several important recommendations:

Periodically review data classification with business stakeholders. Backup administrators often classify protected data into various categories based on their experience and apply data protection policies accordingly. Not that it is wrong, but the policies are rarely reviewed — and thus rarely adapt to new demand like cloud. In a changing environment, it is highly likely that the business stakeholders' expectations around backup and recovery have also changed.

Automate backup policies to reduce risk of data loss. Our study found that many organizations still rely on manual processes to back up their mission- and business-critical data, pointing to ineffective policies. With enterprise application data volumes ranging in the petabytes, managing data protection via manual methods is asking for disaster. Also, as cloud, DevOps, and other automation movements accelerate the pace of change, automation becomes mandatory. A cloud-based approach fits well with this new mode of approaching automation, but on-premises elements will also be essential. Further, automating backup policies not only increases speed, it significantly improves quality by eliminating human error.

Consolidate backup and recovery solutions. Many organizations suffer from "an excess of expertise," having implemented sprawling backup and secondary storage infrastructure from multiple vendors.[10] This complexity exacerbates the difficulty of data protection. Integrated backup and data protection not only helps drive technological and economic benefits, but it also provides greater visibility into systems and centralized management via a single plane of glass. Incumbent systems are firmly entrenched, so integrating them with gradual — as opposed to immediate — replacement is better. The flexibility of a data protection-as-a-service delivery model helps with this approach.

Leverage data protection-as-a-service to improve technology. Highly distributed firms struggle to ensure 100% coverage of the deployed technology across a hub-and-spoke organizational model. Remote and branch offices pose a particular challenge that edge computing will exacerbate even more. The flexibility and scalability of data protection-as-a-service solutions enable organizations to improve coverage of such distributed data that is important, but historically could not be backed up.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 150 organizations in the US and Canada that have deployed or are expanding the use of hypervisor technology to evaluate data backup and protection strategies. Respondent organizations ranged in size from 100 to 5,000 or more. Survey participants included decision makers at manager level and above with responsibility for: their organizations' IT infrastructure or operations; data center and servers; cloud services/virtualization; or storage and backup. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was fielded in November 2017.

Appendix B: Demographics

"In which country are you located?"

US
67%

Canada
33%

"Using your best estimate, how many employees work for your firm/organization worldwide?"

15% 5,000 or more

35% 1,000 to 4,999

28% 500 to 999

22% 100 to 499

"Which title best describes your position at your organization?"

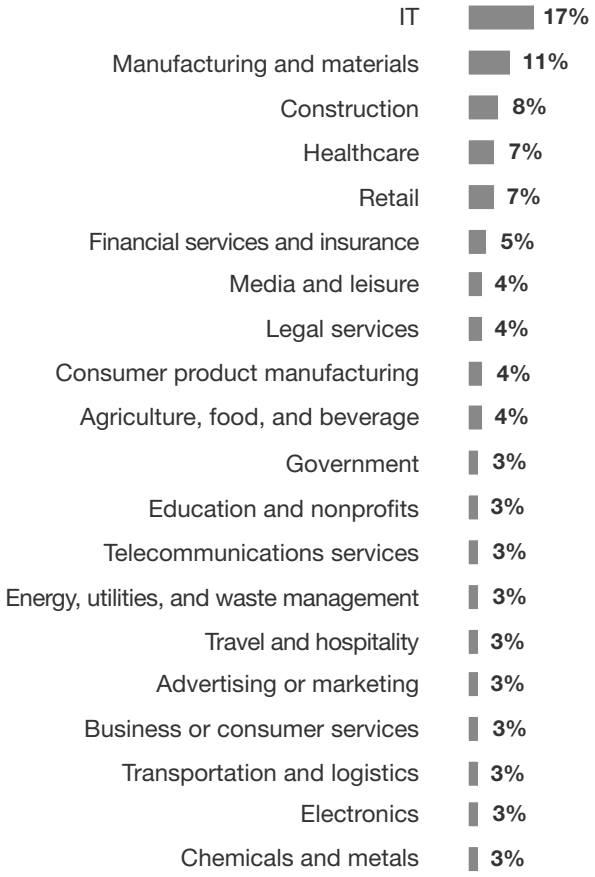
16% C-level executive

34% Vice-president

26% Director

24% Manager

"Which of the following best describes the industry to which your company belongs?"



Base: 150 IT professionals at organizations in the US and Canada
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, November 2017

FORRESTER®

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"Three Vendors Disrupting Integrated Secondary Storage And Data Protection," Forrester Research, Inc., October 30, 2017.

"The State of Business Technology Resiliency, Q2 2017," Forrester Research, Inc., July 14, 2017.

"Embrace Cloud Economics For On-Premises Enterprise Storage," Forrester Research, Inc., May 18, 2017.

"Back Up Your SaaS Data — Because Most SaaS Providers Don't," Forrester Research, Inc., December 29, 2017.

"Vendor Landscape: Data Resiliency Solutions, Q3 2016," Forrester Research, Inc., August 25, 2016.

"Brief: New Data Resiliency Approaches Render Backup Obsolete," Forrester Research, Inc., February 5, 2016.

Appendix D: Endnotes

[1] Source: "How big is a petabyte, exabyte or yottabyte? What's the biggest byte for that matter?" ZME Science, March 17, 2017 (https://www.zmescience.com/science/how-big-data-can-get/).

[2] Source: "Vendor Landscape: Data Resiliency Solutions, Q3 2016," Forrester Research, Inc., August 25, 2016.

[3] Source: Forrester/Disaster Recovery Journal November 2016 Global Disaster Recovery Preparedness Online Survey, Forrester Research Inc.

[4] Source: "Ransomware Protection: Five Best Practices," Forrester Research, Inc., July 27, 2017.

[5] Source: "Brief: New Data Resiliency Approaches Render Backup Obsolete," Forrester Research, Inc., February 5, 2016.

[6] Source: "Back Up Your SaaS Data — Because Most SaaS Providers Don't," Forrester Research, Inc., December 29, 2017.

[7] The 18% using cloud for recovery includes 10% that use a fully packaged DR-as-a-service offering and 8% that use infrastructure-as-a-service to configure their own DR in the cloud.

[8] Source: "On-Premises Vs Cloud Data Storage: Which Is Right For Your Organization?" Advanced Network Professionals, November 3, 2017 (https://www.getanp.com/blog/8/on-premises-vs-cloud-data-storage-which-is-right-for-your-organization.php).

[9] Source: "Hybrid Cloud Is The Foundation For Storage Agility And Economics," Forrester Research, Inc., April 28, 2017.

[10] Source: "Three Vendors Disrupting Integrated Secondary Storage and Data Protection," Forrester Research, Inc., October 30, 2017.