Progress® DataDirect®

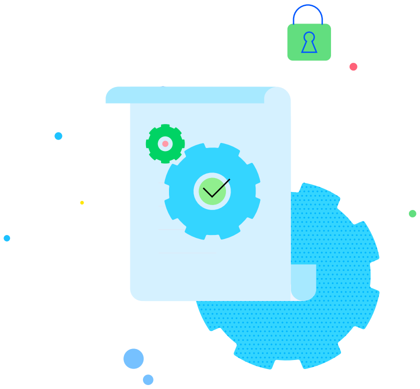
Data Connectivity 2022

Challenges and Opportunities in Modernizing Connectivity When Moving to the Cloud

REPORT

Table of Contents

© 2022 Progress. All Rights Reserved.



1. Executive Summary: Balancing Modernization with Data Accessibility and Data Protection

The 2022 data connectivity survey pivots somewhat from prior years' studies. Data connectivity and data integration are well established in the traditional on-premise computing environment. But we've seen that as organizations increasingly expand their domains to one or more cloud service providers, it is important to better understand the challenges and opportunities for connectivity presented by modernization initiatives.

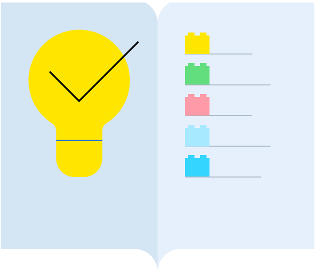
The survey also focused attention on cloud adoption, data migration and the process by which organizations are moving towards a hybrid computing environment. This approach allowed us to explore patterns of data storage in the cloud vs. keeping data in on-premise systems. As organizations expand their data landscapes, there are different needs for data accessibility and simplifying data access using APIs and data services was an important part of the survey. We considered how users are using APIs, who is developing and managing the APIs they use, along with the tools used for API development and implementation.

Most importantly, as concerns grow about the potentially porous nature of the boundaries around a hybrid multicloud data environment, we felt compelled to inquire about respondents' experiences with data security, data protection and other data governance issues such as regulatory compliance. As a result, we were able to infer a more thorough understanding of three key drivers motivating enterprise data modernization: information risk and data protection, data landscape modernization in the cloud and simplifying data accessibility and data democratization via APIs and data services.

Here's a little bit about our respondents: About 80% of the respondents have completed at least a bachelor's degree, with 38% having completed a master's degree and 7% having a Ph.D. Respondents were asked about which roles best describe what they do. The most frequently selected options were Architect/Solutions architect, IT manager and developer, although the range of titles spanned both technical, management, and senior management roles. There were a range of industries represented, with the greatest representation including banking/finance, manufacturing, computer-related products, healthcare, education, retail and insurance.

© 2022 Progress. All Rights Reserved.

The results are intriguing; overall we see small pockets of emerging good practices in combining data policy governance with accessibility of data managed across a distributed environment. We also see opportunities for education and training, especially in the areas of data governance for the purpose of establishing a sustainable and scalable means for managing compliance and ensuring customer confidence. We expect that tools vendors can interpret the results in ways that improve interoperability among different core competencies for managed data connectivity that simplify application development. Data consumers may read the survey results and recognize the tightrope that developers must walk when balancing data accessibility with compliance with data protection and privacy laws. Developers may learn about the need for leveraging better tools to embed data policy compliance into the methods of connectivity.The next section of the report will explore the first theme: information risk, data governance, and data protection. The section following looks at modernization via migrating to the cloud followed by a discussion of our third theme, modernizing connectivity using APIs and data services. Our last theme examines how the responses potentially impact an organization's development tools strategy, and we conclude the report with a short summary.



2. Theme #1: Awareness of Information Risks and Modernizing Data Governance: Compliance, Data Security, Data Protection

2.1 Understanding Information Risk

In general, the concept of risk is associated with the potential or possibility of uncontrolled loss, injury, or other undesired circumstances or consequences. In turn, we can define "information risk" as the potential for loss of value due to inadvertent data exposure, diminished data quality, or other issues associated with the challenges of managing information. The ramifications of ignoring information risks are potentially significant. These impacts to the business may include business disruptions due to the inability to execute operational processes, increased operational costs, decreased revenues, regulatory fines and penalties, as well as other financial impacts attributable to data flaws and data breaches. In turn, damage to an organization's reputation as a result of public awareness of data issues will decrease customer confidence potentially resulting in business loss.

© 2022 Progress. All Rights Reserved.

And while data platform modernization via cloud migration is in vogue, developing a modernization strategy that depends on migrating to the cloud introduces three areas of information risk, namely:

- **Data asset dispersion and distribution.** Data asset dispersion and distribution. As siloed business units increasingly migrate their data assets and their applications to the cloud, the organization's data becomes increasingly dispersed across a distributed multicloud environment. Factor in those data assets that remain on-premise, and the result is increased complexity for managing data across a hybrid multicloud landscape.

- **Data accessibility in the face of hybrid cloud**. There is a clear difference between accessing structured data managed within an on-premise relational database management system and trying to construct a view of data accumulated from multiple cloud-based databases, data lakes or other storage services.

- **Data governance.** Not knowing where data assets are located, whether there is duplication across different cloud platforms, and varying degrees of access controls creates a degree of uncertainty when it comes to establishing data security. With a growing number of laws and regulations governing protection of personal information, ensuring compliance with data security directives has emerged as a discernable area of information risk.

2.2 What were we looking to learn?

It appears that the most pressing information risk today involves data protection and data security. While IT has typically implemented perimeter security intended to prevent breaches at the system level, these controls may not be aware of the corporate data assets that require protection. As a result, when a corporate firewall is breached, this approach provided little, if any, protection of the information managed within the breached environment. As a byproduct, many organizations have launched data governance practices within the past decade, but data security has often been found to lie outside the domain of the data governance organization.

That seems to be changing in accordance with cloud migration (in which data assets are no longer protected behind an on-premise corporate firewall) and the proliferation of laws, regulations and practices to protect sensitive and personal information more effectively. Data policy analysts can better articulate how different classes of information require protection in relation to varying assignments of sensitivity.

© 2022 Progress. All Rights Reserved.

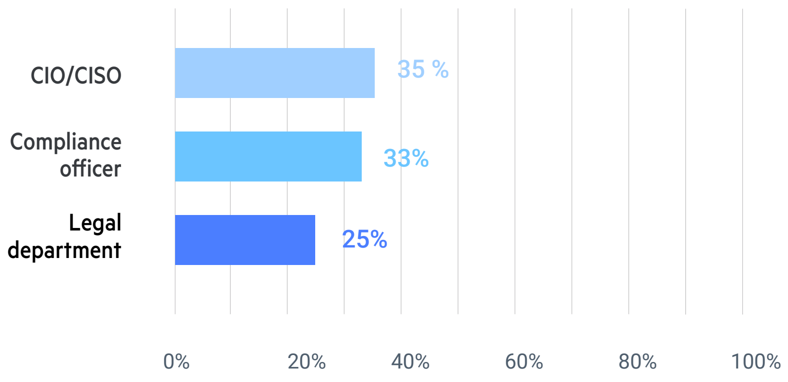
This year's survey solicited information from respondents about their organizations' practices in data security and protection in the context of data governance. We asked questions about what drives organizational requirements for data protection, which roles in the organization are interested in data security, and which roles are responsible and are tasked with data protection policy management. We further drilled down to explore methods, processes, metrics and tools used for ensuring policy compliance. Additionally, our survey looked at the biggest challenges faced in managing data protection and data security policies.

2.3 Results from the Survey

Interest in Data Security and Data Protection

Organizational perspectives of data governance are evolving in concert with increased attention to data security and data protection. The latter has become an enterprise concern, and in this survey, respondents were asked which groups and roles within the organization were interested in data security. Not surprisingly, the groups most interested in data security are IT administrators, architects/solutions architects and security administrators. These answers reflect a relic of traditional platform security management, in which IT administrators managed perimeter security measures to protect against unauthorized entry through the corporate firewall. What was surprising was the frequency of some of the other selections, including the CIO/CISO (35%), compliance officer (33%) and legal (25%). Logically, these three groups/roles should probably be the parties that are most interested in data security!

Figure.1
Interest in Data Security and Data Protection



One consideration would be to drill down into the demographics of the organizations for which the respondents work. While large companies may have individuals assigned to these specific positions (such as CISO), smaller businesses might not have administrative roles clearly defined, nor have separate groups for legal and

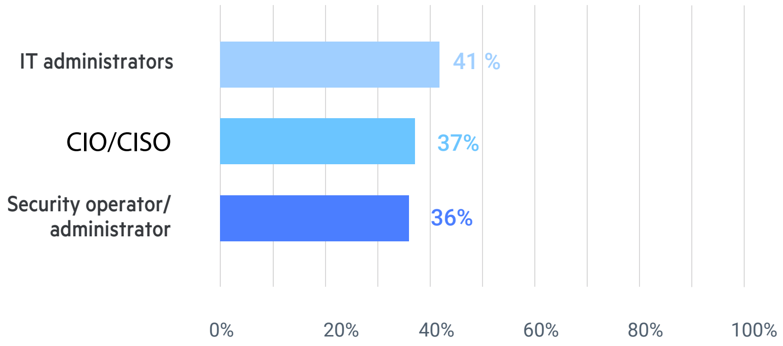
© 2022 Progress. All Rights Reserved.

compliance. This consideration notwithstanding, there are so many technology roles and business operational roles that rely on proper data protection. If anyone's tasks are not performed with the proper diligence and disciplines, it could result in compromised use of or unauthorized access to sensitive data. This suggests that both technology and business roles should be inspired to recognize the need for caution in executing their responsibilities associated with data security and data protection. Disciplined security compliance requires the attention of everyone in the organization.

Responsibility for Data Security and Data Protection

A slightly different question elicited a more expected response. When asked about who is tasked with ensuring data security, 41% indicated that IT administrators were, but 37% of the time respondents selected the CIO/CISO and a similar percentage (36%) opted for the security operator/administrator. Again, because there are IT administrators in nearly all organizations having IT functions, it is not unexpected that this role bubbled up to the top.

Figure.2
Responsibility for Data Security and Data Protection



Data Security Challenges

The survey asked respondents to select their opinions about the most challenging data security processes and systems to integrate and follow. The most challenging data security processes and systems selected by over a fourth of the respondents are data encryption, RBAC (role-based access control), authentication, intrusion detection and avoidance and data leak prevention.

These choices represent a more traditional set of approaches to data protection: guard against unauthorized access, try to prevent breaches and encrypt data just in case. A more nuanced perspective would indicate that organizational perspectives on data protection and data security are immature in the context of data modernization and evolution to a

© 2022 Progress. All Rights Reserved.

hybrid multicloud environment. Low frequency selection of choices such as data masking and obfuscation, content classification, attribute-based access control and data resiliency probably does not mean these processes are perceived to be easy. Rather, it is likely these techniques and processes have yet to be introduced and adopted.

Existing Data Protection Practices

The survey's question about the data security processes that are currently applied in the organization reinforces our conclusion about maturity of data security and protection from a governance standpoint. While over half of the respondents indicated that their organizations have currently applied authentication, antivirus and/or data backups & recovery, it is surprising that the reported adoption rates for critical protections are not 100%!

Common security practices would expect all devices to require user authentication to gain access to them and all computer devices should have some form of Anti-virus software to protect against virus and malware exploits. In addition, backup and recovery is not just a good data security practice, it is a good data management practice. These answers underline the need for improving data protection practices and adoption of a broader array of techniques for data governance.

Subjection to Regulatory Compliance

Respondents were asked if their organization was subject to any regulatory or compliance requirements in terms of data protection. Almost two-thirds of the respondents replied in the affirmative, while 20% said "no," and an additional 14% said they were "unsure." This is almost certainly a situation where what you don't know can hurt you, especially since any organization is likely to be required to comply with one or more jurisdictional consumer data privacy laws.

The response to this question provides some context to answers to other survey questions related to the use of data protection techniques and tools. The low awareness of any need for regulatory compliance may allow for decreased attention to data security and create new vulnerabilities for data exposure, noncompliance, as well as open the gates for data exploits and ransomware attacks. Exploiting these vulnerabilities can cause a huge disruption to business continuity, affect customer truest and negatively impact corporate reputation.

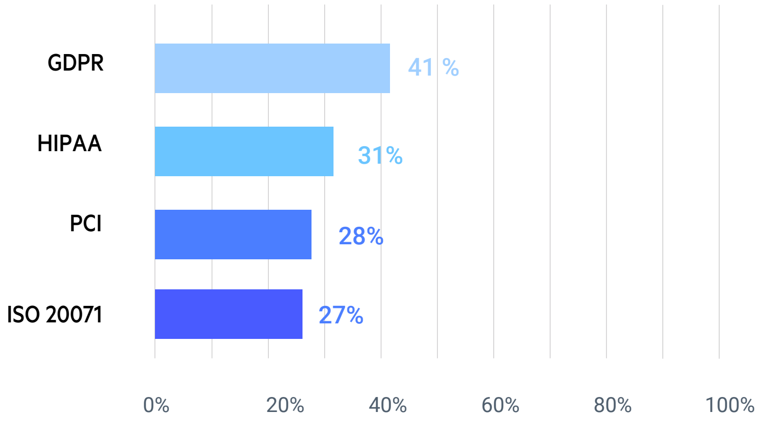
© 2022 Progress. All Rights Reserved.

Regulations to be Observed

A reduced base of those individuals indicating their organizations were subject to regulatory compliance was solicited to identify the regulations their organization needed to comply with. The most frequently reported regulation (at 41%) selected was GDPR, or the European Union's General Data Protection Regulation. This was followed with 31% indicating HIPAA (the US Health Insurance Portability and Accountability Act), suggesting a large contingent of representatives of companies in the healthcare space. The next selection was PCI, or payment card industry data security standard (28%), followed by ISO 20071, the international standard for information security (27%).

Figure.3

The most frequently reported regulation

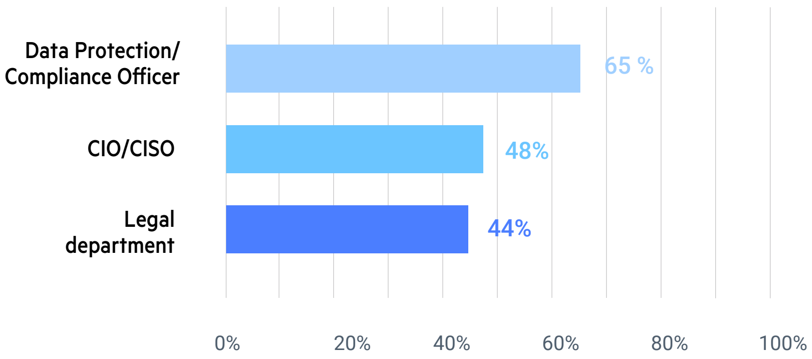


Reflecting on prior surveys highlights that there has been an increase in the number of respondents affirming their organizations must comply with regulatory directives. This suggests two things: first, that despite the large percentage of individuals who are not aware of their organization's compliance obligations, there is bound to be a growing recognition among those who are aware of the compliance demands of the need for the right processes and tools to support data protection and data governance. Second, there are opportunities for vendors in the governance space to augment their products to support simplification of defining data governance policies, automatically implementing security controls, and providing a means for continuous monitoring of compliance.

Interest in Data Governance

The same individuals indicating their organizations were subject to regulatory compliance were asked about interested parties within the organization for data governance and data protection. This reduced set of respondents presumably had a better perspective on accountability for data governance, as 65% indicated that the Data Protection/Compliance Officer is interested in data governance and data protection. 48% of the respondents indicated that the CIO/CISO would be interested, and 44% chose the legal department. When contrasted with the earlier set of questions about interests in data security, this subset of respondents may be more likely to be aware of the implications of enforcement actions taken to address not adhering to compliance requirements (such as penalties, fines or operational limitations).

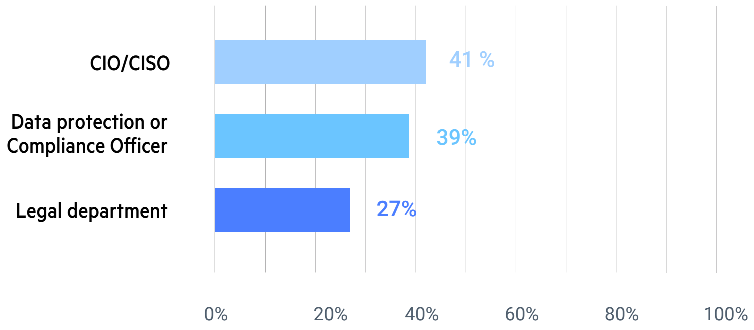
Figure.4
Interest in data governance



Responsibility for Data Governance Policies

The survey then asked the same reduced set of individuals, "Who is tasked with defining data protection policies?" The responses again demonstrated a different, and perhaps early-stage perspective of responsibility for data policy management in the enterprise. 41% selected the CIO/CISO, 39% indicated they have a data protection or a Compliance Officer and 27% said that the legal department plays a role in data protection policies. As in the previous response, individuals working at companies that have regulatory compliance requirements recognize the potential implications for noncompliance. As a result, these types of organizations may assign overall responsibility to senior staff for ensuring the proper controls are in place.

Figure.5
Responsibility for data policy management in the enterprisee



© 2022 Progress. All Rights Reserved.

Data Governance Policy Procedures

Again, the same subset of respondents working for organizations subject to regulatory compliance were asked to select from among a set of choices the procedures in place for data protection policy compliance. The top three selections are not surprising: access controls, password protection, along with employee training. On a positive note, there does seem to be some proactive steps being taken for establishing governance over data protection policies. Over half indicated their organization has risk assessment procedures, and nearly 50% of them report that regular security process reviews are in place. There is some degree of data governance maturity, as 43% report that their organizations have clear statements on data collection and handling procedures.

From a practical perspective, though, the respondents indicated a modulated set of practices for operationalized data protection, allowing for increased information risks. Only 29% reported that their organization implements real time data alerts to monitor for irregularities, and about a quarter of the respondents noted their organizations implement policies for deleting and removing data after a specified time period.

Data Protection Performance Metrics

Our survey asked the individuals whose companies are subject to compliance about whether the organization specified performance metrics for data policy compliance. One third of the respondents said yes, 31% said no, and 36% said that they were unsure. Ensuring that data policies are observed in an auditable manner is necessary for compliance reporting. These results suggest that since only 33% of the respondents were aware of performance metrics for data policy compliance, there may be some governance gaps that increase susceptibility to the types of information risks we have already discussed.

An additional question was posed to those respondents indicating that their organization has regulatory requirements and uses performance metrics about how those metrics are measured. It is valuable to see that 60% to 64% of the respondents chose most of the metrics listed as options in the question (including test results from employee training, frequency of obligatory password updates per year, frequency of security process review, number of approved and rejected items under the risk assessment procedures and number of data breaches per year).

2.4 Implications

Data security is often driven by regulatory compliance, frequently focusing on protecting individuals' personal and private information. Yet as organizations migrate their data to a hybrid multicloud environment, there is a broader "surface area" for exposure of sensitive data. Many IT roles are interested in data security, but ultimately, the actual responsibility must be assigned to a more senior-level role with visibility across the enterprise. This will help in ensuring clear accountability for a company's data protection policies.

Combining the results of the questions about interest and responsibility for data security, it is clear there is a need for increased awareness of data protection and data governance in general among the key organizational stakeholders, as well as a need to effectively communicate the value and criticality of enterprise-wide data governance.

Consolidating Data Protection into the Data Governance Strategy

When reflecting on the challenges of data security and protection, there may be additional variables to consider. For example, data encryption in a hybrid environment may create management and performance challenges, especially with increased data distribution and use of a data lakes or a data lakehouse. A data lakehouse is a data asset management framework, often deployed in the cloud, that uses standardized system designs intended to expand data awareness (using a data catalog), simplify data utility (using simplified methods for access via a semantic data layer), while ensuring improved data consistency (by providing access to data in its original form).

Challenges for role-based access controls are magnified as the communities of data consumers grow and become more diverse. Intrusion detection is challenging as intruders are always coming up with new methods of intrusion. The constant barrage of cyber-attacks attempting to break through perimeter guards creates similar challenges in managing endpoint security. This presents an opportunity for consolidating the strategies for data security and data protection and bundling the management of operational tactics as part of the enterprise information risk management and data governance framework.

Opportunities for Data Protection Policy Maturity

There are some nuances to interpreting the results of questions about responsibilities for defining data protection policies. The details of specifying data protection policies requires a combination of knowledge about the laws and regulations requiring compliance as well as the necessary data management skills needed to operationalize the compliance

© 2022 Progress. All Rights Reserved.

directives. A small organization's CIO, CISO, or legal compliance officer might have that combination of knowledge and skills. However, it is unlikely that scenario is either scalable or sustainable as the number of laws and regulations increases and as data asset volumes grow. Simultaneously, reviewing the most frequent responses to the questions about data security tools, we can infer that many organizations are still in the early stages of assessing their data protection strategies from the tools and the process perspectives. The implication is that significant opportunities remain for companies to establish a data protection strategy that aligns with compliance demands and good data governance practices.

Raising Awareness about Data Policy Governance

A quick summary: of the pool of respondents, two-thirds indicated their organization was subject to regulatory compliance, one-third of those (or 2/9 of the pool of respondents) reported their organization specified performance metrics, and about two-thirds of that subset (or about 15% overall) actively monitor defined performance metrics. While this bodes well for the subset of organizations with more sophisticated data policy governance practices, it also indicates an opportunity for continuing to raise awareness about the need for better practices in data policy management and data governance.

3. Theme #2: Modernizing through Cloud Migration

3.1 Challenges of Cloud Migration

A growing number of organizational technical architects and system designers are acknowledging how multiple aspects of migrating data and applications to a cloud computing platform motivate the business case for data environment modernization, including:

- **Lowered cost of operations:** By enabling the organization to pay only for the computing resources it needs, cloud service providers effectively enable the transfer of large-scale capital expenditures into more manageable ongoing expenses.

- **Flexibility:** Getting started migrating small data sets and their accompanying applications in the cloud is relatively easy.

© 2022 Progress. All Rights Reserved.

- **Accommodating the need for scalability:** Cloud services are eminently expandable in direct proportion to the organization's computing demands. Increased needs for either computational power or storage are easily accommodated in the cloud.

- **Value-added cloud-native services:** Many cloud service providers have developed a broad palette of value-added services layered on top of the core computing and storage resources, including cloud-based databases, data warehousing services, data ingestion, data integration and data pipelines, support for streaming data, as well as advanced visualization, AI and machine learning services.

- **Increased data diversity:** Cloud services support traditional structured data sets as well as more diverse data asset types such as semi-structured data, unstructured text, audio and video.

These all suggest that organizations develop a technology modernization strategy that embraces two separate tactics: "cloud first" development of new applications coupled with migration of selected on-premises applications to the cloud. That being said, an organization may face some migration and modernization challenges based on how data sets are used, and the types of business operations employed. Some aspects of application and data migration that involve potential complexity include:

- **Determining which applications to migrate,** requiring some assessment of the application landscape and determination of a prioritization scheme balancing migration "readiness," how streamlined the migration process is for each application, and the benefits that migration will yield.

- **Devising the right cloud architecture** for storage and computation for each of the migrated applications based on data requirements, use, and consumption.

- **Managing conformance to performance service level agreements** (SLAs), especially when there is some unpredictability in terms of data connectivity and data access latency.

- **Ensuring resilience for high availability and business continuity.** On-premise business continuity planning is relatively mature, but the characteristics of resilience may change as applications move to the cloud.

- **Ensuring proper data protection**, by considering what are the requirements for data security and what supporting tools need to be evaluated to ensure that data is properly protected at rest and in transit.

© 2022 Progress. All Rights Reserved.

In summary: data that is critical to the business operations must be managed properly which might include strategies like data replication, to ensure resilience and support business continuity in the event of a cloud vendor environment disruption. At the same time, migrated applications must be provided with low latency connectivity to ensure high performance.

3.2 What were we looking to Learn?

This year's survey looked to solicit information about organizations as they are starting to frame their cloud migration and data modernization strategy. We explore the reasons for organizations to be modernizing and moving to the cloud, what might hinder some from moving to the cloud, as well as examining the current state of data migration. The survey also asked about practical aspects of the hybrid data environment such as the circumstances under which organizations retain data in a single location vs. multiple locations, cloud data access, and how data sets in the cloud are used.

3.3 Results From the Survey

Where Data Sets are Stored

When asked about where organization data sets were stored, half of all respondents store their organizational data both on-premise and in the cloud. When only one of the two is used, storing data on-premise is the more frequent practice. However, that difference shrinks for newly produced data, as more respondents indicated that their organizations choose to store newly produced data in the cloud. One might infer from this that while it may appear that organizations are retaining some systems on-premise, with increasing frequency, new systems are being built in the cloud.

Percentage of Data in the Cloud

When asked about the volumes of data distributed across the hybrid environment, respondents indicated on average that 54% of organizational data stored and managed in the cloud. This suggests that as concerns about security and reliability of the cloud abate, organizations are increasingly embracing the use of cloud technology.

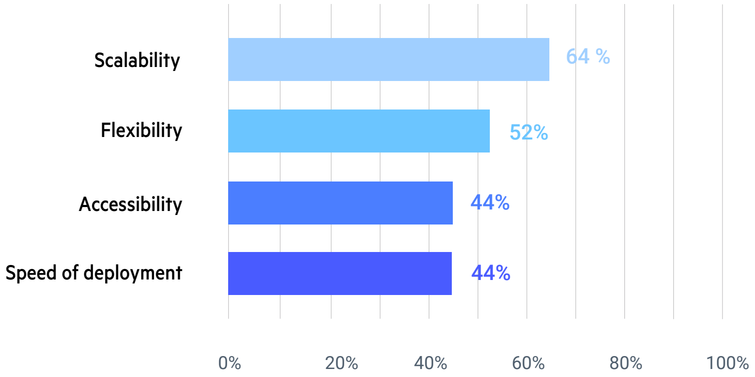
Data Stored and Managed in the Cloud = 54%

Reasons for Migration

Respondents were asked to indicate the reasons their organizations are moving or storing data in the cloud, and the four most frequently provided reasons were scalability (64%), flexibility (52%), accessibility (44%), and speed of deployment (also 44%). As we've already noted, modernization to the cloud is somewhat driven by the need for scalability (both in terms of computational power and storage) and data accessibility (as increased development of APIs provides both internal and external data consumers access to shared data). At the same, the flexibility of the cloud service provider platforms reduces the administrative burdens of setting up development environments. Cloud providers offer a variety of alternatives for a computing configuration requiring less effort and planning to launch, appealing to teams faced with short development and delivery timelines. Rapid self-service deployment solutions speed time to value while reducing IT friction.

Figure.6

Why organizations are moving or storing data in the cloud



Data Replication in the Cloud

As organizations plan their transition to the cloud, there is bound to be a time when the same data used by applications executing on-premise will be copied to the cloud. Of course, part of any data migration process involves replicating data from the on-premise environment to a copy in the cloud, but the question remains: how long an organization would tolerate replicating data in two environments. The survey asked whether "cloud data sets are replicating on-premise data sets," and 39% of the respondents who reported storing data in the cloud or both in the cloud and on-premise said that the cloud data sets replicate on-premise data sets. At the same time, 45% reported the data sets in the cloud do not replicate on-premise data sets.

This suggests an incremental shift in organizational trust of cloud data management. It also might be attributable to data owners being less concerned about maintaining replicas for business continuity purposes, improved availability for cloud data, or that the cloud

© 2022 Progress. All Rights Reserved.

ecosystems provide improved methods and utilities for easy access to cloud data. The responses to this question indicate that organizations are more frequently using the cloud as their primary data store.

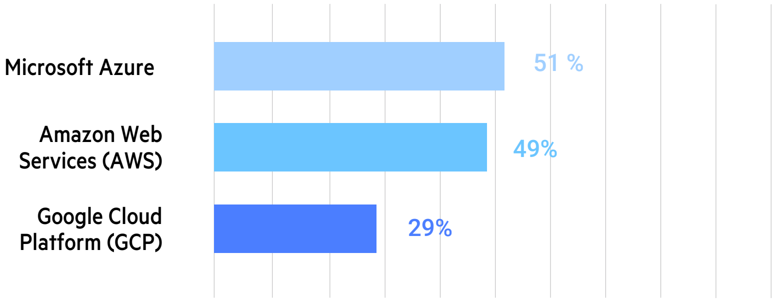
Those who responded that on-premise data sets were replicated in the cloud were further queried about the reasons for maintaining on-premise data. The most frequent answers included security (61%), performance (43%) and data regulations (40%). From a security perspective, it might be interesting to speculate whether data sets are replicated on the cloud as backups in case of a breach or a ransomware attack on an on-premise system or data sets are copied to an on-premise system to alleviate security concerns of the cloud.

Cloud Platform Choice

There are certainly no surprises when examining the responses to the question "Which cloud platform do you use?" The big three remain the top choices, with Microsoft Azure selected 51% of the time, Amazon Web Services (AWS) selected 49% of the time, and Google Cloud Platform (GCP) chosen 29% of the time, while other cloud service providers such as VMware, Oracle, Salesforce, SAP, and IBM, among others lag in terms of selection.

AWS and Azure, the two most widely selected cloud service providers, both offer a wide range of cloud services. Interestingly, prior iterations of this report found higher numbers of respondents choosing AWS over Azure, which might indicate a growing preference for the Microsoft offering.

Figure.7
Which cloud platform do you use?



© 2022 Progress. All Rights Reserved.

Adoption of Cloud Services

While respondents were asked about the cloud services that the organization used, the options for selection were effectively limited to data architecture alternatives. Considering our previous suggestion that cloud adoption is growing, it is not surprising that the most widely selected choices were cloud-native data management (36%) and databases "built for the cloud" (34%). And while there are still respondents indicating that their organization has "lifted and shifted" their on-premises application footprint in the cloud (15%), this perception is much lower than might have been expected. In other words, we see that cloud adoption goes together with use of cloud-native or "built for the cloud" platforms.

Other cloud-based services related to data management and data use included containers (23%), data lakes (22%) and object storage (22%). Viewed together, these are the services employed in implementing data lakes and data lakehouse architectures, and these percentages are indicative of organizations seeking to leverage data architecture paradigms promoting data sharing in the cloud. Increased adoption of governed approaches to cloud data sharing may take some time, as these approaches expect a combination of cloud data management services coupled with an open mind towards transitioning to newer technology architectures.

3.4 Implications

Correct to: Adoption of cloud services, particularly data management services, is growing, but some organizations may exhibit residual hesitancy for a few reasons, including:

- **Level of effort for transitioning,** including the time it takes to choose an appropriate set of data management services, the time to move data sets to the cloud platforms and the time to convert applications from one data technology to another.

- **The need for coordination**, especially as "net-new" applications are being built directly in the cloud yet still must interoperate with preexisting applications operating within their on-premise environments.

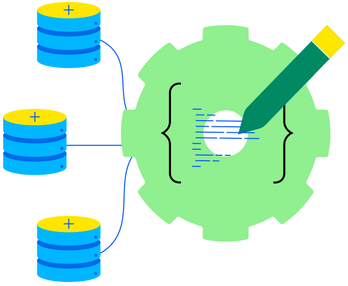
- **Fear of vendor lock-in**, as users don't want to solely depend on one cloud vendor's proprietary technology when there are numerous alternatives. System owners want to reserve the right to move from one cloud service provider to another whenever they want.

System designers and architects are increasingly recognizing how newer technologies can be used to the advantage of the data consumer communities. At the same time, fear of vendor lock-in is inspiring increased focus on the use of open standards for file storage and data organization (such as Apache Parquet and ORC formats, Apache Iceberg and

© 2022 Progress. All Rights Reserved.

Delta Lake), which support application portability, either across on-premise systems or across different cloud service providers.

We can expect in future surveys to see an increase in the use of cloud services empowering data consumers while reducing data latency and data exfiltration costs such as containers, APIs encompassing data services, data lake/lakehouse paradigms facilitating data sharing, and in-memory databases and data caching utilities.



4. Theme #3: Modernizing Data Connectivity and Data Services

4.1 Modern Connectivity Driven by APIs and Microservices

"API" is an acronym for "Application Programming Interface," and represents a method of connectivity between two different application programs. APIs have been around since the early days of computing, providing an abstract reference allowing one application to ask another application to provide a requested service. For example, a bank may establish an API allowing an ATM machine to look up a customer's checking account balance in the back-end database.

The concept of the API has evolved significantly since the early days. Today, a myriad number of web applications, smart phones and other handheld devices, kiosks and other customer-facing applications operate using APIs connecting the front-end device to one or more data services. At the same time, as different types of end-users have different data access privileges to the different data services, developers rely on configurable tools that simplify the generation and deployment of a catalog of different APIs and data services.

Today's API development tools employ low-code/no-code methods to more easily define, configure, and generate API code that can be deployed across a variety of platforms. When combined with methods of bundling code and encapsulating functionality in a portable manner allowing for deployment across different platforms (such as containers), APIs can be used to implement microservices addressing a wide variety of data consumption needs.

This year's survey asked respondents several questions intended to learn about how organizations build, deploy and use APIs and data services. The survey is seeking to infer how API development and usage can be better supported by API development tools. More fundamentally, understanding fundamental aspects of the ecosystem evolving around API development tools can inform the design and implementation of both internal-facing and external-facing APIs that are easily used yet remain secure, including:

- **Configurable data access privileges** and other limitations coupled with integrated adherence to data security policies.
- **Gateway management,** including a Gatekeeper monitoring API traffic, inspecting requests, and overseeing user authentication or token authentication.
- **An API catalog** that developers can search and review existing APIs so that they don't build ones that already exist and adapt APIs with similar requirements for reuse.
- **Tracking and monitoring** of API usage, logging unique request and usage characteristics of each API, monitoring request loads, generating logs, as well as providing early warning of unexpected behaviors.
- **Measurement of key metrics**, especially around availability and responsiveness.

4.2 What were we looking to learn?

As APIs and data services become a core component in an organization's data connectivity framework, we used this year's survey to ask respondents about the evolution of APIs within their environments, their experience in using and developing APIs. Their perspectives on the future of APIs to support data connectivity, especially when accessing data outside on-premise platforms.

4.3 Results from the Survey

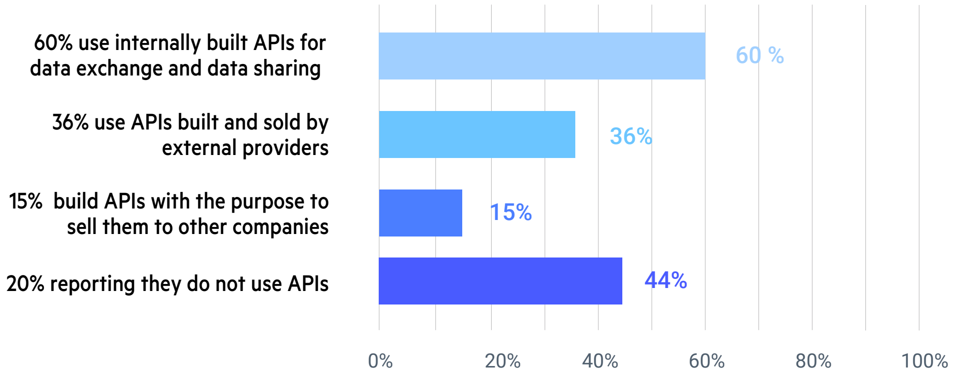
Use of APIs

Respondents were asked about their experience in building and using APIs for data exchange and data sharing, and the responses indicate a healthy commitment to developing and using APIs. 60% of the respondents' teams use internally built APIs for data exchange and data sharing. 36% of the respondents noted that they use APIs built and sold by external providers. There are some API developers among the respondent pool, with 15% reporting that they build APIs with the purpose to sell them to other companies.

© 2022 Progress. All Rights Reserved.

In the survey, only 20% reporting they do not use APIs. While this still may appear to be significant, this percentage might be accounted for by the subset of respondents that are in business, advisory or senior leadership positions.

Figure.8
Use of APIs



Experience Using APIs

The survey further explored the extent of API users' experience using APIs. The distribution of responses provides some reflection into the maturation of the API space from a developer perspective. 39% had between one and five years of experience using APIs and data services. Cumulatively, over 60% of the respondents have more than three years of experience, suggesting that among the respondent pool, the use of APIs is largely established as a core competency for application development. There are some respondents with much greater experience using APIs – 23% reported between 5 and 10 years of experience and 21% of the respondents reported they had more than 10 years of experience.

Use of APIs for Reporting and Analytics

There appears to be strong support for organizational adoption of APIs and data services to support data analysts and other analytical uses. When the survey solicited feedback about the use of APIs and data services for the purposes of reporting and analytics, cumulatively, over half of the respondents use APIs and data services for BI and analytics (to generate reports and/or for ad hoc queries). Specifically, 60% said "To generate reports," 51% said "For ad hoc queries," 46% said "To use BI/end-user analytical tools," and 34% "for data mining."

© 2022 Progress. All Rights Reserved.

However, individuals self-reporting other ways that APIs were used listed a surprisingly wide array of ways APIs were being used. Self-reported uses included (but are certainly not limited to) application access and UI interfaces to back-end systems, connecting mobile services, browser connectivity, data exchange, partner data transactions, cross-application data integration, connecting to third-party products, data movement, and other modes of data connectivity.

Combining these results with the responses about percentages of individuals building and using APIs, we can suggest that there is a healthy “internal developer market” for API development to support data sharing, business intelligence, and analytics. We can predict that this market will only grow as more applications and data assets are migrated to modernized systems in the cloud.

Using Other Data Producers’ APIs

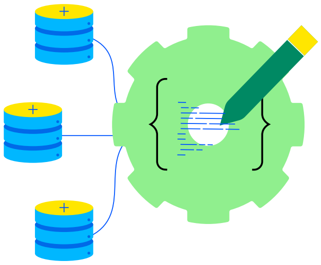
In addition to exploring how users employed APIs for reporting and analytics purposes, the survey solicited feedback about more general preferences for using other data producers’ APIs for data connectivity and data access. And even though the responses to the prior questions seemed to indicate that there is a healthy community of in-house API development being done, the responses to this question seem to indicate a preference for using other data producers’ APIs under certain circumstances. This is certainly the preference when accessing data from the data producers’ environments (47% indicated they prefer the other data producers’ APIs either always or most of the time, and an additional 19% about half the time).

These preferences erode somewhat when accessing SaaS data, accessing cloud platforms that are within the enterprise’s administrative domain, and accessing other organizations’ cloud data. In the latter case, only 33% indicated they prefer the other data producers’ APIs either always or most of the time, while 50% only sometimes or never indicated they prefer the other data producers’ APIs.

© 2022 Progress. All Rights Reserved.

4.4 Implications

One aspect of API use that is not explicitly apparent yet emerges from the responses is the effective decoupling of data access methods from the underlying system platforms. What we learned from the questions about cloud migration and modernization is the recognition that both the enterprise data landscape and the communities of data consumers are increasingly distributed (across a hybrid multicloud configuration) and diverse. Different data consumers with different skill levels all want direct access to data sets in their original formats. However, the organization will not be able to enable untrained individuals to access data from one or more different source systems with which they have little or no experience. APIs bridge that skills gap by providing a simple (and typically standardized) means for democratized data access while embedding data access controls and preventing unauthorized data use.



5. Theme #4: Tools Strategy

5.1 Why do We Need a Tools Strategy?

The results of this survey highlight three characteristics of the modernized computing environment that are influencing architectural decisions about the adoption and use of technology:

- The need to provide a sustainable and scalable way to define, manage, and monitor compliance with data security and protection directives.
- Simplifying application development in the face of an increasing complex hybrid multicloud enterprise computing and data storage environment.
- Empowering data accessibility to citizen data consumers with a range of experience and skills.

Data protection directives will only become more convoluted, requiring better methods to keep track of obligations by location, jurisdiction, and type of transaction. Virtual data lakes and data lakehouses distributed across domains and cloud providers must be made accessible via APIs. All of these concerns can be addressed by considering a tools strategy that embraces technologies for automation of data governance and protection along with data access using APIs and data services.

© 2022 Progress. All Rights Reserved.

5.2 What were we looking to Learn?

Bottom line: we are looking to understand the factors motivating the need for innovation in technology development to meet the emerging needs of the extended information enterprise.

5.3 Results from the Survey

Data Security and Protection Tools

The survey asked respondents about the data security tools they use and three choices truly stand out. The first is that 32% of all respondents reported their organization uses internally built security tools. The second is that 30% of the respondents were unsure about what security tools were being used. We suspect that this likely means that that the respondents are just not aware of vendor products there are in place. The third is that 10% (still a significant percentage!) answered that their organization uses no data security tool. With the huge increase in system exploitation even at the individual desktop/laptop level, it is hard to believe that companies would operate without any security tools.

The most widely selected third-party security tool is FortiGate Next-Generation Firewall, and a cumulative 23% indicated they use tools such as CloudGuard, HashiCorp SaaS, Google Apigee Sense, Egnyte, and Incydr. There were many other tools listed by those responding “other,” with a number of those being specifically data protection tools. However, the criticality of data protection to manage and remediate information risk is too important to rely on home-brewed techniques and tools. We suggest that organizations adopt a more proactive approach to managing data security and protection.

Tools to Help in Defining and Managing Data Protection Policies

The most widely selected third-party security tool is FortiGate Next-Generation Firewall, and a cumulative 23% indicated they use tools such as CloudGuard, HashiCorp SaaS, Google Apigee Sense, Egnyte and Incydr. There were many other tools listed by those responding “other,” with a number of those being specifically data protection tools. However, the criticality of data protection to manage and remediate information risk is too important to rely on home-brewed techniques and tools. We suggest that organizations adopt a more proactive approach to managing data security and protection.

One third of the respondents indicated that they use a data catalog, which may be better suited to managing the policies associated with data asset classification, data access control and linkage to externally defined regulations and directives. Data catalog tools can often help enumerate the data elements that need special consideration, such as limited access controls or field level encryption, data masking, or other special handling according to a defined sensitivity classification. Data quality tools can be augmented to incorporate rules to alert a data steward when a compliance directive has been violated, but only 23% of the respondents indicated the use of data quality tools for that purpose.

Interestingly, when prompted for the names of other tools used by the respondents choosing the "other" option, there were no vendor product names provided. This suggests there is still an opportunity for data policy management tool vendors to raise awareness about how their products support data governance in general and data policy management.

Adoption of API Tools

Collectively, these questions and their responses highlight the criticality of embracing API development as a key component of a data connectivity strategy. Developer enablement is key to this strategy, requiring the adoption and use of tools that simplify specification, development and deployment of APIs in ways that are consistent with current agile development, DevOps and continuous integration and continuous delivery (CI/CD) methodologies. At the same time, organizations must have processes for documenting and cataloging their APIs to minimize redundant effort and increase API reuse.

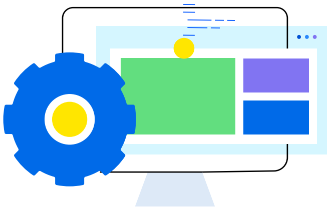
One of the benefits of using an API development tool is that it provides a platform for testing and validating their API code, as well as guidelines for ensuring the security of the developed APIs. The survey asked respondents to select the tools they use for developing and managing APIs, and the most popular selections reflected choices in maturing tools for development and use of cloud services for management and deployment. The largest share of respondents (39%) use Postman to develop and manage APIs, with healthy showings by other tools: MuleSoft, Swagger, Apigee and Boomi, among others. From the cloud perspective, respondents selected Azure API Management, AWS API Gateway, Oracle API Platform and IBM API Management for creating, publishing and managing APIs connecting applicationware and data across the hybrid environment.

© 2022 Progress. All Rights Reserved.

5.4 Implications

The proper tools strategy can help to democratize data access while simultaneously ensuring that data protection policies are in place and are being enforced. A combination of methods can be used to directly integrate authentication, masking and encryption of sensitive data element values.

Instituting data access controls through APIs allows only those individuals or group members having the proper access privileges to access data, thereby plugging security holes and reducing the potential for exploits due to targeted attacks. The result is protection of corporate reputation and appropriate avoidance of legal ramifications stemming from improper data leaks and unauthorized exposure. Tool providers could consider how to evolve their products to meet emerging compliance requirements, improve data democratization, all while reducing vulnerabilities impacting information risk.



6. Summary

As opposed to prior years' surveys that mostly focused on the adoption and use of data connectivity technologies, our intent in this year's survey was to provide a different view on data connectivity from a more subtle perspective. By probing respondents' opinions and thoughts about the contexts in which they develop applications that connect to an increasingly complex data landscape, we were able to get a more thorough understanding of key drivers motivating enterprise data modernization.

The results indicate the need for a more sophisticated integration of data governance within a framework for data connectivity. This includes improving operational integration of both the implementation and monitoring of compliance to data protection policies and automating the specification and development of APIs. Together, these capabilities can empower more data consumers in accessing the data they need, simplifying application development and speed time to value.

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

2022 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved. Rev 2022/06 RITM0165842

f /progresssw
/progresssw
/progresssw
in /progress-software
/progress_sw_

Progress®