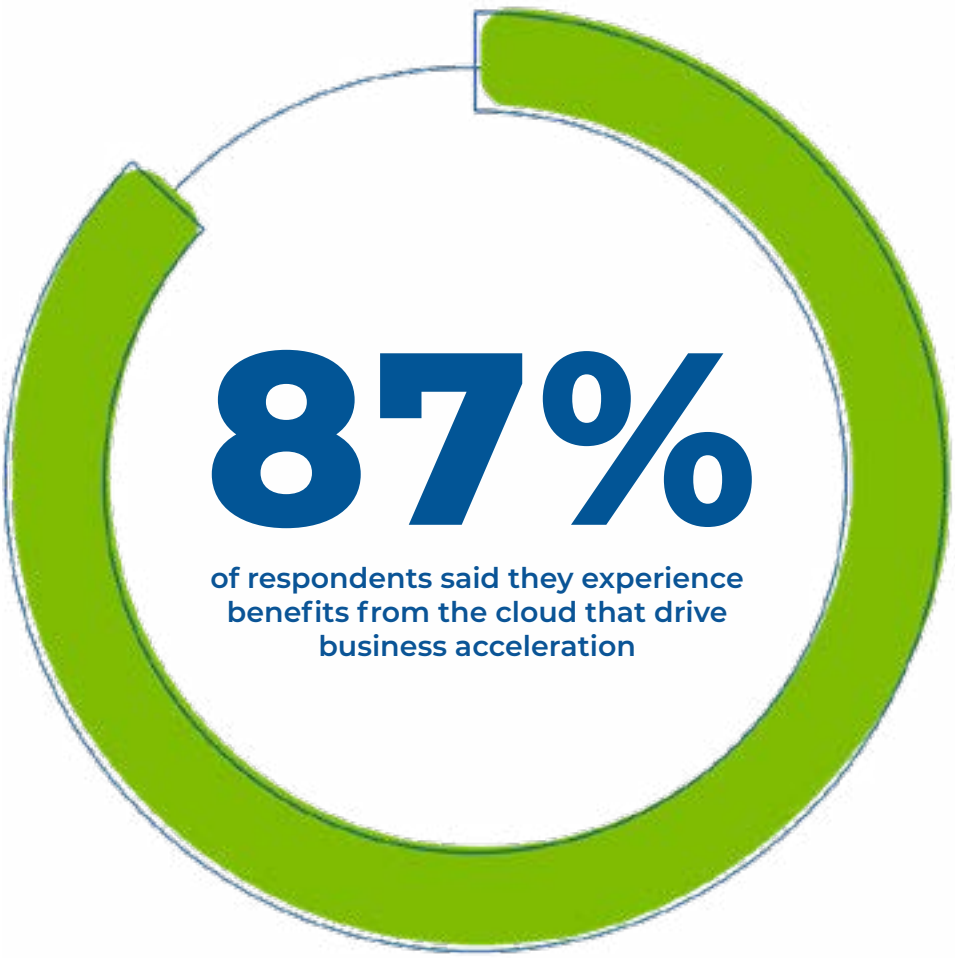
Cloud Computing
BEST PRACTICES

American
Technology Services
a WWTS Company



Use of the cloud drives multiple business benefits, including decreased time to market, increased security, and business growth. And these benefits have become widely recognized. 87% of respondents to McAfee's 2019 Cloud Adoption and Risk Report said they experience benefits from the cloud that drive business acceleration.

But it's important to understand the technology and its unique attributes prior to migrating any infrastructure to the cloud. In this eBook, ATS provides key background info and tips to maximize the benefits for your organization.

Cloud Defined

The term “cloud” is most accurately applied to those solutions that exhibit five essential characteristics of cloud computing, as defined by the National Institute of Standards and Technology (NIST):

- On-demand service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

NIST defines several cloud service models as progressive increases in management by vendors.

Infrastructure as a Service (IaaS)

The vendor provides the infrastructure and hardware including processing, storage, networks, and other fundamental computing resources where the client is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service (PaaS)

The vendor provides a managed environment for clients to deploy client-created or acquired applications created using programming languages, libraries, services, and tools supported by the vendor.

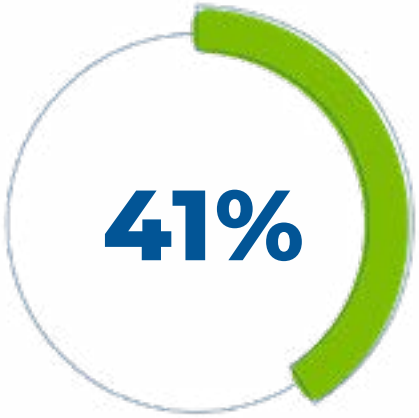
Software as a Service (SaaS)

The vendor provides a fully managed application running on a cloud infrastructure and the client need only supply their data.

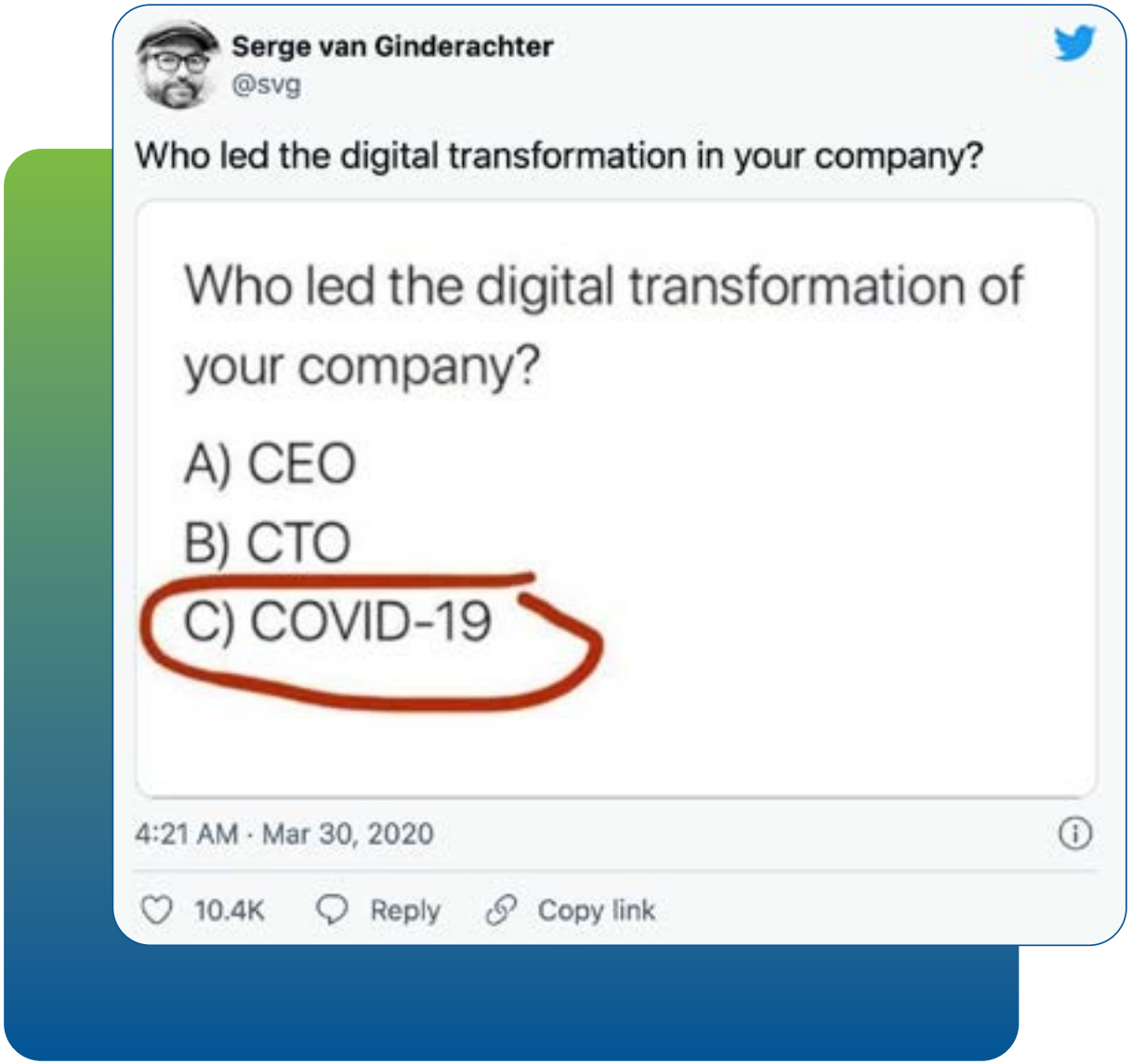
Cloud Adoption is Prevalent and Growing

Cloud adoption continues to grow along with the awareness of the many benefits. According to 451 Research's Voice of the Enterprise survey data, published June 2020, virtually all respondents (97%) are either underway with, or expecting, digital transformation progress in the next 24 months. Over 41% are allocating more than 50% of their IT budgets to projects that grow and transform the business.

97% are either underway with, or expecting, digital transformation progress in the next 24 months.



Over 41% are allocating more than 50% of their IT budgets to projects that grow and transform the business.



Those organizations that weren't already in the cloud promptly found themselves with no choice, as humorously pointed out in this tweet on March 30, 2020.

Use of Cloud Computing in the US Federal Government

In 2010, The Office of Management and Budget (OMB) released the "Cloud First" Policy calling on all agencies to default to cloud-based solutions when secure, cost-effective options are available.

The next iteration of the Federal Cloud Computing Strategy was updated in 2019. "Cloud Smart is a long-term, high-level strategy to drive cloud adoption in Federal agencies. This is the first cloud policy update in seven years, offering a path forward for agencies to migrate to a safe and secure cloud infrastructure."

The policies offer helpful guidance for organizations outside government as well. "The Cloud Smart Strategy encourages agencies to **think of cloud as an array of solutions that offer many capabilities and management options** to enhance mission and service delivery."

Smooth Scaling: Grow IT Capacity at the Rate of Organizational Growth

Legacy hardware perpetually requires updating every few years. Migrating to the cloud enables you to **get off that tedious treadmill and turn IT infrastructure into an annualized cost instead.** Infrastructure that moves to the cloud results in a budgeting change from capital asset expenditures and maintenance to consumption-based pricing.

Additionally, buying hardware internally results in uneven capacity growth. You may buy a server because you need one more of something, such as an email user, but that server provides 100 more. While you may eventually use that capacity, such spikey growth can be problematic, whereas cloud enables smooth growth with corresponding gradual increases in cost.

Failing to Plan is Planning to Fail

In beginning your cloud migration, you must have a clear direction. Don't just chase what's "shiny." Starting with a trendy solution and then trying to determine which problem you'll solve with it isn't the best approach.

Cloud isn't the point. Cloud is the tool you use to get the thing you want.

Additionally, be sure to balance different objectives. While the cloud can result in cost-savings, it's important to focus on a variety of key performance indicators. IT modernization builds capabilities that enable organizational efficiency and growth.

Foster a Supportive Culture

Cloud adoption impacts many areas of the organization both outside and within IT and, as such, your organization's culture must be conducive to this move. The following can help foster a supportive culture:

- Be willing to try new things, adapt, and change
- Give your teams permission to experiment and potentially fail
- Involve the appropriate stakeholders to earn their support, including rank and file staff
- Be agile and consider making changes in smaller chunks with iterative improvements, minimizing the impact of any mistakes

Carry Out POCs and Pilots

Pilots are an essential component of any IT project, and cloud migration is no different. Carry out a proof of concept (POC) to demonstrate that your migration goals are feasible. A POC allows any unexpected issues or errors to be uncovered, investigated, and resolved before you take a bigger leap. POCs also have the benefit of earning buy-in and creating confidence. POCs should involve end-to-end testing including end user communications, end point reconfiguration, mobile device reconfiguration, and collection of feedback.

Cloud Adoption Framework

Microsoft provides comprehensive Cloud Adoption Framework (CAF) documentation consisting of guidance, best practices, and tools. The expansive resources can help you balance speed, innovation, and control by using an agile approach to get started and improve over time.

New Skills and Processes Needed

As part of your cloud migration strategy, you must identify any gaps in skills between your current IT environment and the future cloud environment. The Azure CAF states, "The most important aspect of any cloud adoption plan is the alignment of people who will make the plan a reality. No plan is complete until you understand its people-related aspects."

"Cloud adoption can't happen without well-organized people. Successful cloud adoption is the result of properly skilled people doing the appropriate types of work, in alignment with clearly defined business goals, and in a well-managed environment. To deliver an effective operating model for the cloud, it's important to establish appropriately staffed organizational structures."

Cloud Migration Strategies

There are multiple ways of undergoing a cloud migration. “Lift and shift” refers to picking up your infrastructure and moving it to the cloud as-is. Lift and shift generally involves using IaaS (infrastructure as a service) from the cloud provider. While the advantage is that you don’t have to first exert the effort to adapt prior to migration, the disadvantage is that you don’t adapt… Any application issues you may have struggled with will still remain after moving to the cloud. Lift and shift can also result in lost opportunities for cost savings, which can be significant. Respondents to Flexera’s 2020 State of the Cloud Report estimate that organizations waste 30 percent of cloud spend.

It’s often beneficial to adapt applications so they work more effectively in the cloud environment, and such tweaks can be done after the move. This is sometimes referred to as, “lift and refit.”

You can also choose a hybrid model, in which you move some workloads to the cloud while retaining some on-premises. This may include having live data transfer between cloud and on-prem data centers, as they function as one system across both environments rather than two separate silos.

Finally, “cloud native” are those technologies developed and built specifically for the cloud. The Cloud Native Computing Foundation defines cloud native as technologies that, “empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach….”

Analyze Your Current Environment

The first step to establishing your cloud migration strategy is to analyze your current environment, including:

- Network traffic capabilities
- Internet speed
- Versions of software – server and user-based
- User count
- Data size
- User roles and their needs

You must determine who and what will be affected by migration. Break it down by department, user type, location, and primary work location. Consider what will change and how it will change, for users as well as admins, including how remote users interact with these workloads.

Application Rationalization

Before moving to the cloud, you must decide what to move, which starts with conducting an application rationalization. Dig in and figure out what you have in the data centers, and how extensively those workloads are being utilized. Figure out what makes sense to move and what makes sense to stay. For example, some older systems can't be virtualized.

The goal of rationalization is to lighten burdens by discarding obsolete or redundant apps. To make these determinations, the Federal CIO Council released an Application Rationalization Playbook. The 37-page book outlines the following steps:

01 Identity needs and set governance

02 Inventory applications

03 Assess business value and technical fit

04 Assess total cost of ownership

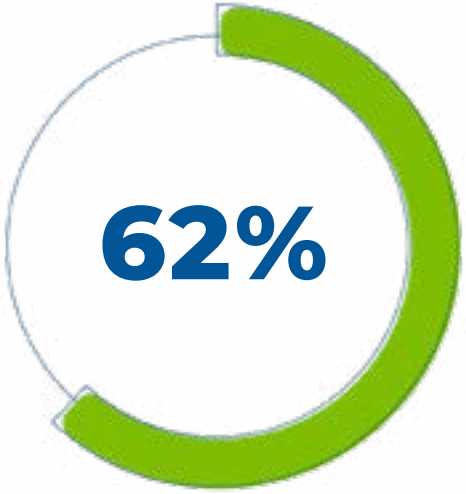
05 Score applications

06 Determine application placement

While cloud confers many benefits, there may still be some workloads that should stay on-premise. Cloud need not be an “all-or-nothing” proposition. The best path might be to use the capabilities of the cloud to build on top of your existing infrastructure and hardware to gain more capacity and availability, resulting in a hybrid solution.

Leveraging multiple cloud providers and resources is also the best path for many organizations. According to Flexera’s annual state of the cloud report for 2020, of those organizations using cloud services, 93% have a multi-cloud strategy that combines multiple public and private clouds. 62% of organizations using public cloud are using more than one public cloud.

93% of organizations have a multi-cloud-strategy that combines multiple public and private clouds.



62% of organizations using public cloud are using more than one public cloud.

Migration Paths and Speeds

In determining your migration path, consider both the size of your infrastructure as well as your level of urgency. You can do a cutover migration in which you move all users at once. As expected, this isn't feasible for larger organizations. For example, Microsoft states, "A maximum of 2,000 mailboxes can be migrated to Microsoft 365 or Office 365 by using a cutover Exchange migration. However, it is recommended that you only migrate 150 mailboxes."

Migrations can, of course, also be done in a waved pattern. With either path, pre-stage and pre-move as much data as possible. While weekend maintenance windows are preferable for organizations that don't operate 24/7, you might not be able to move all the data in a single weekend.

Microsoft offers free migration tools, and other third-party tools are available. Test and ensure they meet your needs, ensure proper throughput, and minimal disruption to users. Choose tools that enable you to pre-move as much data as possible.

Do Your Homework

Thoroughly evaluate cloud vendors before selecting a provider. Check how long they have been in business, as well as Service Level Agreements, security measures, compliance, financial information, etc. Keep in mind a vendor offering discounted pricing may be doing so because they are lacking in some area that is important to your organization.

Migrating Business Productivity Suite

The most common services and workloads to move are email (such as Microsoft Exchange), SharePoint and network shared drives into OneDrive for business. With email, ensure you migrate all mailbox data, including contacts, tasks, archive systems, PST files, and calendar items.

Also look at any minimum requirements that may exist for the cloud services you plan to move to.

Identity & Access (IDaaS)

Identity and access services and products can be consumed “as a service,” and it has become the predominant choice. The role of IDaaS is to facilitate access and authentication to all IT infrastructure, including SaaS apps and on-prem apps, and to minimize friction for the end user while doing so.

Look at federated domain services to allow synchronization of user permissions and policies between on-premise and cloud services and applications.

Network Topology and Bandwidth Needs

Some organizations focus only on the bandwidth needs to migrate data to the cloud service and fail to consider the necessary network topology changes for continuing use. For example, if you have on-prem Microsoft Exchange and file servers, users are connecting to your data center for this access, whereas that connection will shift to the cloud service.

End points need to be able to get out to the internet quickly and effectively. You might need to make bandwidth changes or change agreements with your network providers to ensure there’s adequate bandwidth.

It is important to have a redundant connection to the cloud with different carriers. This will give you another way to access your applications if one carrier experiences an outage.

SaaS Raises New Hurdles to Security and License Management

SaaS has enabled the modern best-of-breed world. For every industry, department, function, and person in an organization, there's some SaaS app that has been built to help them do their jobs better. However, SaaS apps also raise new challenges for security as well as license management.

Gartner analysts write, "The perceived ease of procuring and deploying SaaS belies the underlying complexity of ensuring governance and security without compromising user experience (UX) and user productivity... The SaaS delivery model changes the way users access applications, fundamentally redefining the access boundary."

With SaaS, you pay whether you use the licenses or not. Another onus that falls on IT is to monitor use and ensure coordination between licenses paid for and those needed. It's easy for users in your organization to acquire new SaaS apps and additional licenses. This ease makes it difficult for IT to understand where funds are allocated, if licenses are being used, and where you may have redundancies in apps. This lack of visibility into unused licenses often leads to waste, whereas, a dedicated focus to SaaSOps with tools such as BetterCloud has resulted in savings for some organizations of over $100,000 in less than a year.

Additionally, AWS describes changes to your accounting processes that can be beneficial. "Cloud services provide options to create very granular charge-back models. You will be able to track consumption with new details, which creates new opportunities to associate costs with results." Microsoft Office 365 provides cost-savings potential by enabling you to mix and match licensing, so you're not bound to one type of license for all your users.

Unfortunately, inconsistent user roles and their corresponding rights are inconsistent across SaaS apps. Many organizations simply take the path of least resistance and simply grant access to more data and controls than necessary. In some cases, this can equate to giving nearly everyone super admin rights, leading to increased risk.

You Can't Manage New Tech with Old Tactics and Tools

Gartner also elaborated on the need for Infrastructure and Operations (I&O) leaders to transform the roles and skills of IT teams as they shift to SaaS. "The competing pressures of IT operations and user enablement will demand new skills, tools and roles to lead the transition to SaaS."

Unfortunately, most organizations are failing to make these crucial shifts. "By 2024, 70% of IT organizations will lack the relevant roles, skills and tools to support SaaS-enabled digital transformation." Some of the tools needed include SaaS management platforms which can drive reduced friction, better collaboration, and a better employee experience.

Cloud Security – The Shared Responsibility Model

It is critical to understand compliance requirements and responsibilities around data before engaging any third-party provider. Ultimately, you are responsible for all the potential harm of a breach.

In the "Shared Responsibility Model," the cloud service provider is responsible for protecting the infrastructure that runs all of the services offered in the cloud. While the client retains responsibility for their use of the cloud including data, endpoints, and access management. For a deeper dive into cloud security, read our eBook, "Best Practices in Cloud Security."

It's important to understand the full scope of your responsibility. For example, while it's quick and easy to get up and running with default settings, and you need to go through and do the work to determine which defaults are OK for your organization and which aren't. You have to understand the impact of your selections, since you could be opening ports to the world or putting boxes on the internet without meaning to.

Additionally, while cloud providers such as Microsoft have hardened the walls, there are still threats with social engineering, for example.

Cloud Security Complexities

Securing everything across multiple clouds involves securing access, managing identities, and constant auditing, to name just a few. Additionally, security professionals must keep pace with the ever-increasing velocity of agile software deployment.

Finally, increasing sprawl of workloads across multiple public and private clouds results in difficulty obtaining visibility and a lack of end to end context around risk. These challenges are only exacerbated by the security gaps inevitable with disparate solutions.

“Cloud providers are releasing new features at an astonishing pace. It’s challenging for security practitioners to keep up, which in turn can lead to misconfigurations. “‘In a complex multi-cloud environment, you need an expert for every single platform or service you’re using to ensure that the appropriate security measures are in place,’ says John Yeoh, global vice president of research for the Cloud Security Alliance.”

Leverage Expert Assistance for Digital Transformation

Migrating to the cloud is obviously a massive change and disruptive transformation to operations. As such, it’s important to have the guidance of experts who can help manage the change and drive maximum value.