Microsoft IT cloud computing strategies continue to evolve

Microsoft is on a multi-year journey to adopt cloud computing throughout the company. This complex and strategic undertaking involves multiple teams, public cloud computing, and private cloud computing. Understand the strategy, operations considerations, and cultural shifts that are making this journey successful.

Today’s reality is a hybrid cloud

Since 2011, we have actively pursued cloud adoption to benefit from platform efficiencies, development agility, and rapid deployment capabilities. Our vision has always been “everything runs in the cloud.”

At the outset, our goal was to host 80 percent of our services and applications through public cloud services. Since 2011, the strategy has evolved and been refined to pursue a goal of more than 90 percent of IT services and applications in the public cloud. The reality today is a hybrid cloud, using both public and private cloud computing environments.

What does success look like?

We realized that there are multiple outcomes.

- A simplified application portfolio.
- Enabling IT resources to focus on high-value activities.
- Greater focus on delivering customer capability.
- Ability to respond more quickly to business changes.

Overall, cloud adoption is driving profound cultural and technological shifts that reverberate through all aspects of the business.

Simplified portfolio

Part of our cloud adoption strategy is moving approximately 2,100 line-of-business (LOB) applications to the cloud platform. These applications are spread across eight datacenters worldwide, and comprise over 40,000 distinct operating system instances. Through the cloud adoption efforts, a deep understanding of the portfolio is driving engineering to identify and optimize applications that are aligned to business functions and to reduce waste.

Shift the culture

We realized that our biggest challenge was not a technology issue. The biggest challenge was powering a cultural and process change at Microsoft. To understand our culture and how we decided to migrate a specific application, it helps to understand that our organization has two major groups—and that the culture is changing in both of them.

- Business process units (BPUs) are aligned with specific business processes such as finance, sales, support, and human resources. BPUs are responsible for building and maintaining the portfolio of internal LOB applications in their specific area.
- Centralized IT services are responsible for a variety of services across the enterprise, with a focus on running applications and providing architectural guidance to BPUs. IT functions include server infrastructure management, SAP implementations, and security.

Unique to Microsoft: First and best

The first and best culture is unique to Microsoft. First and best holds that any application or service that Microsoft releases externally must first be deployed and thoroughly tested within our own large-scale enterprise environment. First and best also strives to innovate by showcasing new cutting-edge technologies and inspiring customers. Beyond implementation, we share our learnings with customers using a variety of engagement models and materials.

Evolution of the hybrid cloud

While the overriding vision is to run everything in the cloud, we understand that Microsoft Azure is an excellent infrastructure platform for many workloads—but some apps are not yet optimal for the cloud. Old application complexity and regulatory requirements made it challenging to immediately move a small fraction of internal applications. Despite this, the vast majority of LOB applications are targeted for migration as soon as possible.

The decision to retain a small number of applications in traditional datacenters for the near future meant that we would run some components in Azure, and some within traditional datacenters. This resulted in a hybrid cloud configuration.

As the Azure platform evolves, it is becoming more and more apparent that the number of internal applications we are planning to keep on-premises is becoming smaller.

Hybrid strategy

A hybrid cloud is a blend of on-premises (private) cloud and off-premises (public) cloud. Orchestration between the two allows mobility of workloads between locations, depending on needs, costs, and flexibility.

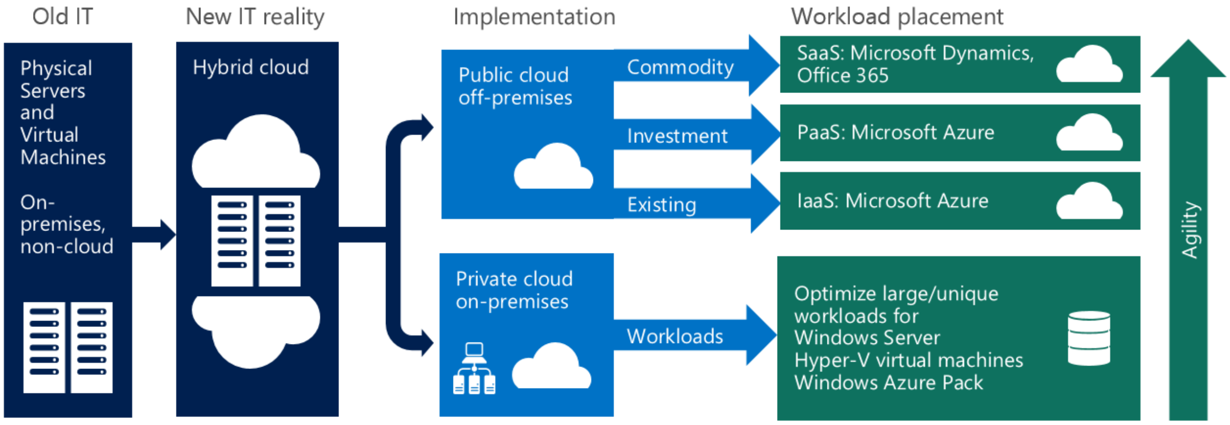
Old IT
New IT reality
Implementation
Workload placement
Physical Servers and Virtual Machines
On-premises, non-cloud
Hybrid cloud
Public cloud off-premises
Commodity
Investment
Existing
Private cloud on-premises
Workloads
SaaS: Microsoft Dynamics, Office 365
PaaS: Microsoft Azure
IaaS: Microsoft Azure
Optimize large/unique workloads for Windows Server Hyper-V virtual machines Windows Azure Pack
Agility

Figure 1. Hybrid cloud strategy at Microsoft

We always choose the public cloud first, because it offers the most agility and scalability. We chose to use commoditized services, such as Microsoft Dynamics CRM Online, SharePoint, and email, through Software as a Service (SaaS). Existing applications with planned investments use Azure Platform as a Service (PaaS), reducing lead-time between strategy and service. If no further investment will be made to an existing (sustaining) app, but it still fulfills a service, it will move to Azure Infrastructure as a Service (IaaS). In addition, all preproduction environments will be moved to Azure.

For the small number of existing applications that have specific regulatory compliance requirements, and that are not available in a public cloud solution, we use our on-premises private cloud.

Moving to the cloud

Cloud adoption has been an evolutionary journey. In the early phases, when we began selecting applications to move to the cloud, we made simple classifications to determine when an application should be targeted for migration. We weighed two factors: technical complexity and business impact.

We began with the least technically complex applications that had the least impact on business. This approach let the team build new architecture models and increase the skills of engineering teams to fully take advantage of the new capabilities without great risk.

Programmatically driving cloud adoption

The Stratus team is a centralized group in Microsoft IT that focuses on driving cloud adoption at Microsoft. The Stratus team provides several critical functions, such as:

- **Analysis.** The team analyzes cloud capabilities, applications, and platform requirements, and determines how those factors enable the adoption of cloud technologies. This is a key function, as Stratus needs to know when application-critical capabilities are available in the cloud.
- **Cloud readiness assessment.** The Stratus team developed a decision framework on where—or if—an application would live in the cloud.
- **Guidance and training.** The team consults with BPUs to provide guidance and training for enabling a cloud-first IT organization.
- **Reporting.** This function is critical to sharing accountability across BPUs.

Application rationalization

The following graphic shows the outcome of the portfolio evaluation process. It shows the output and results of portfolio evaluation, and how the vast portfolio is divided up and slated for adoption. It also shows that half of the portfolio consists of custom LOB apps.

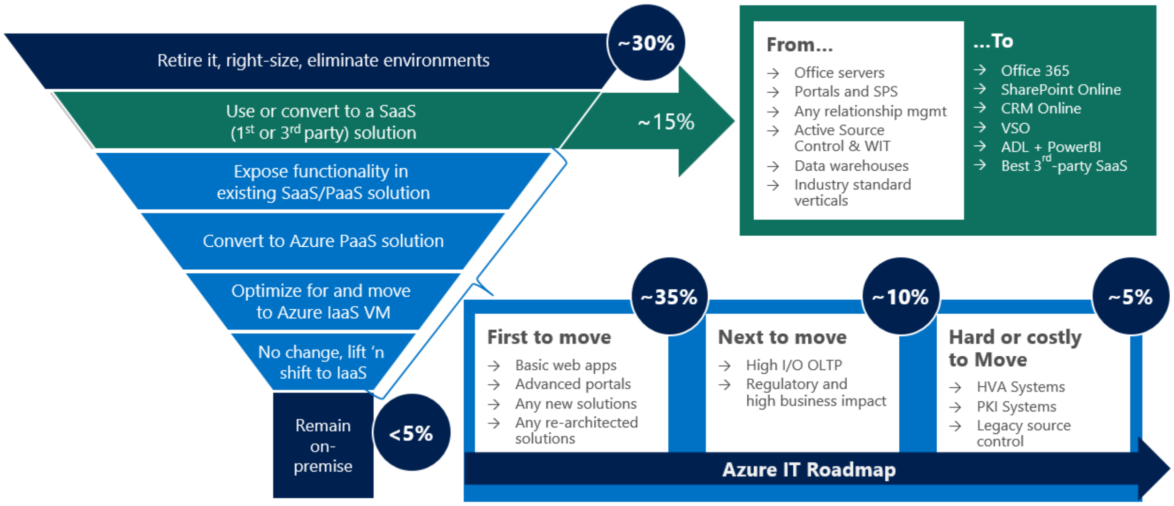

Figure 2. Cloud adoption roadmap planning

- Nearly 30 percent of the app portfolio could be retired, right-sized, or eliminated. We were able to consolidate functionality into a single app or service line. Thousands of physical servers and virtual machines (VMs) have been eliminated.
- About 15 percent of the app portfolio was replaced by SaaS solutions, such as Office 365, SharePoint Online, and some third-party solutions, as they became available. This allowed us to transition functionality from customized applications to retail solutions.

- Complex and customized LOB applications make up 50 percent of the app portfolio. Within that, most have been identified as “first to move.” These are basic web apps or re-architected solutions. The remainder are identified as candidates that are “next to move” aggressively to IaaS. A small portion is identified as “hard or costly to move.”
- Less than 5 percent of apps will remain on-premises.

Governance changes encourage these trends. Starting in June 2015, a variety of approval levels was implemented. Physical servers require a General Manager approval as well as approval from our senior leadership team, and approval from the CFO, CIO, and Azure product development group. On-premises virtual machines require Capital Committee approval.

The governance and approval functions reinforce that we are now cloud-only, unless teams take their specific scenarios to leadership with supporting data.

For more information about cloud adoption at Microsoft, see Driving cloud adoption in an enterprise IT organization.

Operationalizing the cloud

We balance a managed, yet highly self-service, customer approach to cloud operations. The focus is on the cloud subscription team providing tools and capabilities to ensure agility and the engineering automation that enables investment. At the same time, we provide appropriate levels of control and maintain governance.

We centrally provision cloud subscriptions and apply policies that ensure compliance. Internal portals allow IT teammates to request Azure resources or apps through those tools. Cloud resources are co-managed, and follow a Least Privileged Access model. Audit functions such as user access reviews, endpoint verification, and operation log reviews help us monitor people, VMs, security events, and changes to configurations.

Technical and business process management

Technical management practices and governance are followed in such a way that we both set up Azure subscriptions for application owners, and enable new features and apply configuration changes. Business management processes ensure that application owners have a complete understanding of their Azure environment.

There are two key technical management practices:

- **Setting up and configuring subscriptions.** For both automated and manual migrations, Azure subscriptions must be set up for application owners. We have established a specific set of standards and processes for configuring Azure subscriptions to ensure that they operate within a standardized environment.
- **Enabling features.** While the initial configuration and creation of Azure VMs can be automated, the process for enabling and configuring new features cannot be automated. We have created a request process that results in the Service Deployment and Operations (SDO) team making any necessary configuration changes for the application owner.

Governance and business management processes ensure that application owners have a complete understanding of their Azure environment. Two of the processes that ensure that Azure availability and functionality are clearly communicated to business units at Microsoft are:

- **Central Azure registration and commitment management.** These processes give us the ability to understand the scope of a business unit’s involvement with Azure and to manage Azure migration requests.
- **Standards for cloud services and subscription placement.** We have specific standards and processes set for Azure migration. This ensures that both SDO and business units are properly informed on how the migration process works, and what general factors make an application or workload suitable for migration.

Securing the infrastructure

We have combined user education and awareness, outsourced services, segmentation, application security, and other strategies to make its transition to the cloud safe and secure. The pre-cloud focus was on protecting the network perimeter and device security. The network perimeter could be closely controlled, and users had to log in to the corporate network to access any resources. Once apps and services started moving to the cloud, the perimeter became more ambiguous. Security became a logical, rather than physical, challenge.

Users now have access to a wide variety of cloud-based file sharing services. Users need to be educated about compliance requirements, such as where data is stored, and how data is classified. Beyond user awareness, outsourced security services protect physical, network, and application-layer security. Segmentation is key to controlling access (the network layer), and maintaining logical control (which computers can communicate). Application segmentation isolates apps from each other in case of a breach.

It used to be that if a user was inside the perimeter with a valid login, applications were reasonably secure. Now a higher level of security testing, such as intrusion testing, is required during app development or migration.

Hybrid cloud management and monitoring

We use System Center Operations Manager to manage a hybrid environment of Azure and Windows Server instances. System Center Operations Manager displays server availability, health, and performance data in a single window. This lets the team automate repetitive tasks, monitor availability, and identify potential security issues.

Organizations can quickly build a virtual machine in Azure by using one of the images that the service provides. We use image templates to build virtual machines in both on-premises and Azure infrastructures. Using the same image lets IT stakeholders use the same deployment logic in both environments. It also drastically reduces operational overhead compared to maintaining many static images.

Application development teams use Azure Application Insights to monitor applications. Application Insights lets us send performance, usage, and telemetry data to the Azure portal for review. Users can review information about a Microsoft ASP.NET application, an Azure web application, or a Java website.

To learn more about managing and monitoring the hybrid cloud environment at Microsoft, see Managing a Microsoft Azure hybrid environment.

Capacity planning and efficiency

We have a Hosting Resource and Recovery (HRR) program to provide a sustainable, end-to-end solution for Microsoft teams to examine the use of servers and then categorize the results, bringing them into a tiered-response acquisition process. Servers might be decommissioned, reallocated, or otherwise utilized. HRR drives proper usage of our capacity and reduces unused footprint by targeting areas such as underutilized servers, datacenter closures, fully depreciated hardware, and noncompliant categories. HRR tools and services include:

- **System Center Operations Manager monitoring**. System Center Operations Manager monitoring can be used to collect performance details and aggregate the data into categories of utilization from frozen (not used) to hot (over utilized).
- **Identifying poorly utilized servers**. As a starting point, the HRR team monitors on-premises datacenters and Azure virtual servers daily, using System Center Operations Manager performance analytics. Processor, network, and hard drive data is gathered, and the team then makes a determination based on codified thresholds. A customized report classifies servers into five categories: frozen, cold, warm, hot, and on fire.
- **Mitigating underutilized servers**. Underutilized servers are often abandoned because they are no longer needed or because of hardware degradation. On-premises underutilized servers are prime candidates to move to the cloud. Analyzing cold or frozen Azure servers ensures that servers are resized up, resized down, or turned off when not in use. An exception process supports known scenarios for underutilized servers, such as disaster recovery and inactive cluster nodes.

For more information about capacity planning and efficiency, see Managing resource efficiency in Azure and on-premises datacenters.

Networking

Moving to the cloud challenged the existing network infrastructure. Cloud migration greatly changed the volume and nature of traffic flows within and outside the corporate network. Over a 15-month period, traffic from internal corporate networks to the Internet increased tenfold. Most of the traffic was headed for public cloud services, replacing traffic that would have previously traveled to on-premises services on internal networks. Overall, the existing network infrastructure was insufficient to deploy and support new cloud-based solutions at Microsoft. Two main areas where we improved networking were:

- **Distributed Internet and Azure public edge**. We replaced legacy network proxies with hardware-based firewalls to achieve a more distributed and higher capacity configuration. By implementing both a default Internet and Azure public edge, Microsoft cloud destinations can be treated differently in terms of security and service levels from all other Internet-bound traffic.
- **ExpressRoute**. We initially deployed ExpressRoute to address the need for reliable, high-performing, and secure connections between on-premises applications and infrastructure services with computing resources in Azure.

We are modernizing our network architecture. The network edge is growing dramatically. All email and business productivity applications now exit the perimeter. Colors represent logical or physical connections designed for specific services. Those connections need to be optimized for different services. We continue to drive network simplification by reducing network investment and pushing network functionality to apps or resources.

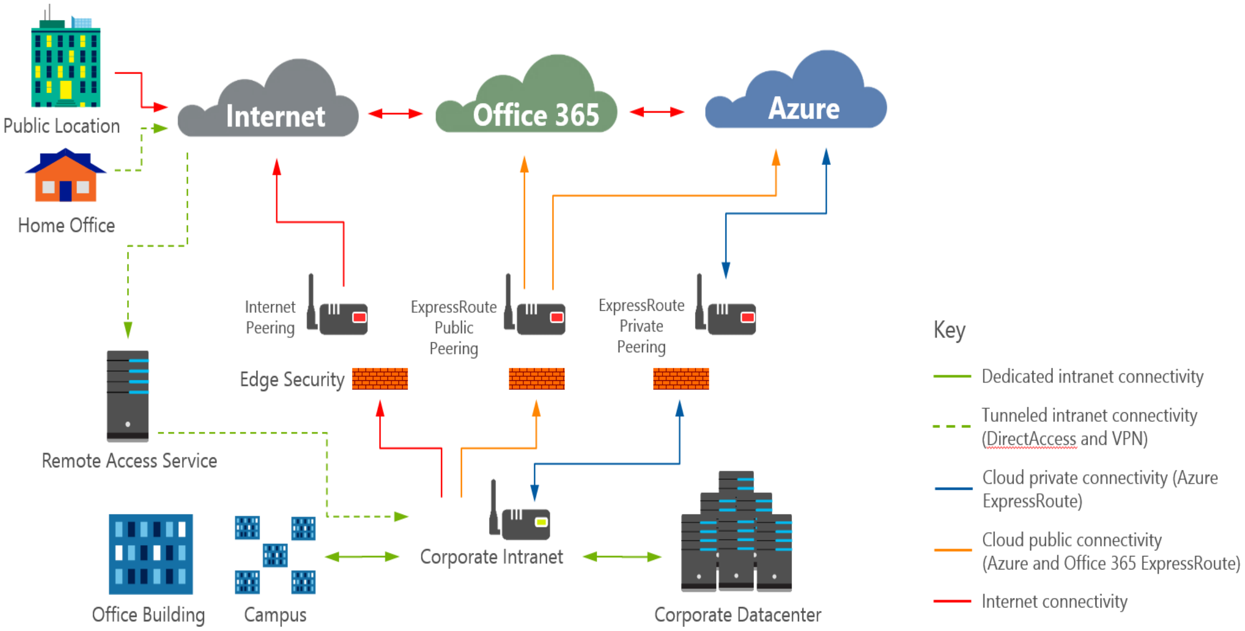
Public Location
Home Office
Internet
Office 365
Azure
Internet Peering
ExpressRoute Public Peering
ExpressRoute Private Peering
Edge Security
Remote Access Service
Office Building
Campus
Corporate Intranet
Corporate Datacenter
Key
Dedicated intranet connectivity
Tunneled intranet connectivity (DirectAccess and VPN)
Cloud private connectivity (Azure ExpressRoute)
Cloud public connectivity (Azure and Office 365 ExpressRoute)
Internet connectivity

Figure 3. Modernizing the network architecture at Microsoft.

Modernizing application development

Within Microsoft, many different organizations develop their own applications. An analysis of applications revealed that for many, all functionality was contained within the application itself. This design made the application large, cumbersome to host, and difficult to maintain. We decided to modernize application development strategies and make them more efficient.

We first created a shared group of internal business and data services. The business, data, and utility services can be used by applications throughout the organization. The services ensure that developers and engineers consistently interact with the same resources and data. Design principles were applied to make adoption and integration of new, modular applications as simple as possible. At the same time, low-level functionality like notification, logging, and security processing functionality were encapsulated into reusable utility services.

Today, it no longer takes three months to release a new feature. With the flexibility and speed of the modern engineering approach, high-priority projects are released in as little as two weeks from inception. Ultimately, the team plans to deliver incremental updates on a continuous basis—to release every day.

For more information about our modern application development strategies, see Improving the Microsoft enterprise network for public cloud connectivity.

Culture and organizational change

Many of the benefits of cloud adoption have enabled us to be a strategic partner to the business. By reducing operational overhead, we are able to focus on delivering value and capabilities to the business. Customer experience is paramount, and all disciplines collectively own the experience and the service, and are committed to the Live Site culture.

The cloud has boosted forward-thinking and strategic technology investments. Experimentation is encouraged and failures are used as learning opportunities that are widely shared. With the shift to the cloud, our core role has changed as well. Where we used to act as a central owner and allocator of resources, the distributed model of cloud computing means that we now have to effectively manage an environment that is increasingly self-service.

Adapting roles

Beyond the need for changes to organizational culture, our specific roles must adapt to support the cloud model. This was identified as one of the greatest benefits of cloud computing migration, but also the most disruptive. Once migration to the cloud occurs, IT organizations are less involved in the day-to-day operations of running servers, and are free to expand their roles to include more solution-focused responsibilities. This provides additional opportunities for IT professionals to develop their careers, as they move from technology and service providers to business process enablers.

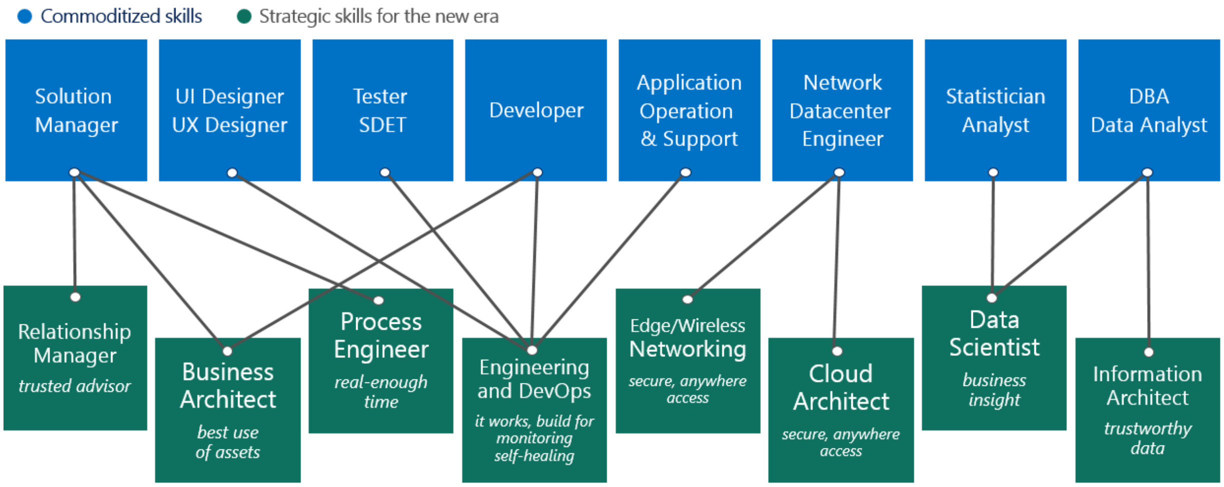
● Commoditized skills
● Strategic skills for the new era
Solution Manager
UI Designer UX Designer
Tester SDET
Developer
Application Operation & Support
Network Datacenter Engineer
Statistician Analyst
DBA Data Analyst
Relationship Manager trusted advisor
Business Architect best use of assets
Process Engineer real-enough time
Engineering and DevOps it works, build for monitoring self-healing
Edge/Wireless Networking secure, anywhere access
Cloud Architect secure, anywhere access
Data Scientist business insight
Information Architect trustworthy data

Figure 4. The evolution of the IT pro skill set

Faster development, cost savings, and operational efficiency

The ongoing cloud migration at Microsoft has yielded faster application development, cost savings, and operational efficiencies. The graphic below shows the trends of physical servers and IaaS/PaaS adoption, as well as incident trends.

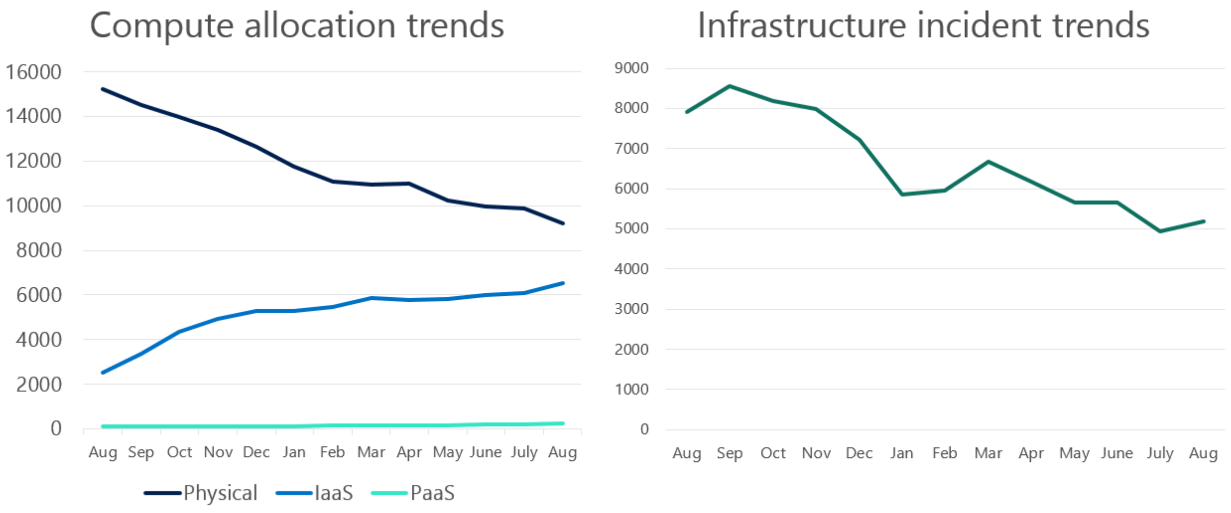

Figure 5. Changes in computing resource allocation and infrastructure incident trends.

Automation has increased, and support costs have decreased, as the adoption of PaaS and IaaS has accelerated year over year (YoY). At the same time, the number of on-premises physical and VMs has decreased, and the number of infrastructure incidents has decreased.

Specifically, the organization has seen:

- On-premises physical servers down 63 percent YoY, from 14,584 to 9,208
- PaaS adoption up 257 percent YoY, from 88 to 252
- IaaS adoption up 286 percent YoY, from 2,536 to 6,507
- Incidents are down 66 percent YoY, from 7,902 to 5,197

As a result, operational costs are down. Using a self-service function, for example, a user can quickly requisition a VM. PaaS automates DevOps functions. Support costs have also decreased.

Well on our way to cloud adoption

We are well on the way to cloud adoption and have realized benefits already. The very speed of technology innovation has accelerated from the time we started our cloud initiative. The cloud has allowed us to create things that didn't even exist when we started the cloud adoption initiative. For example, when cloud apps were created in 2010, Azure containers did not exist. A container runs inside of an operating system, and allows new application architectures. We anticipate a continuing evolution of cloud strategy and adoption.

For more information

Microsoft IT Showcase

microsoft.com/ITShowcase

Managing a Microsoft Azure hybrid environment

Managing resource efficiency in Azure and on-premises datacenters

Driving cloud adoption in an enterprise IT organization

Improving the Microsoft enterprise network for public cloud connectivity