



Cloud Infrastructure

Microsoft Practice Development Playbook

Published: July 2021



aka.ms/practiceplaybooks

About the Playbook

Developed by partners, for partners, as a guide to building or expanding a cloud infrastructure, migration and modernization, and operations and management practice.

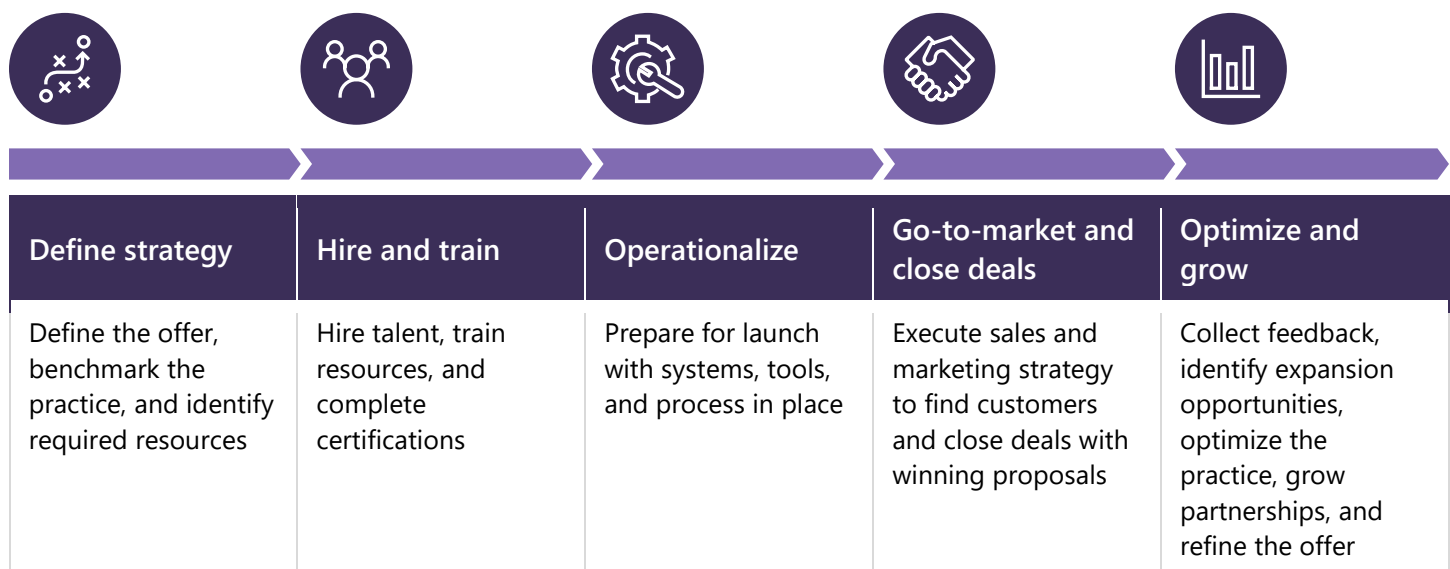
This playbook provides high-level guidance and valuable resources for driving new revenue opportunities, developing strategies for marketing and lead capture, selling, and building deeper and longer-term engagements with customers through potential new offerings such as managed services.

It offers guidance on the technical skills needed, the Microsoft resources available to accelerate learning, and the key opportunities for technical delivery. The intent is to help partners understand the practice opportunity and best practices, not to re-write the existing body of detailed guidance on how to perform any given recommendation. Instead, it points to the relevant resources at any given stage of building an application development practice.

Many of the resources and programs referenced in this playbook require membership in the Microsoft Partner Network (MPN) to access. There is no cost to join. Information about the program and how to register can be found on the [MPN website](#).

Partner Practice Development Framework

The playbook is structured into five stages that take a practice from concept to growth.



How this playbook was made

This playbook is part of a series of guidance written by Microsoft Partner [Opsgility](#), in conjunction with the Microsoft Global Partner Solutions group and 22 other successful Azure partners that have volunteered time to provide input and best practices to share with the rest of the partner community.

To validate the guidance provided in these playbooks, we conducted two separate surveys of 1,136 and 364 global Azure partners with MDC Research. In these surveys, we gathered insights on a range of topics, including how partners hire, compensate and train resources; their business model, revenue, and profitability; what practices and services they offer; and what skillsets they have in place to support their offers. The results of this survey are provided in-line with the guidance found within this playbook.

CONTRIBUTING PARTNERS	
Artis Consulting	Mirabeau
Atea	New Signature
AwareComm	OpenSistemas
Blue Meteorite	PC Solutions
DEFTeam Solutions	Perficient
NTT	PlainConcepts
Empired	Slalom
Equinix	Softjam
Fragma Data Systems	SpanishPoint
Hanu Software	SQL Services Ltd.
Kloud Solutions	Theta

Contents

About the Playbook	2	Identity and access management (IAM)	81
Digital transformation	5	Configuration management	96
Market opportunity	9	Availability and business continuity	98
Define the Strategy	10	Compliance and monitoring	103
Introduction.....	11	Multi-tenant management.....	106
Define the practice focus	12	Management in any environment.....	107
Define and design the solution offer	14	Automated management of virtual machines	109
Define the service offering	16	Support and incident management	110
Additional managed services offerings	26	Automation and DevOps	112
Key Azure services for MSPs	27	Deployment strategies	112
Leveraging intellectual property	38	Deploying code	114
Tools for enhancing solutions with IP	40	DevOps and containers	115
Define vertical offerings	42	Continuous integration/continuous deployment	116
Microsoft licensing options.....	43	Key contracts and practice tools.....	117
Microsoft incentive plans and programs	44	Go-To-Market and Close Deals	118
Define a pricing strategy	46	Introduction	119
Apply for Azure incentive programs.....	48	Identify potential customers	120
Hire & Train	50	Engage existing customers	121
Introduction.....	51	Consultative selling and technical pre-sales	122
Build a team	52	Discovery	123
Management resources	53	Agile as a pre-sales tool	127
Sales and marketing roles	53	Sales compensation planning	128
Technical roles.....	55	Microsoft Technology Centers	129
Support resources.....	58	Architecture design session (ADS)	130
Recruiting resources	59	Phases of a successful ADS	130
Training and readiness.....	60	Implement a proof of concept (PoC)	132
Marketing training	62	Optimize & Grow	133
Business development training	63	Introduction	134
Certifications	65	Partnering with Microsoft.....	135
Operationalize.....	66	Best practices.....	136
Introduction.....	67	Playbook Summary	137
Cloud Adoption Framework for Azure	68		
Azure Well-Architected Framework.....	69		
Cloud-native architecture and design	71		
Enterprise-scale landing zones.....	72		
Choosing virtual machines	74		
Customized virtual machine images.....	76		
Azure Virtual Datacenter	77		
Managing Azure subscription creation	78		
Managing Azure subscription access.....	80		

Digital transformation

The path to unprecedented growth goes through the cloud, helping customers connect people, data, and processes in new ways to embrace the possibilities enabled by modern technologies. To succeed in a digital-first world, business leaders are bringing business and IT closer together and optimizing processes to create new value for customers.

The potential is huge. By 2022, IDC estimates that 70% of all organizations will have accelerated their use of digital technologies, resulting in 65% of global GDP becoming digitized, driving more than \$6.8 trillion in direct digital transformation investments from 2020 to 2023.¹

There are many advantages to adopting the cloud. Businesses moving to the cloud do so for a range of motivations, seeking a variety of benefits. These benefits fall into four categories: cost, agility, service quality, and new scenarios:

- **Cost:** Cloud computing offers significant potential cost-savings over on-premises infrastructure, especially considering the full cost of the latter. In addition, cloud computing enables organizations to move IT spending from capital expenditure (CapEx) to operational expenditure (OpEx). Since the fixed costs associated with shared infrastructure are avoided, the cloud also provides much greater visibility into the true cost of individual applications.
- **Agility:** Where traditional on-premises infrastructure can take weeks or even months to deploy, Azure offers near-instant provisioning of resources. This enables Azure projects to move much more quickly, without the need to over-provision resources in advance or spend considerable time on infrastructure planning. To take full advantage of this new flexibility, organizations are accelerating the adoption of new ways of working, such as by using agile software development methodologies, continuous integration and deployment (CI/CD), and modern PaaS-based application architectures.
- **Service quality:** Azure's infrastructure has been designed to support some of the world's most demanding workloads. These workloads continuously raise the bar on the quality-of-service Azure must provide. As a result, migration to Azure often offers significant improvements in performance, reliability, and security over on-premises infrastructure.
- **New scenarios:** Azure enables new application scenarios which are simply not possible, or would be prohibitively expensive to deliver, using on-premises infrastructure, such as big data storage and analytics, machine learning, and compliance with industry certifications such as ISO, PCI, HIPA and GDPR, where customers can leverage the certifications offered by cloud providers. These technologies are enabling new application scenarios, driving innovation and competitive advantages only available in the cloud.

These changes affect all aspects of a modern business, both internal and external. Microsoft models these changes in four pillars:

ENGAGING CUSTOMERS

- Give them new personalized experiences that bolster acquisition and strengthen loyalty.
- Customer centricity integrated across the business.
- Creating fans & segment of one.
- Data driven customer insights.
- Marketing leaders as technology decision makers.

EMPOWERING EMPLOYEES

- Boost productivity with flexible workstyles and mobile solutions that enable a data-driven culture.
- Intentional about people priorities and related strategies.
- Using more data to drive insights and decision making.
- Delivering self-service & simplifying processes.
- Enhancing HR employee skills.

OPTIMIZING OPERATIONS

- Drive efficiencies with a cloud platform that accelerates agility.
- Harnessing technology for next level of efficiency.
- Leveraging digital platforms to reduce delivery timeframes.
- Testing new products and services at a fraction of the cost.
- Anticipating and solving customer issues before they become issues.

TRANSFORMING PRODUCTS

- Create new revenue opportunities using intelligent technology to innovate new products and processes.
- Leveraging data to enter new markets.
- Revising business models to prioritize agility and emerging trends.
- Making customers business partners.
- Connecting products to amplify and redefine their value.

FURTHER READING

- ➔ [Microsoft Digital Transformation eBook Series](#)
- ➔ [Designed to Disrupt: Reimagine your apps and transform your industry](#)

These benefits are all central to a successful digital transformation strategy.

Reduced costs and the shift from CapEx to OpEx dramatically lowers the cost of innovation, enabling a 'fail-fast' experimental approach.

This is supported by the increase in agility that lowers innovation cost and enables a faster time-to-market. The scale, performance, reliability, and global reach of the cloud enables small development teams to develop global services for global audiences.

Most of all, new technologies including big data, IoT, machine learning, and AI empower the insight and customer focus upon which digital transformation depends.

These technologies are often only available in the cloud or are prohibitively expensive on-premises. Moreover, competition between major cloud providers is driving a tidal wave of innovation within the cloud itself. New features and services are added on a weekly or even daily basis, providing an ever-richer platform, and enabling business to continue to experiment, innovate, reduce cost, and deliver increasing value.

Embracing the cloud is not simply the easiest, or cheapest, or fastest way to drive digital transformation—it is the only way. For many businesses, the first step on this journey is to migrate existing applications to the cloud.

Business Value of the Cloud



Costs

CapEx → OpEx
Transparency
Cost Savings



Agility

Instant Provisioning
DevOps and CI/CD
Modern Application Architectures
Faster Time to Market



Service Quality

Performance
Scalability
Reliability
Security and Compliance



New Scenarios

Big Data and IoT / Analytics
Machine Learning
Artificial Intelligence
Digital Transformation

Partners play a key role in helping businesses make the platform and cultural shifts needed, and such transformations are creating amazing partner multiples. IDC estimated that for every dollar of revenue that Microsoft generated in 2020, partners generated an additional \$9.58 of revenue through their own value creation (approximately \$984 billion). That multiplier effect is expected to grow to \$10.04 for every dollar of Microsoft revenue by 2024 (\$1.2 trillion in partner revenue)¹.

¹ IDC FutureScape: Worldwide Digital Transformation 2021 Predictions, October 2020

CLOUD OPERATIONS		DIGITAL TRANSFORMATION VALUE
IT becomes an enabler to the business	➔	Driving envisioning and agility
Security by design	➔	Continuous regulatory compliance delivery expertise
Dynamic monitoring with anomaly detection	➔	Proactive insight into end user experience
DevOps tools and processes, CI/CD skillsets	➔	Scale up, scale down, and move to different geographies
Solution and application-based SLAs	➔	Meet business outcomes and customer performance expectations
Decentralized operations and resources	➔	Modernize operations
Software and cloud-based solutions	➔	Automation and orchestration
Expertise consulting, designing, architecting, automating, and optimizing for the cloud	➔	Increase agility and optimization

Market opportunity

As companies embrace the opportunities presented by cloud computing to connect with customers and optimize their operations, they will seek help in migrating their systems, applications, and services, and then to managing, automating, and optimizing them for the Microsoft Azure platform.

CHANGING BUSINESS NEEDS WITH THE CLOUD

As organizations transform digitally, technology becomes the source of competitive differentiation and customers are asking themselves how their current organizations need to change to adapt into delivering a successful and sustainable digital business. With IT organizations becoming the primary means of meeting the needs of the business they need to evolve from supporting the business to being a part of the business by delivering value through services hosted in the cloud.

Cloud migration is a highly technical endeavor and requires skills and experience that are lacking in traditional IT departments. Recognizing this, many businesses seek outside expertise to help them with their cloud migration journey. And as IT organizations become more closely aligned with the business, their roles and responsibilities will also evolve. Many customers see IT staff transitioning directly into business units which takes away from core IT. This creates a three-fold business opportunity for partners: First, to provide application migration services; second, to provide the ongoing maintenance, support, and related services for migrated applications; and third, to become a trusted, strategic partner in the customer’s digital transformation journey, by leveraging the data generated by those applications to deliver insight, innovation, and enhanced services.

BUSINESS VALUE AND AGILITY IN THE CLOUD

As customers transition to cloud computing platforms, they are faced with managing not just a new set of technologies, but also a new way of approaching the management and operations of their digital estate. While the cloud can bring greater business value and agility, it can also bring new concerns, including cloud sprawl.

PC Sprawl (1995+)	Server Sprawl (2000+)	Cloud Sprawl (2015+)
Active Directory	Management suites	Managing PaaS and SaaS applications in addition to IaaS
Patch, asset, mobile management	Virtualization, monitoring, patch, backup	Security, threats
Secure access	Identity, workload	Monitoring, backup

Partners must be prepared to help customers understand how to manage, automate, and optimize their digital estate hosted in Microsoft Azure. In addition, partners should be positioned to ensure that customers have a solid foundation on which to execute their cloud strategy.



Define the Strategy

Cloud Infrastructure



aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

With an understanding of the opportunity for building a practice focused on the delivery of Azure migration, operations, and management services, the first step is to define the strategy to build the practice.

There are many benefits to the cloud, and not every customer has the same motivations. Understanding the value proposition is the first step in the process of defining the service offerings.

Next see the revenue models and pricing models for both application migration and on-going managed services, showing how partners can maximize their returns by aligning their pricing to the value offered by their services.

Finally, learn how to identify and close a deal for a migration project, including the common objections. This section closes with an outline of the implementation approach that will be the focus of the remainder of this playbook.

Define the practice focus

Customers will have varying needs based on how far they have come in their digital transformation journey and how established their digital estate is today.

The ability to address customer needs at any phase of their cloud transformation is the hallmark of successful cloud service delivery and management practice. Customers may at the start of their journey, looking for help deciding which applications can be migrated, the impact on the organization, and the dependencies of the application. Others may have existing on-premises deployments today which are targeted to be migrated to an Infrastructure-as-a-Service (IaaS) environment, or current applications which are being transformed for hosting in a Platform-as-a-Service (PaaS) offering.

And some customers will already have one or more Azure subscriptions, application deployments, and cloud-ready applications in use day. They might be looking to add more workloads to the cloud or build deeper integrations to create systems of intelligence for better analytics. In the cloud, partners can continue to optimize and create more value.

Migration and modernization

Prior to defining the practice strategy, it is helpful to understand the migration process. At a high level, it can be broken down into three key phases: Assess, migrate, and optimize.

ASSESS

The assessment phase is where the team will use a mixture of software tools and consultancy best practices to discover what applications can be migrated, what their current configurations are, the people within the customer organization that will be impacted by the migration, and the dependencies of the application. The output of the assessment will include a comprehensive plan for what to do with the application and the expectations on availability and functionality.

This phase is discussed in detail in the [Migration assessment section](#) of the playbook.

MIGRATE

The migration phase is when the recommendations in the assessment plan are put into place. The following steps are usually taken.

- Setup Azure subscriptions using best practices for security, connectivity, policies, and general governance prior to migration to ensure that customers are using Azure correctly from the start.
- Perform the migration using the prescribed method identified in the assessment plan: rehost, retire, replace, rearchitect or retain.
- Evaluate and test to ensure the migrated application meets the criteria outlined in the assessment.
- Learn more about rehosting applications in the [Lift and Shift section](#) of the playbook, and to learn more about rearchitecting applications for Azure see the [Modernizing Apps section](#).

OPTIMIZE

In the optimization phase, partners will use Azure security and management resources to govern, secure, and monitor the cloud applications in Azure. This is also the time to look for opportunities to optimize spending. Common tasks at this stage are:

- Review Azure Cost Management and Azure Advisor to track spending and identify areas for cost savings.
- Evaluate migrated applications for opportunities to right size over provisioned virtual machines and services.
- Implement automation to resize or stop based on a utilization schedule.
- Identify applications that could benefit from optimization with platform as a service (PaaS) services or containers.

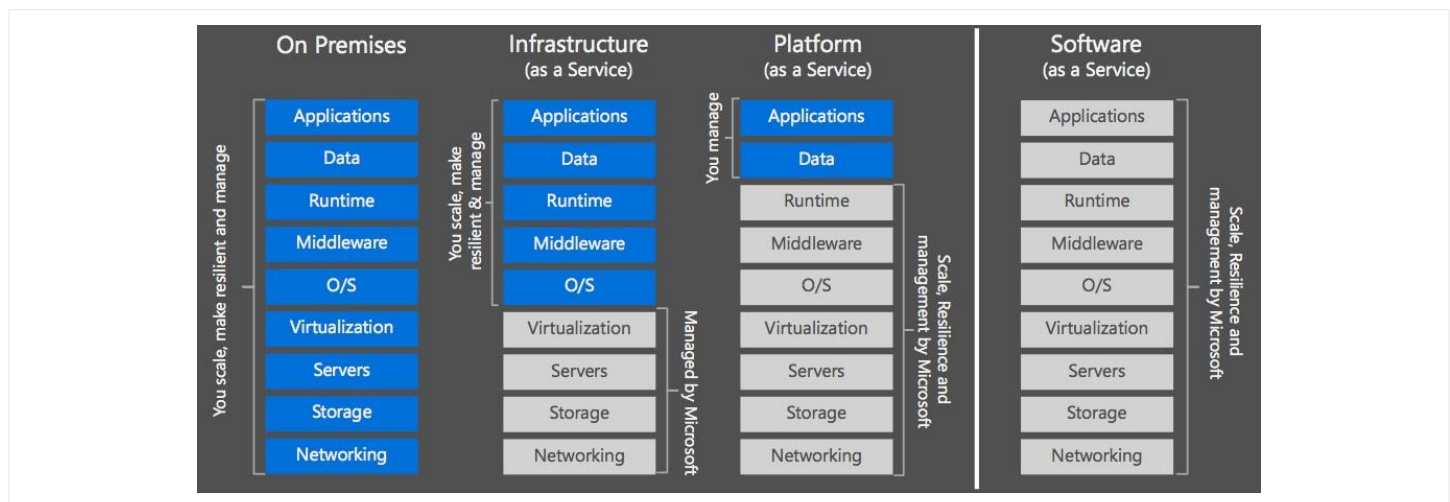
Operations and management

As workloads get migrated to the cloud, partners help customers adopt new technologies and process, keep them productive and secure, and help envision further innovation. Partner services and expertise allows customers and their IT staff to focus on their business and not day-to-day operations.

Customers often will not have the manpower or expertise to monitor and maintain a hybrid cloud environment, or ensure they are secured and prepared for outages, breaches, inefficiencies, and disaster scenarios. Partners offer support while delivering on service level agreements and provide customers with governance over their cloud usage by managing their billing and Azure capacity planning.

IDENTIFY CUSTOMER NEEDS

Some customers will already have one or more Azure subscriptions, application deployments, and cloud-ready applications in use day. Others will be at the start of their journey, looking for guidance on their journey. Customer needs and the services partners can offer will be highly dependent upon their existing technological stack and future goals for when that stack is hosted in Microsoft Azure.



If customers are targeting an IaaS environment, partners can focus on several Azure services, including monitoring and maintaining the security posture of virtual machines, networks, storage, and services related to disaster recovery and backup. As customers mature and begin to entrust their PaaS workloads to partners, additional opportunities will surface such as the ability to monitor application builds and deployments and offer additional automation services.

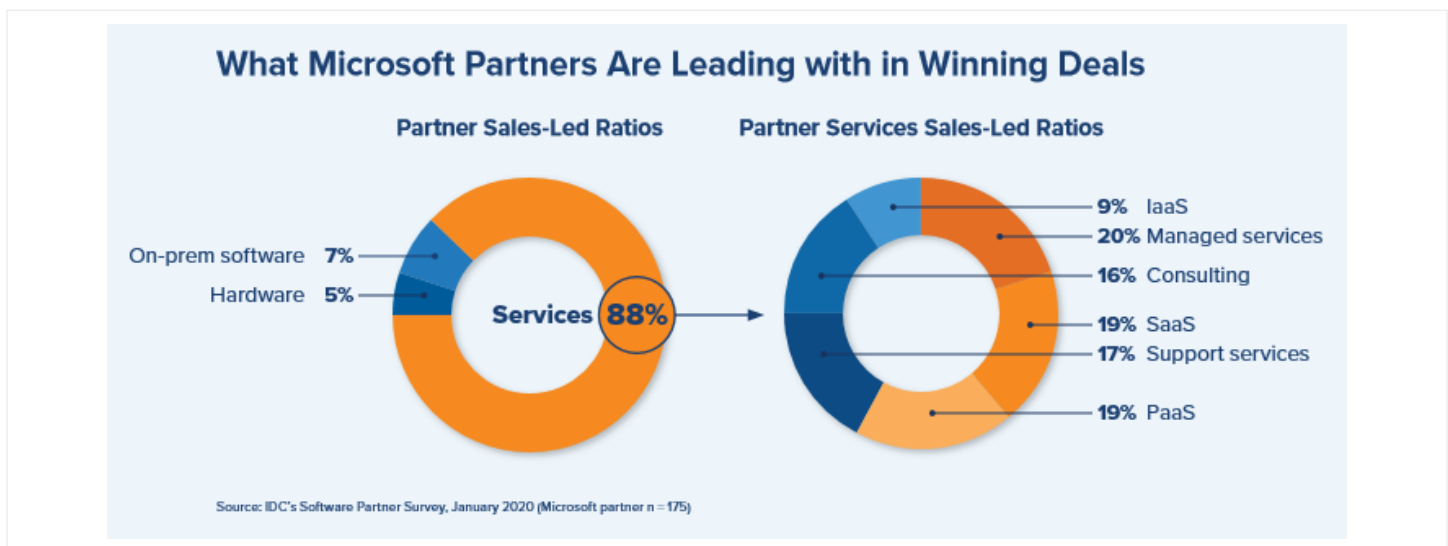
Define and design the solution offer

With the opportunity identified, the next step is to create the solution offer or, ideally, multiple offers based on the solution or set of services.

With the increasing cost of customer acquisition and longer sales cycles, partners are moving ever larger portions of their businesses from project-based time and materials offers to a more predictable outcome-based model with steadier cash flow, that leverages the resources, expertise and skills across projects and customers already in the pipeline and extends the customer lifetime value.

The goal is to shift the conversation from cost avoidance and savings to enabling and transforming the business. As a result, the lift-and-shift cloud project service offerings are fast becoming bundled combinations of Microsoft cloud services, ISV solutions, a partner's own IP, and one or more project, managed, adoption, consumption, or advisory services offered with a monthly subscription fee.

The offers will vary by partner type, but all are driving for higher levels of vertical or workflow specialization with offers that map to where the customers are in their cloud journey and tell an integrated transformation story that extends the customer lifetime value.



MAKING THE SHIFT

Partners that are successfully shifting customers to modern cloud solutions are performing the following tasks:

- Shift from time-and-materials pricing to monthly subscription pricing to maximize margins and cash flow.
- Accelerate the go-live by starting with smaller projects that deliver value and build trust.
- Use analytics and monitor and measure the ongoing customer investment to help them realize ROI sooner.
- Target market segments and specialize by industry or workload.
- Identify three offers for every segment (basic, standard, premium) and make pricing transparent.
- Determine subscription tier pricing (Per user/location/hour/transaction/device, usage, percentage of savings, etc.)
- Ascend the IP staircase toward full vertically integrated cloud solutions.
- Place packaged offers on AppSource or Azure Marketplace.

For more, watch [Nine Steps to Shift from Project Services to Subscription Revenue](#)

MAP OFFERS TO THE CUSTOMER CLOUD JOURNEY

Start by driving the need for cloud optimized versions of traditional on-premises manage services and helping them build their vision and define the business benefits of moving to the cloud. This might be delivered as cloud advisory services with readiness assessments to compel prospects to share their long-range business objectives.

As customers build trust, the next step might be to put higher level resources behind performance monitoring and infrastructure management services.

And as customers move more workloads to the cloud it drives the need for multi-cloud or hybrid cloud management and application integration and management services.

And the last step in the customer cloud journey allows them to focus on innovation using advanced analytics and insights as a service to drive more value from their cloud investment.

RESOURCES

- ➔ [The solution lifecycle](#)
- ➔ [Cloud business development videos](#)
- ➔ [Solution Workspace \(exclusive to MPN members\)](#)

Define the service offering

Different organizations will have different objectives and priorities when moving workloads to the cloud.

For example, some may be strongly motivated by the new business scenarios which the cloud enables, whereas others may be focused on reducing costs or increasing agility. These different customer motivations in turn offer different potential business models for a partner. And the revenue streams from those business models will also differ.

Partners that focus almost entirely on product revenue have the biggest barrier, and typically see margins in the range of 5–20%. This is because the margins for this revenue line are tied to vendor incentives. These partners are subject to changes in strategy and the desire to fund programs and have the least control over their own destiny.

Project services typically drive a range of approximately 35% gross margin, but this has been under pressure for some time. This is a result of little differentiation in the channel, which has caused billable price points to hold steady over the past five or more years. Concurrently, increasing salary and benefit costs of consultants and inflation have eroded profitability. As a result, aggressive and entrepreneurial members of the channel have adapted and gone after the higher-margin opportunities of managed services, which generate on average 45% gross margin and packaged IP, which often exceeds 70%.

It is these partners who are setting themselves up to be rewarded. Mergers and acquisitions spaces are quite active. The partners who gravitated toward the recurring revenue lines and realized healthy growth are being presented with much higher valuations. This can have a dramatic increase in the cash event of the company and overall shareholder value—far higher than what a traditional partner focused on product and billable services can realize.

A business plan is a critical asset that can help envision and think through the details of a practice, identify gaps the will need to be addressed, and explain the fundamentals of the practice to others. Leverage the [Cloud Practice – Develop a Business Plan](#) guide for details, profitability scenario overviews, business plan templates, and financial models.

Read on to understand what types of project services, managed services, and intellectual property to consider in an cloud practice, and leverage the [Define and Design Your Solution Offer guide](#) define the value proposition, solution and vertical offerings, and partnership opportunities.

Migration services

The most common service offered is 'lift-and-shift' migrations to Azure infrastructure services (IaaS). This focuses on cost reduction by reducing or removing the dependency on on-premises infrastructure. Within this area, a range of complementary services can be offered, such as migration assessments and networking services.

In addition, some providers focus on application modernization—transforming existing applications to take advantage of Azure platform services (PaaS). While these are more complex and typically longer migration projects, they provide increased agility and manageability in addition to cost savings.

Some partners specialize in enabling new business scenarios, working with customers at the business rather than infrastructure level to re-define existing processes to take advantage of advanced cloud technologies such as machine learning and big data. These projects are the most complex, but also have the potential to deliver the greatest value by generating new revenue streams as well as reducing costs.

Offerings can vary in other ways. For example, ongoing application support can be offered at different levels, from 24-hour response times, down to 1-hour or even 15-minute response times as a premium service. Some providers focus on Azure-based services, while others provide a hybrid service spanning on-premises infrastructure, traditional hosting, and Azure.

It is not an either/or choice. For example, a common combination is for a partner to specialize in 'lift-and-shift' migrations, and to provide application modernization as an additional service once those applications are migrated. Another example is providers whose operations teams specialize in extracting business insight from application usage data once the application has been migrated.

Within each of the major service areas—migration assessment, migration execution, and (especially) ongoing operations—there are a wealth of opportunities for additional services offering additional value. For example, some customers choose to run their own operations, but will need guidance and training on how to transform and optimize their processes and roles.

Top professional services provided when migrating to Azure

- Implementation and migration
- Architecture and design
- Proof of concept
- Cloud assessment
- Network assessment
- Application modernization development
- Network remediation and hybrid connectivity

Other project services

Project based services are services to help customers design, configure, implement, or support a solution and are typically charged on a one-time or non-recurring revenue basis. For example, a key service for making an organization cloud ready, is an Azure governance service, setting up customers' subscriptions for governance.

For customers with a hybrid cloud platform, cloud networking is foundational service and could involve extending an existing wide area network to the cloud with [Azure ExpressRoute](#) or to providing connectivity services between virtual networks using site-to-site VPN or peering.

By automating routine tasks partners can lower their delivery costs and offer superior SLAs – driving a virtuous cycle of efficiency and repeat business. Automation is the key to creating the right balance between cost, reliability, speed, and time to market.

AZURE GOVERNANCE

Azure provides several built-in tools to help apply governance at scale. A resourceful cloud practice can also build tooling, scripts, templates, and policies to accelerate customers to apply more control. Key services for this offering include:

- Configure and set up the Azure Enterprise Agreement (EA) portal
- Configure governance for the control of create/read/update/delete, naming, tagging, cost, and auditing/logging of Azure resources using the following services:
 - [Azure Management Groups](#)
 - [Azure Resource Manager Policies](#)
 - [Azure Blueprints](#)
 - [Configure Role Based Access Control \(RBAC\)](#)
- Set up Power BI for Azure EA monitoring
 - With [Microsoft Azure Consumption Insights for Power BI](#), partners can enable customers to quickly import and analyze their Azure consumption data in Power BI for insights into which departments, accounts, or subscriptions are consuming the most. It also provides visibility into which service the organization used most and trends for spending and overall usage.

HYBRID CLOUD NETWORKING

Many customers are developing a multi-cloud strategy and lack the technical expertise required to connect their existing data centers or sites to the cloud and build a disaster recovery solution between their location and the Azure cloud. Customers are often unsure of how much bandwidth or capacity is needed, or they have compliance issues and are not sure how to protect their infrastructure to build compliant solutions. Key services for this offering include:

- Network design and bandwidth planning.
- Enabling hybrid connectivity with ExpressRoute or Site-to-Site networking (or both).
- Building geo-redundant or multi-cloud solutions with Azure Traffic Manager.
- Performing network readiness assessments for Office 365 customers that require ExpressRoute.
- Deploy firewall virtual appliances and network security groups to secure the network and ensure compliance.
- Implement secure connectivity for remote administration and development and test with point-to-site networking.

RESOURCES

- | | |
|--|--|
| ➔ Azure ExpressRoute | ➔ Protecting the Cloud Boundary with Azure |
| ➔ ExpressRoute for Office 365 and Dynamics CRM | ➔ Azure Traffic Manager |
| ➔ Optimize ExpressRoute routing | ➔ Azure Virtual Network Peering |
| ➔ Apply to become an ExpressRoute Partner | ➔ Protecting Data and Privacy in the Cloud |
| ➔ Site-to-Site VPN | Whitepaper |

AUTOMATION AND DEVOPS

Automation and orchestration are extremely important functions for a successful Azure practice. It offers significant customer benefits as it can optimize Azure spending and increase reliability for workloads that have varying resource requirements.

Key customer challenges:

- Lack of technical expertise required to efficiently manage PCs, servers, software, user access, and policies.
- Lack of a unified toolset for implementing an appropriate configuration management work stream.
- Lack of a unified management plan and instead carries out changes on live equipment on an ad hoc basis.
- Lack of resources and knowledge to maintain their own system and integrate automation capabilities.
- Automation tools are perceived as too complicated and too expensive to implement.
- Lack of familiarity with DevOps approach to operations – or unable to bring the cultural change required to adopt DevOps as a way of doing things.
- Fear and uncertainty surrounding the loss of control associated with automation.
- IT environments are not mature or well defined enough to warrant automation.
- Developer costs associated with unnecessary development resources.

Key services for this offering:

- Template and script authoring.
- Automatic start and stop of virtual machines.
- Cost management of developer cloud resources.
- Automatic scale down of services.
- Continuous deployment and integration.
- Configuration management.
- Container management.

Some other popular project-based services to consider include:




Backup and storage deployment	Health checks
Virtualization migration and deployment	Custom application development
Proof of concept	Training
Systems integration	Network readiness assessment
Deployment services	Security and compliance enablement
Solution configuration/customization	Security and compliance assessment
Disaster recovery deployment	Scalability and load testing
Solution analysis, scope, and design	Mentoring
Data center migration	Bandwidth planning
Cloud readiness assessment	Network remediation
Solution support and training	Security-penetration testing
Simple file server migration	Desktop virtualization
	Cloud solution costing and spend optimization

Managed services

With managed services, customers are offered white-glove services on a regular basis spanning planning and enablement to day-to-day operations and support.

For more than 20 years, large enterprises have relied on service providers to manage their IT assets and workloads, either in their own data centers or those operated by their customers. The cloud, however, requires a new method of management because of its focus on scale, elasticity, and automation. For CIOs, cloud represents a paradigm shift in the way they think about embracing IT. Dev-ops has completely changed the way applications are developed and maintained. The hyper-scale nature of cloud provides a completely new meaning to scalability, elasticity, and resiliency—and has redefined how applications are architected and delivered. The pay-as-you-go model provides a fail-fast, agile method of app development. Device and data proliferation mean customers want to—and can—do so much more with their IT assets, with cloud providing the computing resources.

Because of the cloud, CIOs are demanding a new way to think about data governance and security. A cloud MSP is someone who helps their customer transition to (and embrace) this paradigm shift in technology—by guiding them in all aspects of their cloud journey. From consulting to migrations, to operations management, cloud MSPs show customers all the benefits that come with cloud adoption.

		
PLANNING	ENABLEMENT	SUPPORT OPERATIONS
<ul style="list-style-type: none"> Assess the customer's IT environment and determine risks and policies that are viable security opportunities Deliver ongoing Security Assessments utilizing Secure Score Offer customers a roadmap based on their Secure Score mitigation or recommendations Provide TCO and ROI analysis for moving their security to the cloud 	<ul style="list-style-type: none"> Migrate workloads to Azure and Office 365 Remediate security gaps found in the Security Assessment Workshop Address security needs across enterprise, including on-premises Optimize security workloads for apps running across on-premises and in Azure and Office 365 cloud environments Optimize advanced security workloads 	<ul style="list-style-type: none"> Offer further support while delivering on SLAs and uptime guarantees Operate and monitor the customer's Azure, Office 365, and hybrid cloud environments Provide customers with governance over their cloud strategy by managing their policies

TOP MANAGED SERVICES

Support as a managed service: MSPs need to consider the level of support that makes sense in terms of resources and revenue to assist customers with outages, breaches, inefficiencies, and disaster scenarios.

Security as a managed service: MSPs can offer their services to ensure enterprise clients are secured and that they are prepared for outages, breaches, inefficiencies, and disaster scenarios.

Cloud monitoring services: Most mid-market and enterprise organizations simply do not have the time, resources, or dedicated staff required to monitor every aspect of IT, and this is where MSPs add the most value.

Hybrid device management: MSPs can add value to organizations facing the challenge of managing and maintaining compliance over BYOD and organization-owned devices.

Identity and access management: Azure Active Directory provides a comprehensive, enterprise-grade identity and access management solution. It works with on-premises Active Directory to offer an integrated solution enabling a common identity to be used to access both on-premises and cloud-based services, including third-party services.

Support as a managed service

One of the most important functions of a managed service practice is supporting customers once their applications and data are firmly in the cloud. No matter how well a cloud or hybrid environment is planned, provisioned, operated, or monitored, problems will arise. It is the job of a Managed Service Provider (MSP) to deal with outages, breaches, inefficiencies, and disaster scenarios. MSPs need to consider the level of support that makes sense in terms of resources and revenue, as well as the customers they serve.

KEY CUSTOMER CHALLENGES

They lack the expertise and resources to troubleshoot problems.

They are unable to determine the root cause of performance issues and glitches.

They do not know how to remediate problems when they correctly identify them.

They do not want to spend time and resources fixing problems.

KEY SERVICES FOR THIS OFFERING

- **User support:** Provide support for frequently asked questions, setup and usage, best practices, questions around billing and invoicing, break-fix support for developers, architecture design, and solution design support for architects.
- **System support:** Provide customers with information on any service interruption, and relay expectations on when the system will be back online.
- **Product support:** Provide support when the Microsoft product is not working as expected or the service stops working. Escalate to Microsoft when the issue cannot be resolved with existing documentation and/or training.
- **Extended support hours:** Many customers need the ability for 24/7 support but cannot justify the overhead internally.
- **Account management:** Offering an account manager that is responsible for reporting service consumption and ultimately minimizing time to resolution is a service that can be offered at a premium.
- **Dedicated support:** Engineering resources that already know the customers' environment, including the business and technical reasons for how a solution was implemented can add a tremendous value over the lifetime of an agreement.

Security as a managed service

The current digital security landscape for businesses can accurately be described in one word: complicated. More numerous and advanced threats, more nebulous and complex compliance requirements, more difficult and intricate infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job—and organizations are having trouble keeping up. The graphic below illustrates the myriad offerings and postures taken by security companies, highlighting the fragmented nature of the market. However, this harsh environment represents a significant opportunity for partners looking to offer security as a managed service.



For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. MSPs can offer their services to ensure enterprise clients are secured. But in this age where we hear about security breaches almost daily, how can partners help customers stay ahead of the game, and avoid becoming a statistic?

KEY CUSTOMER CHALLENGES AND QUESTIONS

- They lack the tools and expertise to effectively get ahead of security threats and compliance risks.
- They are unable to identify, assess, and mitigate security risks.
- They can detect threats but are unable to correctly respond in a timely fashion.
- They are unfamiliar with security best practices and the overall threat landscape.
- They are confused with the myriad offerings out there.

EXAMPLE OF A SECURITY MANAGED SERVICES OFFERING

Basic	Pro	Premium
\$ per user per month with Microsoft 365	\$\$ per user per month with Microsoft 365 and EMS	\$\$\$ per user per month with Microsoft 365 Advanced Security & Compliance and EMS
<ul style="list-style-type: none"> Plan and deploy Microsoft 365 capabilities Provide end-user training Email and data migration to cloud Deliver end user support and incident management 	<ul style="list-style-type: none"> Plan and deploy Enterprise Mobility Suite Increase incident and user support roles Create monthly services health reports and manage critical IT services dashboards Enable Advanced Threat Analytics, device management and Identity Management services + Basic benefits 	<ul style="list-style-type: none"> Monitor the following services: <ul style="list-style-type: none"> SaaS app usage Top targeted users Unusual sign-ins Potential threats Sensitive information sharing to external users Manage customer security policies including secure score reports Support data classification policies + Pro and Basic benefits

SECURITY OFFERINGS	PROTECT	DETECT	RESPOND
Identity	Eliminate passwords, use multi-factor authentication, move to risk-based conditional access	Proactive notification of suspicious behavior and unusual authentications	Automatically elevate access requirements based on risks
Device	Device encryption, management of devices, consistent compliance	Auto-identify suspicious or compromised endpoints	Block, quarantine suspicious devices
Apps & Infrastructure	Identify unsanctioned apps and enforce policies on cloud resources, monitor cloud data	Detect any deviations from baseline, policies, or behavior	Deploy new controls and block risky apps
Data	Policy-based data separation, containment, classification, and encryption	Notification of any attempts for unauthorized data access	Revoke unauthorized access to documents, wipe device data

Cloud monitoring services

Back in the early 2000s, managed services was synonymous with remote management and monitoring (RMM).

In the cloud world, the tools and requirements have evolved, but the problem statement hasn't fundamentally changed: How do customers monitor the health and performance of their IT infrastructure? Most mid-market and enterprise organizations simply do not have the time, resources, or dedicated staff required to monitor every aspect of IT, and this is where MSPs add the most value. While Azure offers many monitoring capabilities built into the platform, there is still a place for partners who can provide additional, deeper tooling, triage the alerts, and proactively act upon the alerts before any measurable loss in performance.

KEY CUSTOMER CHALLENGES

- Do not have the time or resources to monitor all my hosted and internal IT assets.
- Need a single view that tells them how their apps and VMs are performing at any point in time.
- Find it challenging to diagnose the root cause of breakdowns or outages.
- How do I respond to so many alerts? How do I differentiate the false positives from the concerning ones?

KEY SERVICES FOR THIS OFFERING

SYSTEM HEALTH MONITORING	LOG ANALYTICS AND ALERTING	DATABASE MONITORING	APP PERFORMANCE MONITORING
Complete monitoring of VMs, CPU utilization, memory usage, storage IOPs, and OS performance. Includes monitoring of application performance and operation health, and dashboards and reports on system health	Every client, device, and user accessing a network produces data that is logged. Analyzing those logs can offer deep insight into performance, security, resource consumption, and several other meaningful metrics	A view into the customer's database that helps MSPs ensure high availability of database servers. The process involves keeping logs of size, connection time and users of databases, analyzing use trends, and leveraging data to proactively remediate issues	End-to-end tracking of all aspects of an application (or webpage). App monitoring involves watching every part—from shopping carts to registration pages—of a customer's app(s) for performance issues to provide the best user experience possible

RESOURCES

- [Azure Advisor](#)
- [Azure Application Insights](#)
- [Azure Diagnostics](#)
- [Azure Monitor](#)
- [Azure Monitor logs](#)
- [System Center](#)
- [Automation](#)

THIRD-PARTY RESOURCES

- [App Dynamics](#)
- [Nagios](#)
- [New Relic](#)
- [Science Logic](#)
- [Splunk](#)
- [Logic Monitor](#)

Hybrid device management

With the increasing demand to support bring-your-own-device (BYOD) scenarios, organizations are faced with the challenge of finding the right balance between allowing their employees to choose which devices they use, while making sure those devices have access to the right set of applications and meet corporate data protection and compliance requirements.

KEY CUSTOMER CHALLENGES

- Demand their own choice of devices and apps.
- Expect anywhere connectivity and productivity.
- Needs to maintain compliance and data protection.
- Must avoid the complexity and cost associated with many discrete management infrastructures.

KEY SERVICES FOR THIS OFFERING

	<p>Microsoft's solution builds on market-leading client management by combining System Center Configuration Manager with Microsoft Intune to provide organizations with a comprehensive, cross-platform, and user-centric way to deploy applications and manage users' devices, whether they are corporate-connected or cloud-based.</p>
	<p>With Configuration Manager and Intune, organizations can enable their employees to choose devices, unify management infrastructure, and simplify IT administration. IT can deliver and manage consistent application experiences for employees based on their corporate identity, network connectivity, and device type, helping maintain productivity as employees use various devices throughout their day. Through a single infrastructure and administrative console, IT can manage PCs, servers, mobile devices, endpoint protection, and virtual machines across various platforms, including Windows, Linux/Unix, Mac OS X, iOS, and Android.</p>
	<p>Simplified server and client deployment, streamlined updates, and consolidated reporting enable an IT staff to easily manage mobile, physical, and virtual client environments, reducing costs and increasing efficiency through comprehensive application and device management. Unified security, including System Center Endpoint Protection, protects corporate information and helps better manage risk by deploying software updates and antimalware definitions to PCs, as well as enabling selective wipe of mobile devices. New improvements—such as the support of latest Windows 10 features, Windows in-place upgrade, more frequent and easier updates, unified end-user portal, and on-premises MDM—make deploying and managing Windows easier than ever.</p>

RESOURCES

- ➔ [Managing Corporate Devices](#)
- ➔ [Choose between Microsoft Intune Standalone and Hybrid Mobile Device Management with System Center Configuration Manager](#)

Additional managed services offerings

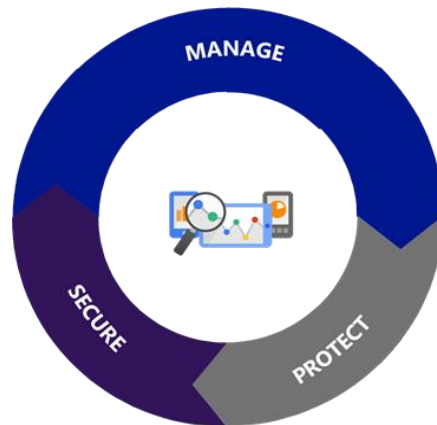
The project services discussed earlier are all potential offerings in a managed service offering. Beyond those, MSPs can offer a much broader set of long-term support and consulting offerings.

In the Microsoft Cloud Practice Development Study, 866 partners that identified as having a cloud infrastructure practice were asked which managed services they offered within their practices. Consider this data when designing managed services-based offerings.

Virtual machine management and upgrading	PowerShell script automation
Configuration management	Network monitoring
Microsoft support (interface between MSFT and customer)	Reporting and analytics
Domain management	Critical response support
Troubleshooting	Anti-virus monitoring
Update and patch management	Reports and dashboard maintenance
Hybrid environment support (basic infrastructure)	Security management and identity protection
User rights and account management	Application lifecycle management and support
Azure consumption monitoring and optimization	Virtual database administration
Reactive help desk support	Data center performance monitoring and optimization
Disaster recovery monitoring and testing	Regulatory compliance via O365 infrastructure
Performance monitoring and reporting	Online training and self-paced learning
Proactive backups and anti-virus monitoring	Virtualization support and efficiency Optimization

Key Azure services for MSPs

Azure offers many services for visibility and control across customer environments – from their on-premises datacenter to Azure, or even to other clouds. Partners can offer services that help their customers manage, protect, and secure their workloads.



Manage

Azure Monitor, Log Analytics workspaces, Application Insights, and Azure Automation are the core Azure services which comprise the management stack. Each of these services can help customers gain visibility into their environments, reduce mean time to resolution when errors do occur, and improve the performance and usability of the applications that they deploy in Azure.



COMPREHENSIVE VISIBILITY

Comprehensive visibility across platform, apps and workloads
Collect and correlate data from multiple sources incl. multi-vendor solutions
Gain insights to act on using machine learning and advanced analytics



REDUCE MEAN TIME TO RESOLUTION

Visualize and alert on the health, performance and utilization
Discover app and network components and map their connections
Detect and respond to issues before they impact users



IMPROVED PERFORMANCE AND USABILITY

Learn, iterate, and improve the performance and usability of the apps



CHANGE AND UPDATE MANAGEMENT

Install OS patches
Track virtual machine changes
Automatically track inventory changes

Azure monitor

All the monitoring data needed to operate and maintain Azure resources is centrally available through Azure Monitor.

Azure Monitor provides base-level infrastructure metrics and logs for most services in Microsoft Azure. Azure Monitor is one of several core monitoring services in Azure and provides fundamental, required monitoring across Azure resources allowing admins to:

- Monitor Azure resources with detailed logs.
- Set up alerts and take proactive, automated actions.
- Use flexible configuration and data consumption options.
- Integrate with analytics and notification tools that are familiar.

VIEW AND MANAGE MONITORING DATA

Azure Monitor provides detailed, up-to-date performance and utilization data, access to the Azure activity log that tracks every API call, and diagnostic logs that help debug issues for customers.

ALERTING AND AUTOMATED ACTIONS

In addition to providing access to customers' performance and utilization data, partners can also configure Azure Monitor with alerts and take automated actions based on those alerts. This allows partners to be proactive with customer workloads that are hosted in Azure by detecting issues before they affect their business. Azure Monitor's automated actions can auto-scale resources, start Automation runbooks, and even call webhooks.

DIAGNOSE OPERATIONAL ISSUES QUICKLY

Not all events can automatically be remediated, so Azure Monitor also provides the tools to analyze and diagnose operational issues in customer environments and resolve them efficiently. Partners can create dashboards with graphs of performance metrics, search through subscription activity, and share insights with customers.

INTEGRATE WITH EXISTING TOOLS

Azure Monitor also integrates directly with many of the other solutions discussed in this playbook, including Application Insights and Log Analytics (also referred to as Azure Monitor logs). Azure Monitor also integrates with a variety of partner tools, potentially allowing customers to leverage existing vendor relationships and technology investments. Partner can also build their own custom integrations by using REST APIs and webhooks to read metric and log data, even log data from custom sources.

Log Analytics workspaces

Centralize log data from multiple systems and environments, including those external to Azure, in a single data store.

Through a Log Analytics workspace, Azure Monitor logs can transform a customer's Azure activity data and managed data resources across one or more subscriptions into actionable insights. Through Azure Monitor logs, partners gain deeper insights into their customer's environments hosted in Azure or on-premises.

- Quickly connect and collect log data from multiple sources.
- Correlate and analyze using powerful machine learning constructs.
- Search and query interactively using an expressive language.
- Develop deep insights use purpose-built management solutions.

COLLECT AND CORRELATE DATA FROM MULTIPLE SOURCES

Azure Monitor logs can help correlate data in new ways using powerful joins and a rich query language. With these deep insights, users can concentrate on the data that is important to them, performing advanced date-time analysis. Azure Monitor logs near real-time capabilities can quickly identify the root cause of operational issues in customer subscriptions.

SMART ANALYTICS

Log data is stored in a Log Analytics workspace which is based on Azure Data Explorer. The interactive query engine used by Data Explorer offers one-click diagnosis of performance issues from the advanced analytics portal. With machine learning, partners have access to advanced learning algorithms to detect and mitigate potential issues before they impact customers.

RICH EXPLORATION WITH INTERACTIVE QUERIES

As queries and visualizations are built, that data can be combined with the data from resources such as Azure Monitor, offering customers a rich view of the performance of their environments while allowing operations resources to understand performance and activity in each environment.

BUILT-IN NOTIFICATION AND AUTOMATION

The data that is stored in a Log Analytics workspace becomes actionable through Azure Monitor, including the ability to natively integrate with service management solutions such as ServiceNow and provides for the correlation of alerts from various sources. Through Azure Monitor, that data can even be automated, with the ability to trigger remediation through Azure Automation, Logic Apps, and Azure Functions.

Application insights

Get rich performance monitoring, powerful alerting, and easy-to-consume dashboards to ensure customer's applications are available and performing as they expect.

Application Insights allows partners to offer customers a cloud-first and cloud-ready application performance management suite. The rich data sets from Application Insights can uncover issues before they become larger problems, identify who and what are affected, and the performance root cause analysis to find and fix issues.

- Detect and diagnose exceptions and application performance issues.
- Monitor Azure websites, including those hosted in containers, plus websites on-premises and with other cloud providers.
- Seamlessly integrate with a DevOps pipeline using Visual Studio Team Services, GitHub, and our webhooks.
- Get started from within Visual Studio or monitor existing apps without redeploying.

APPLICATION PERFORMANCE MANAGEMENT

Data stored in Application Insights can be used show trends in application performance and behavior, identity usage patterns, and get quick answers to questions about website performance. By using the same query engine as that in Log Analytics, partners can leverage the same skillset for operators across multiple solutions.

INTERACTIVE DATA ANALYTICS

The data in Application Insights is powerful on its own, but like many other Azure services, it can be combined with Log Analytics workspaces and Azure Monitor, offering partners the ability to aggregate application performance data, Azure activity logs, and operational data from Azure virtual machines in a single data set.

MACHINE LEARNING

Application Insights includes smart detection capabilities, leveraging machine learning and service analytics which continually analyze application telemetry. Through this continual analysis, the Application Insights service can provide anomaly detection, failure counts, performance changes, and even platform behavior analysis. This data can be actioned through the same notification and alerting mechanisms as Azure Monitor and Log Analytics, again providing a familiar interface for operations to interact with Azure.

DEVOPS INTEGRATION

Application Insights can be easily integrated into existing DevOps processes to bring Application Insights rich monitoring to continuous integration and continuous delivery pipelines. This includes integrations with Visual Studio Team Services or GitHub for issue tracking and resolution.

GET STARTED QUICKLY

Application Insights is not just for a customer's applications – it can also be used to instrument and understand existing websites hosted in IIS, offering partners the opportunity to onboard customers into the service early in their cloud journey.

Azure automation

Automate, configure, and install updates across hybrid environments

Azure Automation delivers a cloud-based automation and configuration service that provides consistent management across Azure and non-Azure environments. It consists of process automation, update management, and configuration features. Azure Automation provides complete control during deployment, operations, and decommissioning of workloads and resources.

- Control hybrid environments.
- Integrate management systems using serverless runbooks.
- Ensure consistent management for Windows and Linux.

LOWER COSTS THROUGH AUTOMATION

By automating operations, partners can focus on work that drives value for their customers. Azure Automation allows partners to automate all their frequent, time-consuming, and error-prone cloud management tasks. This leads to lower operational costs.

UPDATE MANAGEMENT

Azure Automation can be combined with Log Analytics workspaces to offer a cloud-hosted patch and update management services for both Windows and Linux operating systems. With Azure Automation's hybrid capabilities, update management and compliance can be managed across Azure, on-premises, and even other cloud platforms. The rich orchestration engine also provides for defined maintenance windows, exclusions, and more.

CONFIGURATION MANAGEMENT

Azure Automation offers a first-party virtual machine configuration service hosted in Azure with support for Desired State Configuration (DSC). Along with DSC, the automation service can be used to author and manage PowerShell configurations, import existing scripts, and generate node configurations – all in the cloud.

INVENTORY MANAGEMENT

Through Azure Automation's inventory and change tracking functions, partners can provide customers full inventories of operating system resources, including installed applications and even custom configuration items. A rich reporting interface with powerful search allows operators to quickly find detailed information on everything that is configured within an operating system – both Windows and Linux.

Inventory changes can also be tracked across Windows services, Linux daemons, software, registry, and individual files to promptly investigate issues. Inventory and change tracking are built on Log Analytics workspaces, allowing partners to configure automated alerts to track unwanted changes.




INTEGRATE WITH SERVICES

In addition to configuration management, Azure Automation also offers a rich automation and scheduling service based on runbooks that can be authored in.

PowerShell or Python. This allows partners to integrate not just other Azure services, but also any public systems that customers require for deploying, configuring, and managing the end-to-end lifecycle of resources deployed in Microsoft Azure. These runbooks can be triggered from systems outside of Azure, bringing integrations with existing ITSM, DevOps, and monitoring systems to fulfill requests and ensure continuous delivery and management.

Protect

Azure Backup and Azure Site Recovery will allow customers to experience the benefits of high availability, disaster recovery, and backup. With these Azure services, partners can offer a full suite of services around business continuity and disaster recovery.

	REDUCED COST No need to purchase additional hardware No secondary site resource costs Pay for use
	REDUCED COMPLEXITY Faster onboarding with cloud services Simpler execution for testing and failover Integrated business continuity as a service
	INCREASED COMPLIANCE Industry-leading certification portfolio Deploy in one of Azure's 38 global datacenters Increase coverage of applications to meet compliance requirements

Azure backup

Protect customer data with a cloud-based backup-as-a-service

Azure Backup can back up, protect, and restore customer data in the Microsoft cloud. Azure Backup replaces existing on-premises or off-site backup solutions with a cloud-based solution that is reliable, secure, and cost-competitive. All Azure Backup components can be used to back up data to a Recovery Services vault in Azure.

- Keep data in Azure and on-premises safe.
- Backup supports all machines, including VMware and Hyper-V virtual machines running on Linux and Windows, as well as physical Windows Servers.

REDUCE COSTS

Azure Backup is a pay-as-you-go service, giving partners and customers the flexibility to choose the data that they want to protect for as long as they need to protect it. Azure Backup is designed to be cost-effective for both short-term and long-term data retention scenarios. Virtual machines and individual files or folders can be restored – in Azure or on-premises – as needed, for free.

QUICK ONBOARDING AND DEPLOYMENT

Azure Backup enables hybrid deployment and management of customers environments quickly and easily. Backup can be used to protect Azure and on-premises workloads and comes with support for Windows, Linux, VMware, and Hyper-V. When deployed into virtualization environments such as VMware, Backup can automatically detect virtual machines and connect them to Azure.

All customer backup information is surfaced in a centralized dashboard, allowing partners to quickly decide what to restore in an event which generates unexpected data loss. Backup reports can also be exported to Power BI, offering partners richer visualizations and data analysis, along with the ability to share deeper insights with their customers.

RANSOMWARE PROTECTION

In the age of ransomware, customers can never be too careful with their data. Azure Backup allows partners to offer customers piece of mind that their backups are secured through limited access controls, automated notifications if suspicious activity is detected in a Recovery Services vault, and unauthorized deletions are kept for days, providing ample time to secure the environment and start the recovery process.

Ransomware attacks occur every 40 seconds	4,000 daily attacks since 2016 300% increase over 2015	\$5 billion damages predicted in 2017 15x increase over 2015
---	---	---

Sources: <https://securelist.com/kaspersky-security-bulletin-2016-story-of-the-year/76757>, <https://www.justice.gov/criminal-ccips/file/872771/download>, <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion>

Azure site recovery

Reduce application downtime during IT interruptions, without compromising compliance. Azure Site Recovery supports applications in Azure and on-premises, providing comprehensive coverage across Linux, Windows, VMware and Hyper-V virtual machines, and physical servers.

Azure Site Recovery (ASR) contributes to the business continuity and disaster recovery services that partners offer their customers. The Site Recovery service helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines from a primary site (Azure or on-premises) to a secondary location (Azure or on-premises). When an outage occurs at a primary site, ASR will fail over to a secondary location and access hosted workloads from there. And after the primary location is running again, ASR can fail back to it.

REDUCE INFRASTRUCTURE COSTS

Partner can offer lower on-premises infrastructure costs by using Azure as a secondary site for conducting business during outages. Or partners can help customers eliminate their on-premises costs altogether by moving their workloads to Azure and setting up recovery between Azure regions. ASR can perform discovery on customer environments to pre-assess network, storage, and compute resources needed to replicate and run applications all while paying for only the compute and networking resources needed to run customer workloads in Azure during outages.

SIMPLE DEPLOYMENT AND MANAGEMENT

Replicating applications and workloads between Azure regions can be accomplished in just three steps. When it comes to orchestrating a failover, there are often multiple steps and sequencing issues. ASR integrates with Azure Automation, offering partners and customers a wide range of automation options and integrations to orchestrate the recovery of even the most complex multi-tier applications.

TRUSTED RECOVERY

Recovery and backups are only good when they are tested and vetted on a regular basis. ASR makes it easy to test failovers and integrity of failover solutions with isolated recovery options, so partners can test their recovery scenario end-to-end without impacting production workloads or users.

AUTOMATED RECOVERY

After ASR has been deployed, configured, orchestrated, and tested, partners can configure automated recovery of applications to Azure with minimal downtime. ASR is backed by a 99.9 percent SLA and 24x7 support to ensure customers that their applications will be available and compliant.



Before, it could take months and potentially millions of dollars to replicate infrastructure and recover data after a disaster, in addition to suffering disruption of business operations. Now we can recover instantly and at no cost.

JIM SLATTERY,

Chief Financial Officer, Capstone Mining

SECURE

Azure Security Center, Azure Firewall, network security appliances, and advanced networking features of Azure allow partners to secure customer workloads and offer on-going management services around the Azure security stack.

	<p>GAIN VISIBILITY AND CONTROL</p> <ul style="list-style-type: none"> Unified view of security across Azure resources Central management of security policies Integrate with existing processes and tools like SIEM
	<p>DETECT THREATS AND RESPOND EARLY</p> <ul style="list-style-type: none"> Identify real threats with advanced analytics Gain insight into attack campaign with Intelligent Security Graph Remediate quickly with prioritized alerts and recommendations
	<p>PROTECT AGAINST ATTACKS</p> <ul style="list-style-type: none"> Remediate vulnerabilities with ongoing assessment and recommendations Rapidly deploy built-in security controls and integrated partner solutions Reduce attack surface with predictive analytics

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, partners can apply security policies across customer workloads, limit their exposure to threats, and detect and respond to attacks.

Azure Security Center offers partners the ability to ensure their customers deployments are secured with centralized policy management, continuous security assessment, actionable recommendations, advanced cloud defenses, prioritized alerts and incidents, and integrations with connected solutions.

- Monitor security across on-premises and cloud workloads.
- Apply policy to ensure compliance with security standards.
- Find and fix vulnerabilities before they can be exploited.
- Use access and application controls to block malicious activity.
- Leverage advanced analytics and threat intelligence to detect attacks.
- Simplify investigation for rapid threat response.

UNDERSTAND SECURITY POSTURE

Azure Security Center (ASC) brings a unified view of security across a customer's on-premises and Azure-hosted workloads. ASC integrates with Log Analytics, offering automated onboarding of new Azure virtual machines and automated discovery of other Azure resources like Azure Storage and Application Insights. The collected data can include other solutions as well, including next-generation firewalls and other marketplace solutions.

ENSURE COMPLIANCE AND SECURITY STANDARDS

ASC can help ensure compliance with a customer's or regulatory security requirements by centrally managing security policies across all their hybrid cloud workloads. Security policies define the desired configuration of customer workloads and can be tailored to the type of workload, or the sensitivity of the data hosted within those workloads.

FIND AND REMEDIATE VULNERABILITIES

By continuously monitoring the security of customer's machines, networks, and Azure services, ASC can surface vulnerabilities quickly and, in many cases, offers automated remediation. In cases where automatic remediation is not available, ASC will guide admins through the steps to remediate vulnerabilities.

LIMIT THREAT EXPOSURE

Go beyond the basics and offer customers advanced protection, including adaptive threat protect and application whitelisting to identify malware and other unwanted code. Powered by machine learning, these application controls are constantly monitored for compliance.

In addition, partners can enable advanced networking and virtual machine management features such as just-in-time access for controlling access to management ports on Azure-hosted virtual machines to drastically reduce the surface area exposed to brute force and other network attacks.

RESPOND QUICKLY TO ATTACKS

Partners and their customers can leverage the Microsoft Security Graph to get ahead of evolving cyber-attacks, including denial of service attacks and botnets. The built-in behavioral analytics and machine learning can automatically identify attacks and zero-day exploits and send alerts immediately. ASC also bridges pre- and post-breach activity by monitoring networks, machines, and cloud services.

Azure Firewall

Azure Firewall is a cloud-native network security for resources in Azure Virtual Networks

Azure includes a rich networking stack, with security built-in from design, development, monitoring, threat intelligence, and response. Network access control lists (ACLs) can be configured to restrict access on public endpoint IP addresses. ACLs configured on endpoints can further restrict the traffic to only specific sources IP addresses.

Network Security Groups (NSGs) control network access to virtual machines in virtual networks. This collection of network ACLs allows a full five-tuple (source IP address, source port, destination IP address, destination port, protocol) set of rules to be applied to all traffic that enters or exits a subnet or a virtual machine's network interface. The NSGs, associated to a subnet or VM, are enforced by Azure's networking stack.

For even more security, Azure Firewall can be deployed. Azure Firewall is an Azure service – a cloud-based network security service that protects Azure Virtual Network resources and includes built-in high availability and unrestricted scalability.

FIREWALL AS A SERVICE

Azure Firewall is a turnkey stateful firewall service that supports both inbound and outbound traffic filtering. This includes outbound URL filtering through application fully qualified domain name (FQDN) rules with support for wildcards, network traffic filtering rules with allow or deny rules, and support for outbound SNAT and inbound DNAT support.

As a service that protects resources on virtual networks, Azure Firewall also supports hybrid connectivity when deployed to virtual networks with VPN and ExpressRoute Gateways.

CLOUD SCALE

Azure Firewall scales automatically during peak usage without customer intervention and has built-in high availability with 99.95% SLA. There are no additional load balancers to deploy or manage so partners can focus on the configuration of the service itself and the security of the applications and workloads that Azure Firewall protects.

With seamless deployment and zero maintenance of additional infrastructure, Azure Firewall easy to deploy and configure.

CENTRALIZED LOGGING AND ANALYTICS

Logs for Azure Monitor are integrated with Azure Monitor and can also be archived to Azure storage and streamed for Azure Event Hubs for integration with supported security information and event management (SIEM) systems.

THREAT INTELLIGENCE

Threat intelligence filtering allows Azure Firewall to automatically alert and deny traffic from known malicious sources sourced from the Microsoft Threat Intelligence feed. Threat intelligence can also provide protection for outbound connections which can alert to the potential compromise of protected resources.

Azure network appliances

Use network virtual appliances in Azure

For customers with existing network security solutions or who have needs outside of Azure Firewall, many solution providers offer network virtual appliances (NVAs) in the Azure Marketplace. NVAs bring next-generation firewalls, intrusion prevention and intrusion detection systems, web application firewalls, and more to Azure.

- Industries best-of-breed appliances
- Easy to configure and manage.
- Easily scalable and highly available.
- NVAs offer customers the flexibility to protect resources on virtual networks in Azure with familiar tools while leverage existing vendor relationships.
- The latest list of supported vendors and applications can be found in the [Azure Marketplace](#).

DEPLOY ADVANCED NETWORK SCENARIOS

Existing customer environments can be complex, but NVAs allow partners to build and maintain complex configurations which keeps customers security and compliance requirements front and center. By combining NVAs with core Azure networking features like user-defined routes and forced tunneling in hybrid scenarios, partners can offer customers similar network controls as they have on-premises today and in many cases improve their security posture.



Leveraging intellectual property

Reusable IP can drive efficiency and competitive advantage in every step of the cloud migration and managed service cycle.

The idea of coming up with productized IP may sound daunting. But many partners found that they already had IP, it just wasn't packaged that way. As partners perform more migrations, and manage more Azure-based services, they identify common problems and tasks. These can occur at every stage of the migration cycle, from assessment, through migration, and to operations.

Review the most successful projects to see if there are repeatable elements that can be productized across several customer solutions. Repeatable elements can be about vertical or process best practices, or they can focus on common customer pain points. Start small. IP can be a simple template or just a few lines of code that automates a particular function in a way customer market typically needs. Productizing IP and creating repeatable processes has been a very successful strategy for many partners. Some partners are achieving gross margins more than 70% by productizing IP and selling it to their customers on a recurring revenue basis. Productizing IP helps create stickiness with customers and opens opportunities to sell solutions through the partner channel.

Partners can also look to the partner ecosystem for incremental solutions that can be bundled with Microsoft's offerings to round out a total solution. Buying or building their own repeatable processes or technology to automate these tasks gives their practice a distinct offering and competitive edge.

There are multiple opportunities for building intellectual property that can be used to expedite engagements, or even as an entire engagement. With the ability to create fully automated solutions partners can challenge their creative side to offer up solutions that can save their customers money as well as add a striking differentiator.

Examples of areas of investment include:

- A repeatable discovery, planning, and evaluation methodology that streamlines the assessment process.
- Tools to more accurately forecast prices based on designs or usage data.
- Software and services that organize, manage, and scan application workloads and generate planning and cost models that can be implemented in an automated manner to migrate.
- Software that can analyze workloads and their components and recommend alternative topologies and Azure Services that can be used to modernize applications as part of their automated migration.
- An in-house library of Azure Resource Manager blueprints, templates, or scripts to assist with building proofs-of-concept or even production environments.
- A test framework that speeds up the testing phase of the migration process, while also improving test quality and reducing migration risks.
- An analytics system that helps identify cost savings and optimize running systems.

The possibilities are almost endless. Buying (or using as SaaS) migration software, or building repeatable processes and tools enables partners to work faster, with fewer mistakes, and higher quality. It drives down costs, shortens delivery schedules, and improves the customer experience.

INTELLECTUAL PROPERTY OFFERINGS	
Automated backups and disaster recovery	Automated load balancing
Automated monitoring, alerting, and logging	Automated consumption monitoring and reporting
Office connectivity, plug-ins, and add-ons	Automated disaster recovery testing
Customer self-serve portals	Online training and self-paced learning
Pre-configured dashboards	Middleware for hybrid synchronization
External portals for customer information	

PACKAGE REPEATABLE PROCESSES

Another way in which partners are creating IP is by packaging their assessments, documents, and processes into proprietary, reusable components that only they own and can deliver. For example, they might package a service around an application or other solutions built on Azure. Another example would be deploying a managed server for customers. For instance, a SQL host can be deployed with automated patching and backup.

[Azure Managed Applications](#) unlock these capabilities, allowing MSPs to deliver turnkey solutions through the Commercial Marketplace or through a private service catalog directly to customers.

AZURE MANAGED APPLICATIONS OFFER SEVERAL BENEFITS:

- New revenue opportunities by creating new business models and driving incremental revenue through partner solutions.
- Enhanced control apps provides customers visibility but limited administrative access.
- Stronger customer relationships when turnkey simplicity is provided, and partners engage in support and product feedback.

DELIVER HIGH-VALUE INTELLECTUAL PROPERTY THROUGH APIS

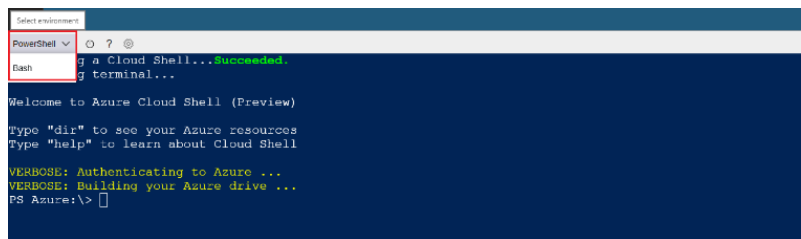
Microsoft Azure is built on a documented and well-known API that provides a common interface for interacting programmatically with Azure services. Whether through REST APIs, Azure PowerShell, the Azure CLI, or Azure Resource Manager (ARM) Templates, partners can build scripts and applications that interact with [Azure Resource Manager](#). Azure Resource Manager (ARM) enables helps deploy and manage the infrastructure for customer solutions and provides a consistent management layer for creating, updating, and deleting Azure resources. Azure Resource Manager is also the management plane that is used for role-based access control, auditing, and tagging to secure and organize resources as they are deployed or after they are deployed.

Interacting directly with the REST APIs for Azure Resource Manager requires experience with the Azure platform and development. When starting out with automating the deployment and configuration of Azure resources, Azure PowerShell and the Azure CLI, along with Azure Resource Manager Templates, can be more approachable and offer turnkey solutions across platforms. Azure PowerShell and the Azure CLI can be installed locally, or they can be run directly from [Azure Cloud Shell](#) which requires no additional installation.

Tools for enhancing solutions with IP

AZURE POWERSHELL

[Azure PowerShell](#) provides a set of cmdlets that use the [Azure Resource Manager](#) model for managing Azure resources. It can be used in the browser from [Azure Cloud Shell](#) or installed locally and used in any PowerShell session. By building a library of common PowerShell scripts, partner can build their own repository of re-usable scripts that can be used for multiple customers.

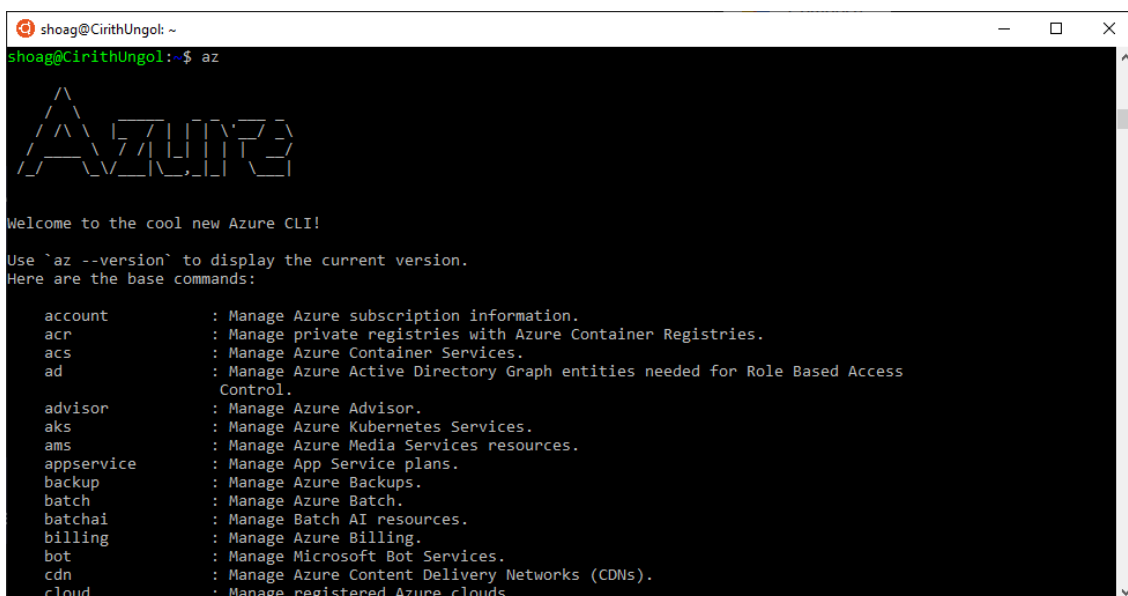


Microsoft offers a library of sample scripts which partners and customers can use to begin building a script repository:

- [Azure Virtual Machine PowerShell Samples – Linux Virtual Machines](#)
- [Azure Virtual Machine PowerShell samples – Windows Virtual Machines](#)
- [Web Apps](#)
- [SQL Databases](#)
- [Cosmos DB](#)
- [Azure-Docs-Powershell-Samples On Github](#)

AZURE CLI

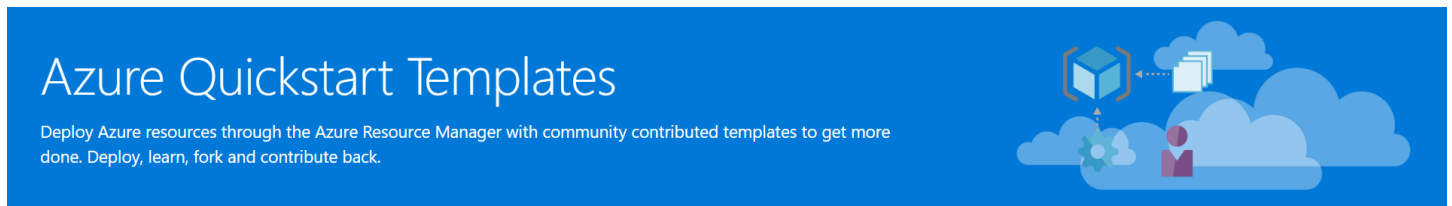
The [Azure CLI](#) 2.0 is Azure's command-line experience for managing Azure resources. It can be used from the [Azure Cloud Shell](#) or installed on Linux, MacOS, and Windows to run it locally. The Azure CLI can also be run from a [Docker container](#). Just as with Azure PowerShell, partners can build a library of common scripts that can be re-used across multiple customers.



There is an expansive library of Azure CLI samples which cover the management and configuration of multiple Azure services and resources.

- [Azure Virtual Machine Azure CLI Samples – Linux Virtual Machines](#)
- [Azure Virtual Machine Azure CLI Samples – Windows Virtual Machines](#)
- [Web Apps](#)
- [SQL Databases](#)
- [Cosmos DB](#)
- [azure-cli-samples on GitHub](#)

AZURE RESOURCE MANAGER TEMPLATES



[Azure Resource Manager templates](#) can be used to create templates (in JSON format) that define the infrastructure and configuration of Azure solutions. By using templates, partners can repeat the deployment of customer workloads throughout their lifecycle and have confidence that deployed resources are provisioned in a consistent state.

There are hundreds of community contributed templates available on GitHub in the [Azure Resource Manager QuickStart Templates repository](#). A searchable template index is maintained on Azure.com at [Azure QuickStart Templates](#).

Download these templates and fork the existing repository to begin to build a re-usable intellectual property using ARM templates.

Define vertical offerings

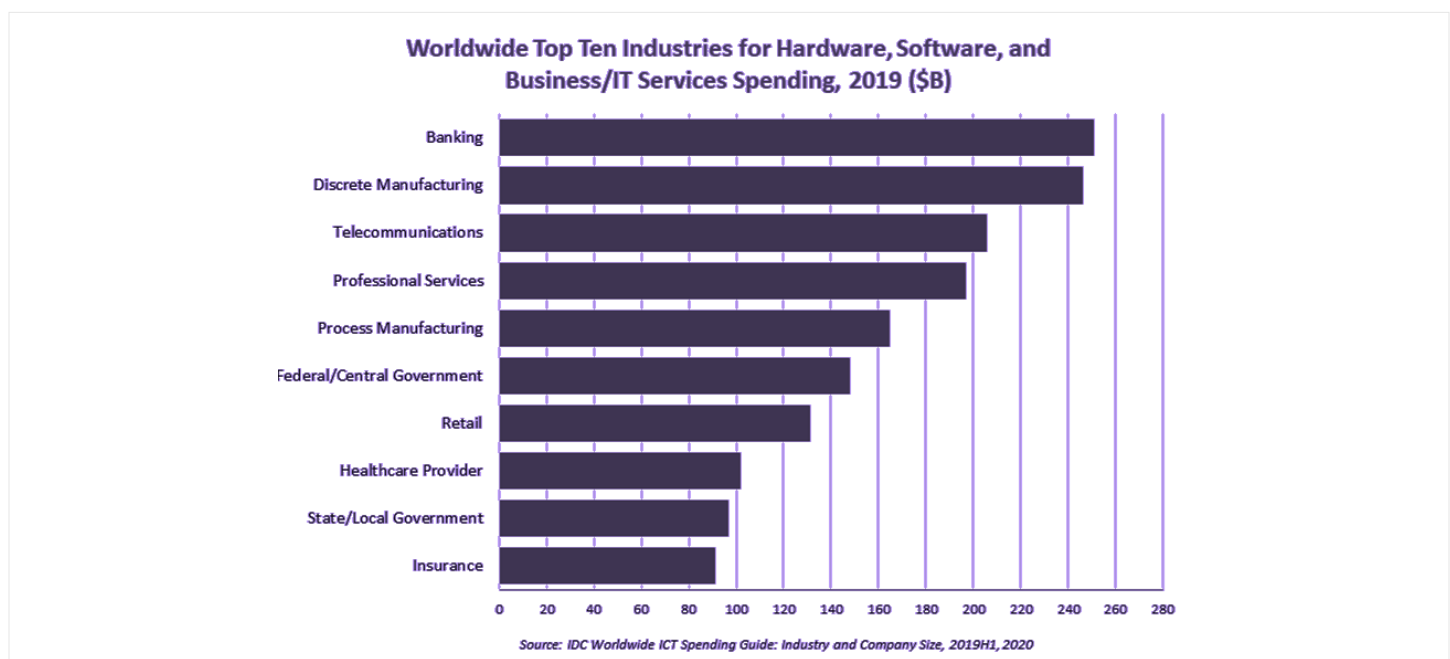
Research shows that a key best practice among top performing partners is to target industries or verticals as a part of their Go-To-Market strategy. The following are examples of these types of specialization:

- Vertical specialization: manufacturing, banking, retail, education, healthcare, government.
- Functional process specialization: accounting, human resources, marketing campaign management.
- Technology specialization: systems management, analytics, enterprise resource planning.

If there is lack of differentiation in the market, then price becomes the primary differentiator. This can erode margins and trap partners in a business they cannot afford to invest in as prices fall.

Once a primary vertical or set of verticals have been identified, it will be important to establish the practice as an expert in these selected areas. This can be achieved through the hiring of subject matter experts, attendance and participation in industry events and online forums, blogging about the chosen topic, sharing customers stories oriented to each vertical and creating content that speaks to the specific needs of customers in each vertical.

Partners also focus on a specific technology and become known as early adopters and technology leaders. But the real value comes from IP and expertise in an industry, vertical or business process. The combination of adding IP to a vertical or business process expertise makes that advantage even more powerful.



The research with partners suggests mastering one specialization before adding additional ones. It is easy to be distracted, by saying “yes” to every request, and by diversifying into too many offerings. But in the long run, it is better to say “no” to those projects that are outside the focus. Partners have shown benefit from having a strict focus on one key solution and growing by expanding one vertical at a time.

To learn more about the advantages of a vertical industry strategy, view the [Ten Steps to Getting Started on an Industry Focused Strategy](#) webinar.

Microsoft licensing options

There are several options to consider when purchasing licenses for Microsoft products and services.

Microsoft offers commitment-based and transactional options to purchase Microsoft cloud services, perpetual software, and/or Software Assurance through Microsoft-assisted, partner value-added, or self-service web options. The [Microsoft Licensing](#) site provides information on all programs including [Microsoft Azure](#), and seat-based offers such as Microsoft 365 and Dynamics 365, and ways to manage volume licenses. Several programs are highlighted below. The best way to stay up to date on the licensing options, including the rollout of the [Microsoft Customer Agreement](#), is to follow [Licensing News \(microsoft.com\)](#).

MICROSOFT CLOUD SOLUTION PROVIDER PROGRAM

Expand revenue opportunities and deliver innovative solutions to customers using our comprehensive cloud portfolio and third-party solutions from the Microsoft Commercial Marketplace. <https://partner.microsoft.com/en-us/membership/cloud-solution-provider>.

MICROSOFT SERVICES PROVIDER LICENSE AGREEMENT (SPLA)

The SPLA is for service providers and independent software vendors who want to license the latest eligible Microsoft software products to provide software services and hosted applications to their customers. For an overview of the SPLA, visit: <https://www.microsoft.com/licensing/licensing-programs/spla-program>.

MICROSOFT INDEPENDENT SOFTWARE VENDOR (ISV) ROYALTY LICENSING PROGRAM

This licensing program makes it easier for ISVs to deliver business solutions by allowing them to integrate Microsoft products into other applications and then distribute the unified solution to customers. To see how ISV Royalty Licensing works, visit: <https://www.microsoft.com/licensing/licensing-programs/isv-program>.

ENTERPRISE AGREEMENTS

This option offers the best value to organizations with 500 or more users or devices that want a manageable volume licensing program that gives them the flexibility to buy cloud services and software licenses under one agreement. For more on the benefits, visit: <https://www.microsoft.com/en-us/licensing/licensing-programs/enterprise>.

MICROSOFT PRODUCTS AND SERVICES AGREEMENT (MPSA)

This is a transactional licensing agreement for commercial, government, and academic organizations with 250 or more users/devices. For more on purchasing through an MPSA, visit: <https://www.microsoft.com/licensing/MPSA/default>.

Microsoft incentive plans and programs

MICROSOFT CLOUD ACCELERATORS

Microsoft Cloud Accelerators provide a set of pre-made workshops that enable partners to accelerate the customer journey, including a rapid deployment program to address customers' current needs for business continuity. Leveraging these accelerators enables partners to facilitate more productive customer conversations, help customers envision the possibilities, and more efficiently realize their opportunities.

Updated Cloud Accelerator website capabilities include:

- New and updated workshops focused on driving customer intent.
- Partner Center integration promote co-selling opportunities.
- Streamlined partner onboarding and payment processes.
- Optimized customer approval processing.
- Updated program dashboards and web experience.

END CUSTOMER INVESTMENT FUNDS (ECIF)

The End Customer Investment Funds (ECIF) program (formerly known as Business Investment Funds (BIF) or Customer Investment Funds (CIF)) allows Microsoft to set-aside funding in fiscal budgets to pay for services to end-customers in support of Microsoft products and solutions. ECIF may be delivered through internal services engagements (e.g. Enterprise Services, CSS, Premier) or external services engagements (provided by ECIF-approved suppliers, partners, Vendors).

<https://onefinance.microsoftcrmportals.com/knowledgebase/article/KA-01248/en-us>.

PIE

Partner investment offers support assessments, Proof of Concepts, and deployments across key Microsoft solution areas: Apps and Infrastructure, Data and AI, Modern Workplace, and Business Applications. Sign into review offers and manage funding requests. <https://mspartnerinvestments.microsoftcrmportals.com/signin>.

FASTTRACK

FastTrack helps customers deploy Microsoft cloud solutions. Customers with eligible subscriptions to Microsoft 365, Azure, or Dynamics 365 can use FastTrack at no additional cost for the life of their subscription.

<https://www.microsoft.com/fasttrack>.

AZURE MIGRATION PROGRAM (AMP)

The Azure Migration Program offers the proactive guidance and tools to set up a cloud environment, migrate infrastructure, databases, and application workloads, and move forward with confidence.

Wherever the customer is in their cloud journey, the Azure Migration Program can help accelerate progress.

All customers can access resources such as free migration tools, step-by-step technical guidance, training and help in finding a migration partner. In addition, customers may be eligible for direct support from Azure experts and offers to help with the costs of migration. <https://www.microsoft.com/azure/partners/amp>.

Calculate Azure practice costs

A practice relies on Azure services to deliver customer success, so understanding the Azure-related expenses incurred in delivering a customer solution is critical.

Using the [Azure Pricing Calculator](#) to estimate Azure costs, build an estimate online and then export it to Excel for further refinement and analysis. This tool provides the retail rates (also known as the Pay-As-You-Go option) for the Azure services, so treat it like the “high end” of any consumption estimate.

Become familiar with the discounted pricing and Azure credits:

- **Graduated pricing:** Services like Azure Blob storage have tiered pricing based upon the volume used.
- **Enterprise agreement:** By making a three-year monetary commitment, Azure services are available at a discount off retail rates. To learn more, see Enterprise Agreements.
- **Azure credits:** Microsoft Partners can receive Azure credits as a part of their benefit. For example, partners with the Silver Cloud Platform Competency receive \$350 USD per month in Azure credits; those with Gold Cloud Platform Competency receive \$600 USD per month in Azure credits.

It can be helpful to identify items that are used elastically versus items that have a fixed monthly cost. Significant savings can be achieved via elastic use of resources because they can be turned off (or paused) when they are not in use.

For example:

- **Elastic:** Azure Synapse Analytics is used only during month-end calculations. It can be paused for the rest of the month. Another example of elastic use is to leverage the auto-scale capabilities of the resource, such as auto-scaling the number of Azure App Service instances down in the evenings and back up during the workday.
- **Fixed:** Azure App Service hosting a website in a Web App. This Azure App Service needs to run 24x7 because visitors will arrive at all hours.
- If it is unclear how much of a given resource will be used, consider building a scaled-down proof-of-concept to get an initial estimate.

COST MANAGEMENT

[Cost Management](#) licensed by Cloudyn, a Microsoft subsidiary, helps make the most of Azure and other clouds by providing the tools to monitor, allocate, and optimize cloud costs and accelerate future investment with confidence.

- Monitor and visualize cloud usage and costs.
- Gain rich operational and financial insights.
- Improve organizational accountability.
- Optimize cloud efficiency.

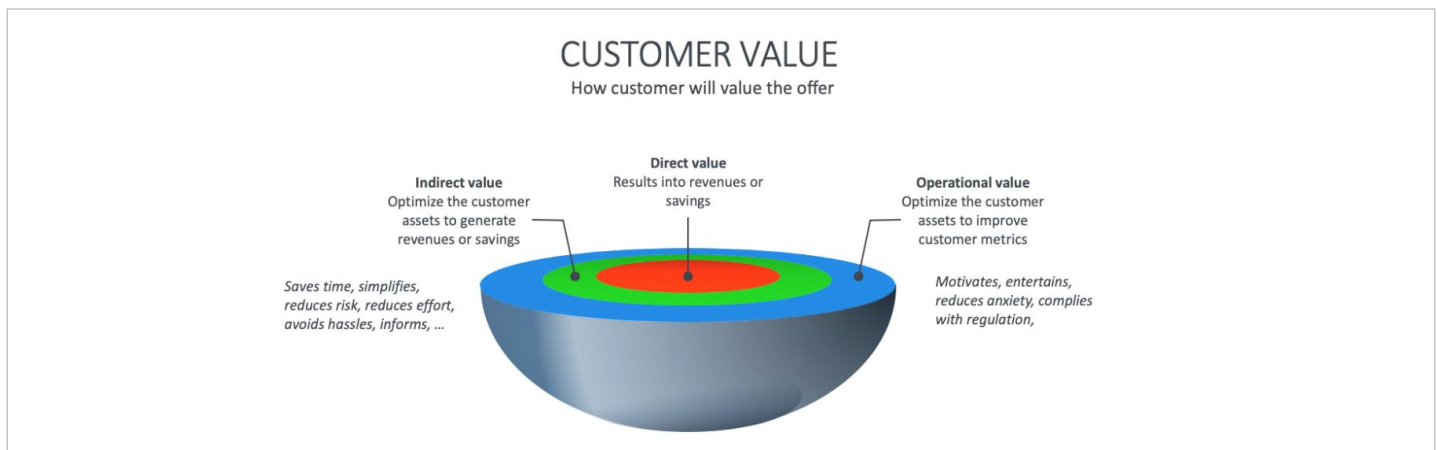
Define a pricing strategy

Pricing strategies are still evolving in the cloud era and have become very dependent upon the types of solutions being offered.

Selling cloud solutions transforms pricing models for partners looking to extend the customer lifetime value of their services. Increasingly, the price of a partner's service is based on the expected return on value for the customer and the added value that comes from being a better customer. With cloud subscription services, customers will only pay as much as the value they expect to receive from the offering, and partners who are able to determine that value can set prices that are appreciated as a good return for their customers.

The goal with value-based pricing is to make price a sales weapon that compels customers to realize more value with additional services over time. Cloud subscription offers typically carry smaller prices, paid at prescribed intervals. Each follow-on sale becomes easier, with a shorter time to decision as customers realize the value.

There are several considerations when pricing cloud offers, starting with types of value shown in the diagram for applicability with a customer's business.



The pricing models that cloud partners are using effectively are explored further in the [Pricing Guide](#), a great reference for making price part of the value proposition, something to share proudly throughout the customer journey.

Maintaining the solution

In addition to providing the customer support, maintenance and on-going feature requests should become a lucrative part of the practice.

MAINTENANCE CONTRACTS

Before any effort with the customer begins, include a maintenance contract, which defines how issues discovered within the application get fixed and how the application is kept up to date.

There are two approaches a maintenance contract can take:

- **Recurring maintenance fee:** In this approach, a maintenance contract is written to provide up to a certain number of hours of maintenance for a recurring price. For example, it might cost the customer \$4,000 per month for up to 40 hours of maintenance each month. This maintenance would be used to address either break/fix issues or could be applied to new feature requests.
- **Time and materials fee:** Alternately, the customer could have the option of paying for break/fix and new feature work on a time and materials basis. This creates new projects for each set of new work items which are billed accordingly.

In either situation, the goal is to keep a satisfied customer using the solution and both approaches provide additional revenue. However, a recurring fee model provides an increased likelihood that the fee is paid but not always fully consumed by maintenance efforts – thus increasing practice profits.

When maintenance contracts expire, companies face the risk of disruptions to their critical application services. Therefore, they are incented to ensure they receive timely notification of any pending contract expirations and respond to them accordingly. Ideally, this leads to timely renewals and perpetual fees for the practice.

Apply for Azure incentive programs

Microsoft offers several incentive programs for Azure usage. Take advantage of these programs to boost a practice.

Over recent years, Microsoft has transitioned from a company focused primarily on software licensing, to a provider of online services. This is a fundamental shift and creates new opportunities for Microsoft's partner community.

This focus on services places the Microsoft partner front-and-center in the relationship between Microsoft and its customers. The partner role has expanded far beyond reselling licenses, to helping the customer in their use of Microsoft services throughout the customer lifecycle.

The revenue model has also changed. The shift from software to services has moved revenue from one-time license sales to monthly billing. For partners, this change is reflected in new incentive programs to share these new revenue streams.

In this section, we will review the incentives Microsoft provides to partners who help drive business in Azure.

CLOUD SOLUTION PROVIDER

The primary incentive program for Managed Service Providers is the [Cloud Solution Provider \(CSP\)](#) program. This program supports not only Azure, but all Microsoft cloud services including Office365, Enterprise Mobility + Security, and Dynamics CRM Online.

The CSP program enables a partner to own the customer lifecycle and relationship for their consumption of Azure service. They set the price, bill customers directly, and directly provision and manage subscriptions. The CSP also acts as the first point of contact for customer support.

There are two CSP models: direct and indirect. It is important to understand the difference, and to choose carefully where in this ecosystem the practice will thrive.

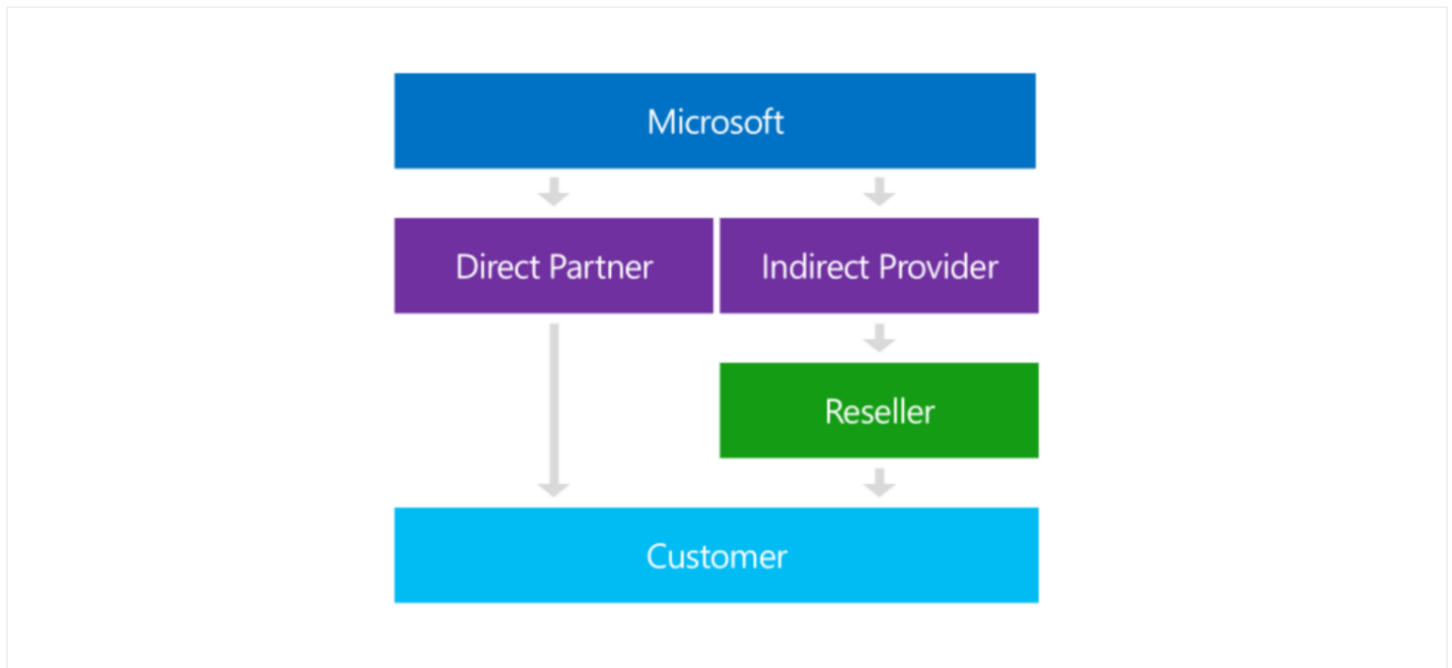
DIRECT PARTNERS

This model is designed for resellers or Managed Service Providers who have the in-house capability to bill and support their customers at scale.

In this model, partners work with both their customers and with Microsoft directly. They take on the entire customer relationship, including support, billing, and invoicing. They become a customer's only point of contact for their Azure services. This provides continuity in the customer experience and helps build strong business relationships.

Azure CSP direct partners are responsible for customer support. Microsoft does not provide support for Azure CSP customers and relies on Azure CSP partners to manage their Azure workloads and resolve technical problems.

Azure CSP direct partners are also responsible for customer pricing, billing, and invoicing. Microsoft provides partner-facing billing capabilities to Azure CSP direct partners through the Partner Center portal and APIs.



INDIRECT PROVIDERS AND RESELLERS

The Azure CSP indirect model defines two types of partners: Azure CSP indirect providers (distributors) and Azure CSP indirect resellers. Azure CSP indirect providers work with Microsoft directly, but reach customers indirectly through their partner channel—Azure CSP resellers.

Azure CSP indirect reseller is a good choice for partners who do not want to manage as much infrastructure as an Azure CSP direct partner, so they team up with an indirect provider to handle their support, billing, and invoicing needs. They still build strong relationships with the customer and get many of the benefits of the Azure CSP program, but they offload support and billing to Azure CSP indirect providers.

To learn more about the Azure CSP program, start with the [Azure CSP Overview](#).

DIGITAL PARTNER OF RECORD

In some cases, customers may prefer to use their own Azure subscriptions rather than an Azure subscription provided by partners under the CSP program. For example, the customer may be receiving discounted Azure consumption via an Enterprise Agreement.

This does not prevent partners from managing services hosted within these subscriptions, nor does it prevent them from benefiting from the Azure consumption which they help to enable.

The [Digital Partner of Record](#) program enables Microsoft partners to benefit financially from the revenue they enable for Microsoft. As with the CSP program, this program is eligible across Office 365, Dynamics CRM online, Enterprise Mobility + Security, and other online services, in addition to Azure.

For further details, and to learn how to register, see [Digital Partner of Record](#).



Hire & Train

Cloud Infrastructure



aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

The previous section looked at the various services that partners can pursue as they set up or build their cloud practice. With avenues of partner success identified, the next step is building and training a team.

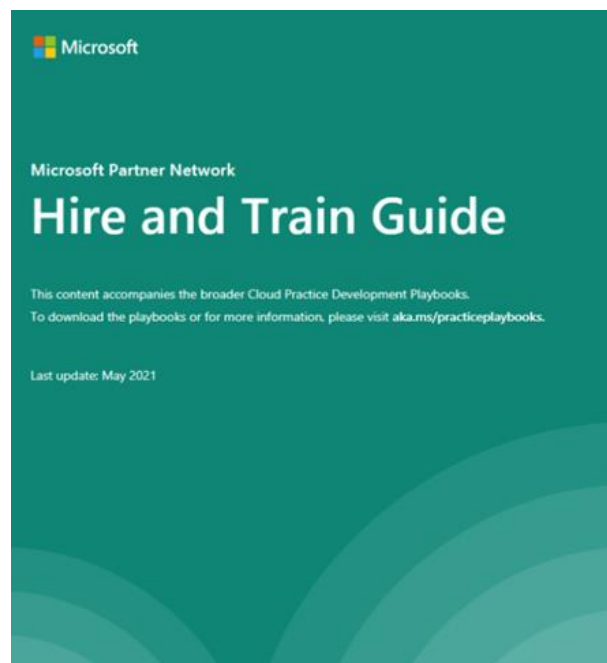
This section will offer role definitions and guidance on the skills needed for an application development-focused practice. It will cover the necessary technical, sales, and marketing training, which starts with an assessment of current skills, and a plan for filling the gaps, whether through new hires, contractors, partnering or training.

To start the hiring processes, there are detailed job descriptions, tips on where to look for resources, the factors to consider in a candidate's skillset, and what to expect to pay by role and region.

A big focus of this section is ensuring all practice resources are trained and continue to receive ongoing training.

RECRUIT, HIRE, ONBOARD, AND RETAIN TALENT PLAYBOOK AND HIRE AND TRAIN GUIDE

Leverage the Microsoft resources available in the [Recruit, Hire, Onboard, and Retain Talent playbook](#) and the [Hire and Train guide](#) for comprehensive job descriptions and to learn best practices to find the right people, grow their skills, and retain talent.

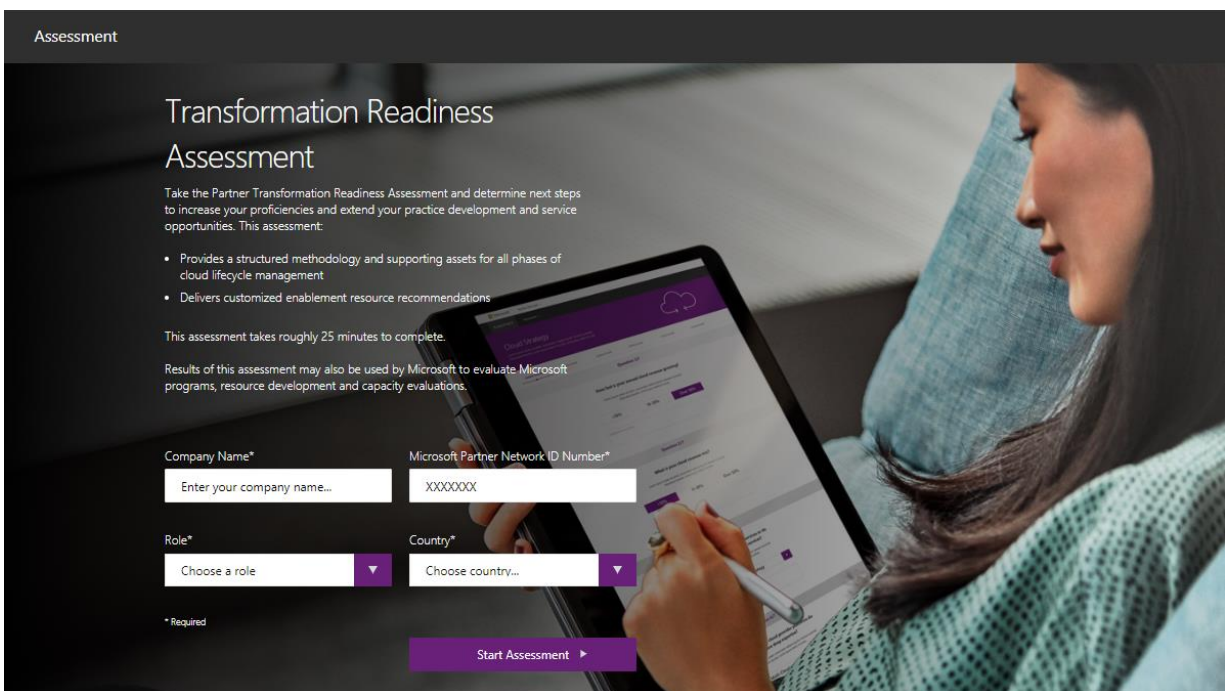


Build a team

Human resources are a critical asset to any service-based practice. Starting a new practice requires an evaluation of existing team members and then a decision of whether to hire new employees or bring the existing team up to speed.

When building a new practice, partners evaluate the solutions and services to offer, identify some avenues of success, and form and train the team to pursue that business.

Before hiring for a practice area, it is a good idea to start with an assessment of the current skills capability to determine where to invest in new hires versus training or hiring vendors to fill any role gaps. All partners are encouraged to take the [Partner Transformation Readiness Assessment](#) when creating a hiring plan. It is a great tool for determining current business and technical capability and which areas of the practice require attention. Upon completion, partners receive a Partner Transformation Index score that shows their current cloud maturity level, and how they ranked compared with other Microsoft partners. Partners also receive recommendations on the next steps to grow their capability.



The image shows a woman in profile, looking at a tablet. The tablet screen displays the 'Transformation Readiness Assessment' form. The form has a dark header with the title 'Transformation Readiness Assessment' and a sub-header 'Assessment'. Below the title, there is a paragraph explaining the purpose of the assessment. A bulleted list highlights two key features: 'Provides a structured methodology and supporting assets for all phases of cloud lifecycle management' and 'Delivers customized enablement resource recommendations'. It also states that the assessment takes roughly 25 minutes to complete and that its results can be used by Microsoft for various evaluations. The form includes input fields for 'Company Name*' (with a placeholder 'Enter your company name...'), 'Microsoft Partner Network ID Number*' (with a placeholder 'XXXXXXXX'), 'Role*' (a dropdown menu with 'Choose a role'), and 'Country*' (a dropdown menu with 'Choose country...'). A small asterisk indicates that these fields are required. At the bottom, there is a purple button labeled 'Start Assessment' with a right-pointing arrow.

Successful practices begin putting the right people in the right roles. This guide will help define the members of the team and the skills they should bring to the table. When hiring to fill gaps, find detailed job descriptions, as well as ideas on where to look for resources, and the factors to look for in a candidate's skill set. A big focus of this section is ensuring ongoing training. It covers not just technical training, but also sales and marketing training.

PARTNER SKILLSETS

Referrals and LinkedIn are top sources for identifying skilled labor. Once a candidate is identified, work history, cultural fit, and years of experience become the important considerations.

Depending on the type of practice, the amount of experience needed will vary, but most companies engage in at least annual ongoing staff learning efforts like conferences/events and online training. A median of 8.5% of technical resource time is spent on training. Role descriptions.

Management resources

Consider the following management positions if the development effort will involve eight or more technical staff. In smaller teams, senior-level employees sometimes take on management duties along with their other responsibilities.

ROLE	DESCRIPTION
Product Manager	Establishes and sustains the business case for the project and plays a key role in identifying and setting priorities across the target audience. This includes ensuring that business expectations are clearly articulated and understood by the project team and that the functional specifications respond to business priorities. This role owns the vision statement for the project. Read the full job description at https://aka.ms/productmgr .
Program Manager	Owns the specification for a solution's features and functionality and coordinates the day-to-day communication required to develop the solution effectively and consistently within organizational standards. This role has a key communication and coordination role with input from other team leads and assists Product Management in articulating the vision for the project. Read the full job description at https://aka.ms/programmgr .

Sales and marketing roles

Even the best products need a strong sales team to gain maximum market traction. Consider hiring the following sales and marketing positions for broad reach.

ROLE	DESCRIPTION
Account Executive	Proactively identifies target accounts and acquires new customers. This role accurately qualifies both self and marketing generated leads, defines the deal strategy, manages, and guides all resources supporting the sales pursuit, responsibly manages sales costs, and accurately forecasts revenue and close dates. Read the full job description at https://aka.ms/accountexec .
Business Development Representative	Manages the full sales lifecycle, from qualification through closure and renewal. This role focuses primarily on acquiring new cloud customers within designated industry verticals, leveraging repeatable sales motion. This role also works closely with marketing resources to execute demand generation programs and continuously improve and refine sales assets and artifacts. Read the full job description at https://aka.ms/bizdevrep .
Change Management Consultant	Works directly with customers to drive the people and process side of digital transformations to fully realize value for the business. This role will work with executives and business leaders in a variety of industries to drive effective change programs aligned with the business solutions. Read the full job description at https://aka.ms/changemgmt .
Content Marketer	Generates inbound leads by writing authoritative, thought-leadership content. This position is responsible for strategizing and executing content creation and delivery, tracking metrics that influence content strategy, and collaborating with both technical and subject matter specialists to produce relevant content that engages the emotions of their target audiences. Read the full job description at https://aka.ms/contentmktg .
Customer Development Representative	Responsible for upselling and cross-selling new cloud solutions to existing customers, as well as all contract renewals. This role works closely with marketing to introduce and sell "Next-

ROLE	DESCRIPTION
	Best-Offfer" waves within a designated industry vertical, through an accelerated remote sales motion. Read the full job description at https://aka.ms/customerdevrep .
Customer Success Manager	Drives successful adoption and expansion of workloads within their accounts. Primary responsibilities include developing long-term relationships within a portfolio of strategic clients, aligning customer business needs with Microsoft technology solutions, and helping customers bridge the IT/business gap. Read the full job description at https://aka.ms/customersuccessmgr .
Graphic Designer	Responsible for the creation, maintenance, and updating of visual print and digital media marketing assets to support the brand and marketing goals. This position manages all phases of the design process including concept definition, mock-up production, content review and integration, as well as the finished product. Read the full job description at https://aka.ms/graphicdesign .
Marketing Leader	Drives marketing strategy, tactics, campaigns, and programs to produce top-line results that raise brand awareness, recognition, and loyalty for the company. This position is tasked with demand generation and marketing funnel optimization using the brand, advertising, creative, digital, field, and channel marketing. Read full job description https://aka.ms/marketlead .
Pre-Sales Cloud Solutions Engineer	Supports the Account Executive, Business Development Representative, and Customer Development Representative in driving their active sales pursuits. The role reports to the Sales Leader and is responsible for facilitating both remote and onsite prospect discovery sessions, defining cloud solution fit, and working with the delivery team to develop accurate cloud solution recommendations, scope clarity, and accurate project services estimates. Read the full job description at https://aka.ms/presalesengineer .
Product Manager	Establishes and sustains the business case for the project and plays a key role in identifying and setting priorities across the target audience. This includes ensuring that business expectations are clearly articulated and understood by the project team and that the functional specifications respond to business priorities. Product Management owns the vision statement for the project. Read the full job description at https://aka.ms/productmgr .
Sales Leader	Applies expertise in selling strategies and methodologies, strategic planning, and execution to achieve defined revenue objectives. This role is responsible for creating, leading, and directing a high-performance sales team that achieves revenue, profitability, and MRR targets while consistently delivering customer value. Read the full job description at https://aka.ms/saleslead .
Solution Sales Manager	A senior leader within the enterprise sales organization that leads, develops, and manages a team of high-performing sales and technical pre-sales/post-sales resources to drive solution opportunity revenue and market share by leveraging the Microsoft cloud offerings to meet their customers' needs. Read the full job description at https://aka.ms/solutionsalesmgr .

Technical roles (architecture, infrastructure, and development)

These roles form the heart of a partner solution. Hiring the right people can turn vision into reality.

ROLE	DESCRIPTION
App Maker	Builds solutions to simplify, automate, and transform tasks and processes for themselves and their team where they have deep expertise in the solution domain. This role should be skilled in key technical business analyst tasks such as data modeling, basic UX design, requirements analysis, and process analysis. Read the full job description at https://aka.ms/appmaker .
Automation Engineer	Automates the development and deployment activities. This candidate must be familiar with DevOps tools such as Jenkins, Puppet, Ansible, Redgate, Azure ARM Templates, Azure DevOps, and many more. The ideal candidate should have the skills to implement and support the development activities via Continuous Integration (CI), and Continuous Deployment and Delivery (CD) methods. This role is very skilled at setting up rigorous testing mechanisms to ensure high-quality automated releases are delivered to customers. Read the full job description at https://aka.ms/automationeng .
Cloud Administrator	Manages cloud tenants, interfaces with the support engineers and the cloud provider support, deploys cloud applications based on deployment templates and DevOps processes, and has deep technical knowledge of the various cloud technologies (Networking, IaaS, PaaS, Security). Read the full job description at https://aka.ms/cloudadmin .
Cloud Architect	Drives customer initiatives in collaboration with customers. This role is a technical, customer-facing role that is accountable for the end-to-end customer cloud deployment experience. This role owns technical customer engagement, including architectural design sessions, specific implementation projects, and/or proof of concepts. Read the full job description at https://aka.ms/cloudarchitect .
Cloud Developer	Writes secure, scalable, and robust code that uses the platform as a service component to build new or modernize existing applications. This role should be well versed in new capabilities to take advantage of services not available on-premises. Additionally, this role should also be familiar with automated build tools as well as continuous integration methodologies. Read the full job description at https://aka.ms/clouddeveloper .
Cloud Infrastructure Engineer	Delivers technical solutions and support to customers allowing them to maximize their investment in cloud technology. The ideal candidate will have experience in customer-facing roles and success implementing cloud-based solutions, migrating workloads to the cloud, and experience with connecting and managing hybrid cloud environments. Read the full job description at https://aka.ms/cloudinfraeng .
Compliance Officer (Data Protection Officer)	Ensures that data is kept safe and secured throughout all technology solutions. This role works with internal and external data processors to ensure that legal regulations are followed. This role works with legal bodies and the internal and external legal teams when litigations via lawsuits are involved. This role will also work hand in hand with Security Architects and Analysts to discover, remediate and resolve compliance issues and unauthorized data breaches. Read the full job description at https://aka.ms/compofficer .

ROLE	DESCRIPTION
Data Analyst	Responsible for querying data sources using tools like Excel (PowerPivot, Power Query, Power Map), PowerBI, and other reporting tools such as Tableau, SAS, and Teradata. This role should be familiar with data catalogs, caching strategies, analytic data streaming, and how to build and validate data metrics from their queries. Read the full job description at https://aka.ms/dataanalysts .
Data Architect	Drives customer initiatives to solve the biggest and most complex data challenges leveraging data and analytics services, ranging from SQL Server to SQL Database and SQL Data Warehouse to Cortana Intelligence Suite. This role is a technical, customer-facing role, accountable for the end-to-end customer deployment and usage experience for data services. Read the full job description at https://aka.ms/datarchitect .
Data Developer	Responsible for helping to select and implement the tools and processes required of a data processing pipeline in support of customer requirements. This role may be a customer-facing role, but the primary responsibilities include implementing ETL (extract, transform and load) pipelines, monitoring/maintaining data pipeline performance, and implementing big data or advanced analytics solutions. Read the full job description at https://aka.ms/datadeveloper .
Data Engineer	Responsible for helping to select and implement the tools and processes required of a data processing pipeline in support of customer requirements. This role may be a customer facing role, but the primary responsibilities include implementing ETL (extract, transform, and load) pipelines, monitoring/maintaining data pipeline performance. Read the full job description at https://aka.ms/dataengineer .
Data Scientist	Responsible for identifying the opportunities present in the customer's data and helping shape the data pipeline to deliver insights by applying advanced analytics (e.g., machine learning) in collaboration with the customer. This role is a technical, customer-facing role that, along with the Data Engineer, is accountable for the end-to-end data pipeline envisioning and development. Read the full job description at https://aka.ms/datasci .
DevOps Engineer	This role includes a mix of infrastructure and developer skills. This individual will author automation artifacts such as templates and scripts and work with software build pipelines that support Azure services and infrastructure deployments. They may also function as reliability engineers, working with development and infrastructure teams to help engineer scalable, resilient, and reliable systems hosted in Azure. Read the full job description at https://aka.ms/devopseng .
Electronics Hardware Engineer	This is a key role in developing IoT hardware, including the design of circuit boards for sensors and devices. This position is responsible for researching and developing electronics hardware designs incorporating embedded microcontrollers, physical sensors, wireless data communication, and other required components for a variety of smart, robust, and reliable commercial and industrial products. Read the full job description at https://aka.ms/hardwareeng .
Functional Consultant	Configures and implements the system. This candidate is not necessarily an expert on industry processes but is deeply knowledgeable on the technical aspects of solution implementation. This role is typically trained from graduate or industry hires and experience ranges from 6 months to 10 years. The technical consultant requires deep product training and should be skilled at the subsequent lifecycle management required to ensure continued use of the service. Read the full job description at https://aka.ms/functionalconsultant .

ROLE	DESCRIPTION
Identity Solutions Engineer	Responsible for securing organizational identities. This includes integration with internal and external applications. This role is responsible for configuring trusts and federation and understanding the various standard authentication protocols like OpenID and OAuth. This role is also responsible for what and how profile information is exposed to applications. Read the full job description at https://aka.ms/idsolutioneng .
Mobility Solution Engineer	Responsible for the design, implementation, integration, support, and monitoring of enterprise mobility solutions. The candidate must have prior experience formulating, planning, and implementing a mobile strategy, including formulating policies for the "bring your own device" (BYOD) policy and remote access. Read the full job description at https://aka.ms/mobsolutioneng .
Product Designer	Works at the intersection of hardware and software, actively supporting the user experience (UX) for hardware components, including setup and configuration, device interface, device cosmetics, and product packaging. This position will engage deeply with new hardware programs and with new features being developed. The person in this role should have a strong understanding of design thinking, human-centered design, and human/computer interaction, and be fluent in the latest technology trends. Read the full job description at https://aka.ms/productdesigner .
Quality Assurance/Test Technician	The primary goal of this role is to help avoid defects in the final product or solution. This role will be involved throughout the development process to problem solve and identify technical, procedural, and usability concerns. This role will also coordinate with technical and management teams to ensure that the correct measures are put into place to align the final product with the initial goal. Read the full job description at https://aka.ms/testtechnician .
Security Analyst (Information Security Analyst)	Assess and provide security advice on cloud infrastructure, including network, service, and application components. This role conducts risk assessments, architectural reviews, provides cybersecurity subject matter expertise, and assists in the building and design of secure solutions. Additional duties may include network and application penetration testing, support for cybersecurity investigations, and on-call responses to cybersecurity incidents. Read the full job description at https://aka.ms/security-analyst .
Security Architect	The first line of defense in the prevention of hackers, malware, viruses, and other malicious activities. This role is responsible for setting up policies, procedures, guidelines for system access, and ensuring that SIEM systems are monitoring all business-critical applications. This role will interact with the Compliance Officer and Legal team to provide technical guidance on security incidents. Read the full job description at https://aka.ms/secarchitect .
Services Delivery Manager	Accountable for service delivery to one or more customers and is the primary contact for the customers they manage that consume resources. This role will manage and communicate service descriptions and service level agreements to customers, as well as monitor service levels and costs across one or more clients and ensure those costs are clearly communicated. This role will also function as the primary contact point for non-technical or non-standard requests from customers. Read the full job description at https://aka.ms/servicedelivery .
Site Reliability Manager	Responsible for improving the reliability of solutions across the stack. This role will follow a problem from start to finish and provide the expertise to not only identify the root cause of an issue but also fix it. This role will also participate in the full incident management lifecycle, including escalation, debugging, communication of resolution, and problem management. Read the full job description at https://aka.ms/reliableeng .

ROLE	DESCRIPTION
Software Developer	Designs and builds applications that solve today's business needs. To remain effective, this person must be willing to stay up to date with the fast-moving cloud services landscape including IaaS, SaaS, and PaaS designs. The developer should understand the aspects of the software development cycle, from architecture to testing. This person designs, builds, and maintains efficient, reusable, and reliable code and should have experience with projects using agile methodologies, such as Scrum. Read the full job description at https://aka.ms/softwaredev .
Solution Architect	Drives customer initiatives in collaboration with customers and participates in both pre- and post-sales (e.g., deployment) efforts. This role is a technical, customer-facing role that is accountable for the end-to-end customer cloud deployment experience. Also, this role owns the Azure technical customer engagement, including architectural design sessions, specific implementation projects and/or proofs-of-concept, and deployment. Read the full job description at https://aka.ms/solutionarch .

Support resources

A lot of effort goes on behind the scenes, or in positions that involve post-sales customer engagement. To ensure long-term success, consider hiring some of these support roles.

ROLE	DESCRIPTION
Cloud Support Engineer	Assists both internal and external customers who are having technical issues with the product or who need help to realize the full benefit of the solution to help them deliver their cloud-based workloads. Training this role on both the product and the infrastructure on which it is built is paramount to their success, and ultimately, the customers' satisfaction. Read the full job description at https://aka.ms/supporteng .
Customer Success Manager	Drives successful adoption and expansion of workloads within their accounts. Primary responsibilities include developing long-term relationships within a portfolio of strategic clients, aligning customer business needs with Microsoft technology solutions, and helping customers bridge the IT/business gap. Read the full job description at https://aka.ms/customersuccessmgr .
Support Specialist	Assists customers who are having technical issues with the product, or who need help to realize the full benefit of the solution in delivering their cloud-based workloads. They will likely be able to help customers navigate the operational challenges of cloud computing, so thoroughly training them in both products and the infrastructure is paramount to their success, and ultimately, customers' satisfaction. Read the full job description at https://aka.ms/supportspecialist .

Recruiting resources

Top 10 sources to find skilled labor and what to look for.

Sourcing skilled labor can be a challenge. In the Microsoft Hiring and Onboarding Playbook Study, referrals (68%), LinkedIn (60%) and website (55%) were reported as the top approaches for generating leads.

TOP CANDIDATE LEAD SOURCES	TOTAL (n=520)
Referrals from employees or partnerships	68%
LinkedIn	60%
Posting on website	55%
Social media	45%
External recruiting vendor	39%
University recruiting	33%
Former employees	28%
Local technical communities	26%
Recruit from competitors	17%
Meetups	14%

Source: Microsoft Hiring and Onboarding Playbook Study, MDC Research, July 2020

With an understanding of where to look, what are the most important factors to look for in a potential hire's skillset? In the Microsoft Hiring and Onboarding Playbook Study, work history remains the most important consideration for new hires.

	TOTAL (n=472)	SMB (n=257)	ENTERPRISE (n=206)
Work history	71%	71%	71%
Cultural fit	43%	37%	49%
Years of experience	39%	41%	37%
Referrals	31%	30%	33%
Professional certifications	28%	24%	33%
Professional training received	18%	18%	18%
Contract to hire or other means to test skills "hands-on"	17%	22%	12%
Reputation through community	13%	13%	14%
Formal education	12%	12%	12%
Publications	3%	4%	2%
Awards received	2%	2%	3%
Other	3%	4%	2%

Source: Cloud Application Development and Modernization Playbook Survey, MDC Research, May 2020

Training and readiness

Preparing and training technical staff

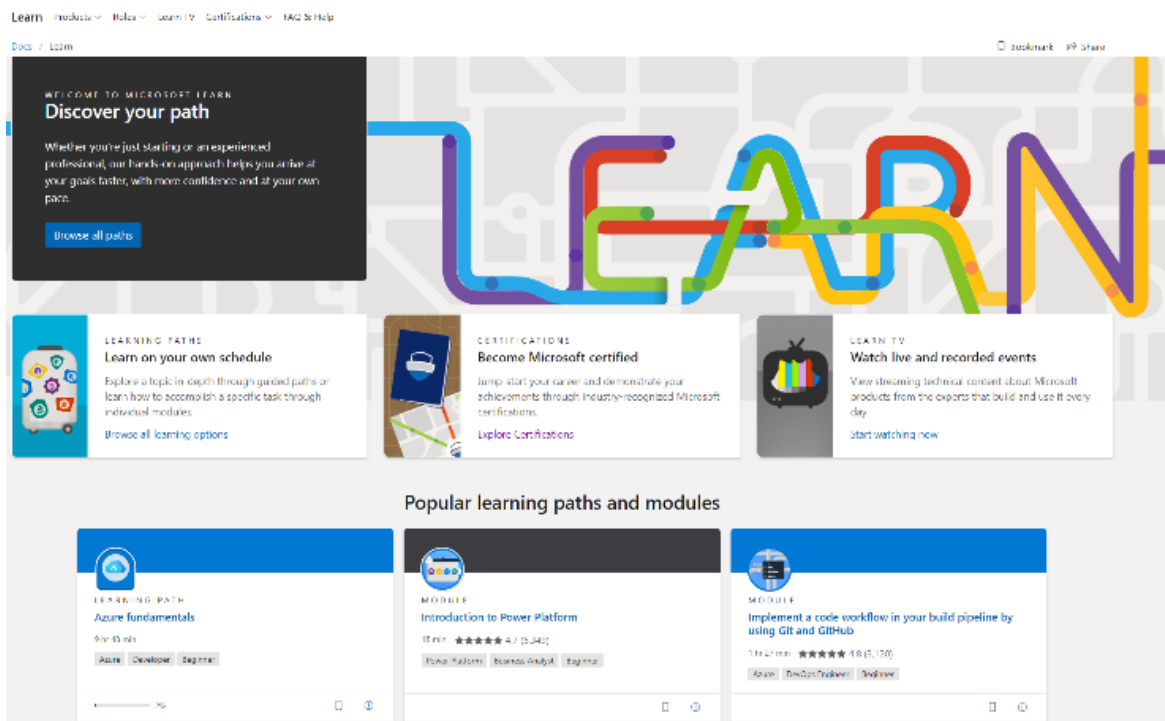
Whether filling a skills gap or looking to improve the team's skill surface area, technical training is critical to partner success.

For technical staff to function as change agents supporting current and emerging cloud technologies, their buy-in for the use and integration of these technologies is needed. For this, the staff need three things:

- An understanding of their roles and any changes to their current position.
- Time and resources to explore the technologies.
- An understanding of the business case for the technologies.

Use the following resources as part of the training for new and existing staff:

[Microsoft Learn](#) offers a wide variety of official curriculum, on-demand, that offers learners hands-on experience with a broad reach of Microsoft technologies, including Microsoft certification preparation courses.



[Learn TV](#) offers guidance on how to build solutions and use Microsoft products from the experts that built them as well as updates on the latest announcements, features, and products from Microsoft.

[The Microsoft Partner Network \(MPN\) Partner Training Center](#) provides a centralized interface with in-person, virtual, and online training opportunities and certification options organized by products, competencies, certifications, and job role.

[Virtual Training Series](#) provides chat-based webinars featuring instructors who deliver targeted information in a consolidated time frame to enhance technical skills for core technical scenarios.

Recommended Learning Paths

Use the filter to select solution or product and skill level.


Filter

Clear all

Role (1)

- ☒ Administrator
- ☐ Architect
- ☐ Business Decision Maker
- ☐ Business Analyst
- ☐ Data Scientist
- ☐ Engineer
- ☐ Functional Consultant
- ☐ Developer
- ☐ Generalist Seller
- ☐ Marketing


Showing 1-9 of 51 Learning Paths



Featured training for exam MS-203

Intermediate - 3 modules - 4 hrs 55 min


2020-06-22



Featured training for exam MS-300

Intermediate - 7 modules - 9 hrs 44 min

2020-06-03



Featured training for exam MS-301

Intermediate - 6 modules - 8 hrs 30 min

2020-06-01

[Partner Technical Presales and Deployment consultations](#) provide 1:1 pre-deployment guidance and developer assistance from Microsoft technical consultants to help ensure a successful implementation for their team.

[Microsoft Learning Partners](#) are available worldwide to help train partners via live instructor-led training. This can be scheduled as a dedicated delivery at a partner's location or virtually using remote learning technologies. Many courses are scheduled as open-enrollment courses, which do not require a dedicated class.

[Pluralsight](#) is a key Microsoft partner that offers Azure training. Gain the know-how and confidence the job demands through these free online courses, delivered in partnership with Pluralsight.

Marketing training

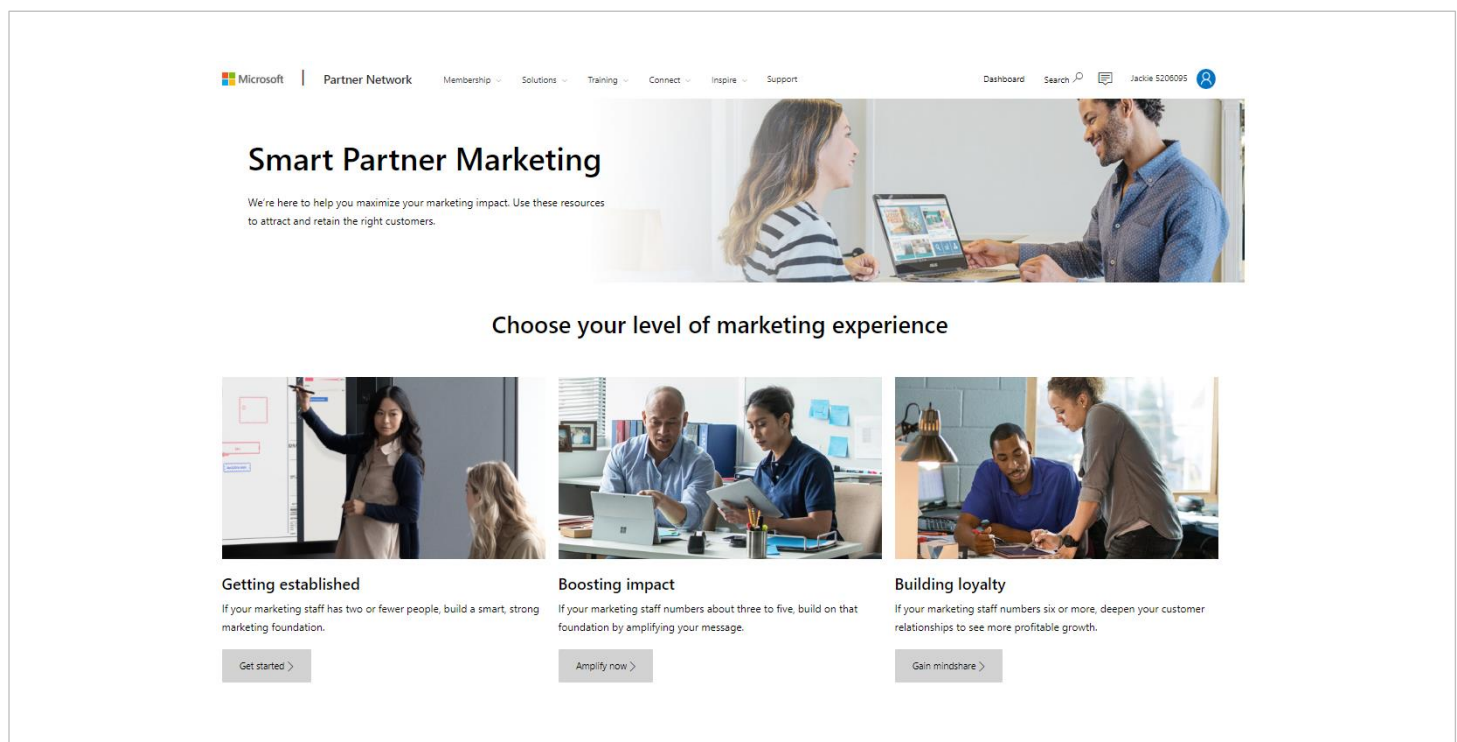
Learn how successful partners attract and retain customers and maximize their marketing impact with the guidance and resources available on the [Smart Partner Marketing](#) site. Depending on the size and skill level of the marketing staff, partners can choose from foundational marketing activities to deeper, customer relationship building programs to gain mindshare.

RESOURCES:

[Video: Understanding the Cloud Buyer](#)

[Smart Partner Marketing Resources](#)

[Digital Marketing Content On-demand](#)




Microsoft | Partner Network | Membership | Solutions | Training | Connect | Inspire | Support | Dashboard | Search | Jackie S208095

Smart Partner Marketing

We're here to help you maximize your marketing impact. Use these resources to attract and retain the right customers.


Choose your level of marketing experience



Getting established

If your marketing staff has two or fewer people, build a smart, strong marketing foundation.


[Get started >](#)



Boosting impact

If your marketing staff numbers about three to five, build on that foundation by amplifying your message.

[Amplify now >](#)




Building loyalty

If your marketing staff numbers six or more, deepen your customer relationships to see more profitable growth.

[Gain mindshare >](#)

Business development training

Successful cloud partners focus on customer lifetime value. To underscore how marketing tactics are changing for cloud buyers, Neural Impact has produced a collection of seven [cloud business development videos](#) covering the fundamentals of building a profitable cloud practice. Learn how partners make the shift from project to subscription revenue and begin to specialize and scale their practices.



Cloud business development videos

Watch a collection of videos that outline the fundamentals of building a more profitable cloud practice by Mark Stuyt, Chief Engagement Officer, and Sharka Chobot, Chief Transformation Officer, of Neural Impact.

[Watch the videos >](#)

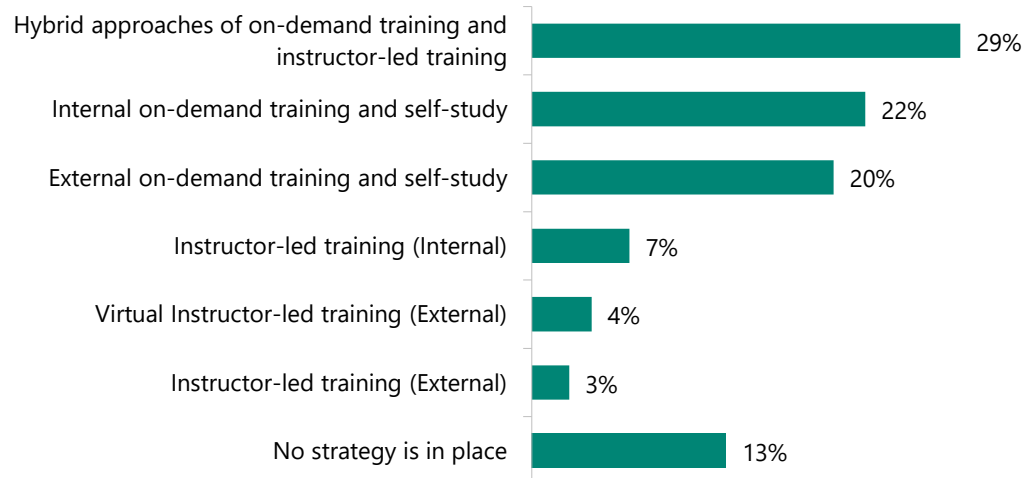
Start with the [Build a Practice](#) page on the Microsoft Partner Network and be sure to take the [Partner Transformation Readiness Assessment](#) to understand current business and technical capabilities. The assessment will recommend next steps and resources to help increase digital capabilities and expand service opportunities.

For more specific guidance on building and optimizing a practice for each Microsoft solution area, see the [Practice Development Playbooks](#), written by partners, for partners.

Survey Data

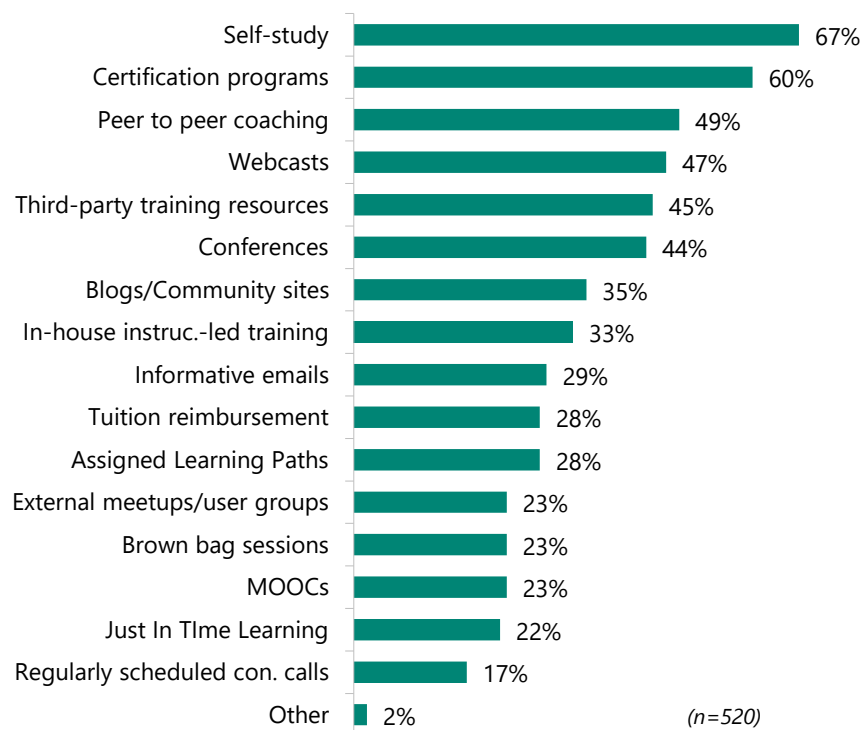
74% of respondents do not have a formal training department but allocate some work hours to employee training.

Technical Staff Training Strategy (on Cloud Technologies)



Hybrid self-study and certification programs are the most common learning processes used.

Learning Processes Used



Source: Microsoft Hiring and Onboarding Playbook Study, MDC Research, June 2018

Certifications










Increase readiness and marketability with Microsoft role-based certifications.

Certifications offer a professional edge by providing globally recognized, industry endorsed, evidence of skills mastery. Partners can demonstrate their cloud application development abilities and technical team members can set themselves up for career advancement. Team members can showcase their team's technical achievements with [certification badges](#), which are digital representations of their achievements consisting of an image and metadata uniquely linked to each team member.

MICROSOFT LEARN

Microsoft Certifications

Earn certifications that show you are keeping pace with today's technical roles and requirements. Select a job role to discover certification paths. [Go to Certification Dashboard](#)

 Developer Developers design, build, test, and maintain cloud solutions.	 Administrator Administrators implement, monitor, and maintain Microsoft solutions.	 Solutions Architect Solutions Architects have expertise in compute, network, storage, security.
 Data Engineer Data Engineers design and implement the management, monitoring, security, and privacy of data using the full stack of data services.	 Data Scientist Data Scientists apply machine learning techniques to train, evaluate, and deploy models that solve business problems.	 AI Engineer AI Engineers use Cognitive Services, Machine Learning, and Knowledge Mining to architect and implement Microsoft AI solutions.
 DevOps Engineer DevOps Engineers combine people, process, and technologies to continuously deliver valuable products and services that meet end user needs and business objectives.	 Security Engineer Security Engineers implement security controls and threat protection, manage identity and access, and protect data, applications, and networks.	 Functional Consultant Functional Consultants leverage Microsoft Dynamics 365 and Microsoft Power Platform to anticipate and plan for customer needs.

There are numerous certifications to consider as motivation for advancing technical skills, creating proof points for expertise, and achieving [Microsoft Partner Network Competencies](#). Competencies help partners highlight their expertise in several areas of cloud app development. For more on Microsoft competencies, see the [Go-To-Market and Close Deals Guide](#).



Operationalize

Cloud Infrastructure



aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

This section covers the steps to operationalize the business plan and engage with customers.

It starts with building the solution delivery process, and the tools and systems to support that process, from customer relationship management to building a customer support program and processes. Learn how to deepen relationships with customers by packaging intellectual property with custom software, creating a new revenue stream for the business.

It covers the Microsoft-provided support options, partner advisory hours, Azure Security Center, support ticket tracking, and publishing a partner offer in the Azure Marketplace.

The section concludes with checklists and templates to use to standardize the customer engagement process.

Operationalize guide

Leverage the Microsoft resources available in the [Operationalize guide](#), for details on preparing for launch with systems, tools, and processes in place. The guide contains the following additional sections:

LEVERAGE INTERNAL USE BENEFITS

Internal use benefits provide complimentary software licenses and subscriptions for use within a partner organization and resell it as well as part of an overall package along with custom software, creating a new revenue stream for the business.

PREPARE KEY CONTRACTS

Support the sales and marketing efforts with guidance on how to operate the business, from how to build materials to support the sales and marketing efforts to the key contracts to put in place.

SET UP SUPPORT PROCESSES AND SYSTEMS

Implement tools and systems with this guidance. Whether building products, providing managed services, or performing project work for customers, partner success may be impacted by the ability to manage customer records, projects, and trouble tickets.

SET UP SOCIAL OFFERINGS

Increase visibility for a practice by reviewing the Microsoft marketplaces, how to get listed on them, and find guidance on the social offerings a practice should set up.

STANDARDIZE ENGAGEMENTS USING CHECKLISTS

Leverage checklists and templates to standardize the customer engagement process.

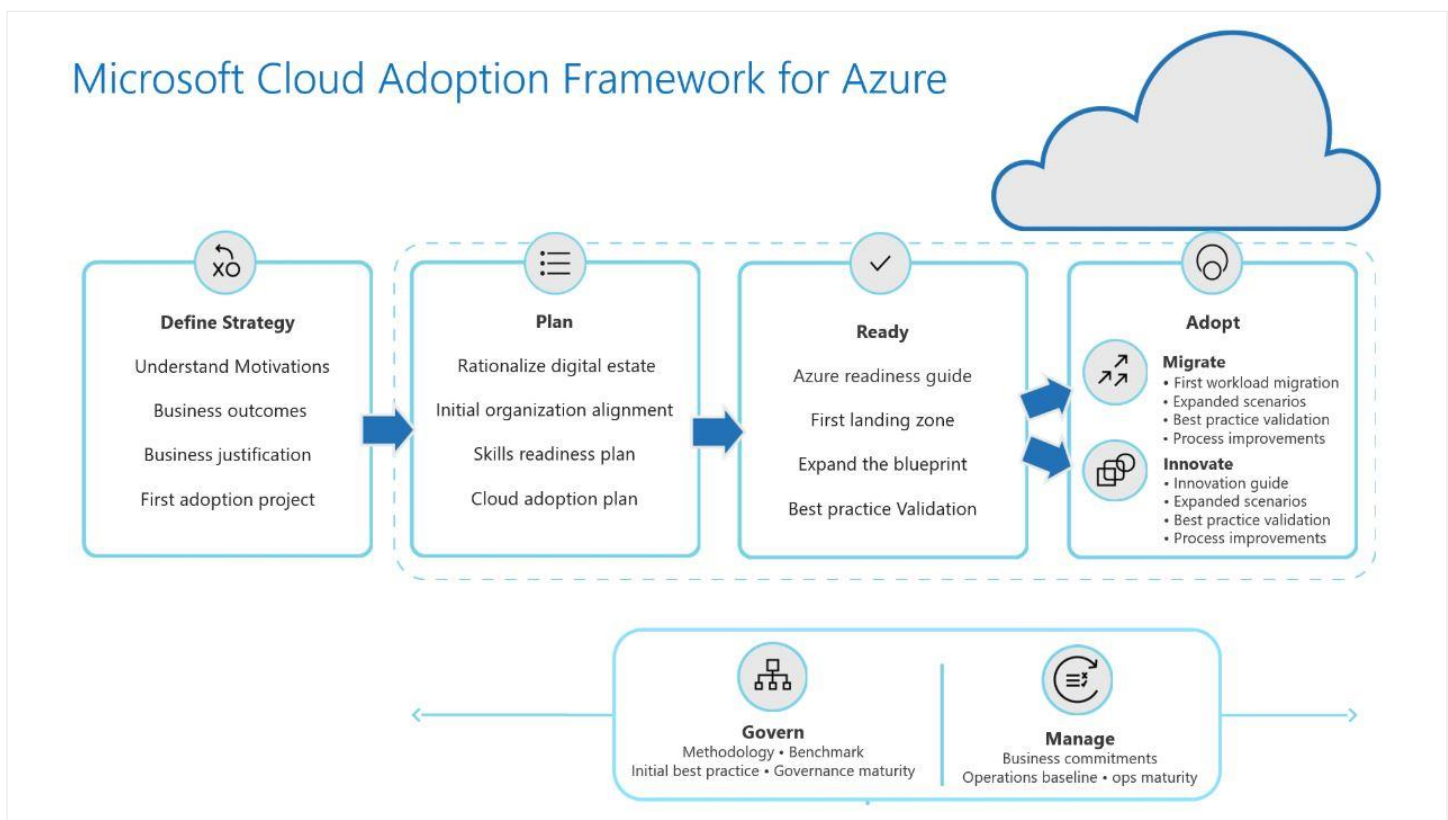
Cloud Adoption Framework for Azure

By using Cloud Adoption Framework best practices, organizations are better able to align their business and technical strategies to ensure success.

The Cloud Adoption Framework is proven guidance that is designed to help create and implement the business and technology strategies necessary for an organization to succeed in the cloud. It provides best practices, documentation, and tools that cloud architects, IT professionals, and business decision makers need to successfully achieve their short- and long-term objectives.

The Microsoft Cloud Adoption Framework for Azure provides an adoption path that works for every organization that is planning a migration and modernization journey.

The Cloud Adoption Framework for Azure provides a workflow roadmap for partners and organizations to follow as they migrate and modernize into the cloud. The Cloud Adoption Framework has six (6) methodologies to the journey: Define Strategy, Plan, Ready, Adopt, Govern, and Manage.



RESOURCES

- ➔ [Tools and Templates.](#)
- ➔ [Microsoft Cloud Adoption Framework for Azure.](#)
- ➔ [e-book about the Microsoft Cloud Adoption Framework for Azure.](#)
- ➔ [Cloud Adoption Framework for Azure Microsoft Learn module](#)
- ➔ [Learn the business value of Microsoft Azure.](#)

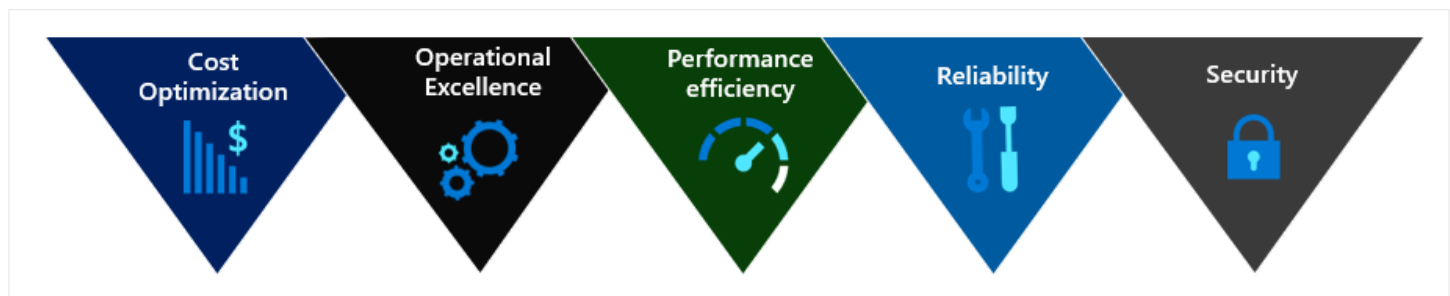
Azure Well-Architected Framework

The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architecture excellence: Cost Optimization, Operational Excellence, Performance Efficiency, Reliability, and Security.

To assess workloads using the tenets found in the Microsoft Azure Well-Architected Framework, see the [Microsoft Azure Well-Architected Review](#).

MICROSOFT AZURE WELL-ARCHITECTED FRAMEWORK

PILLAR	DESCRIPTION
Cost Optimization	Managing costs to maximize the value delivered.
Operational Excellence	Operations processes that keep a system running in production.
Performance Efficiency	The ability of a system to adapt to changes in load.
Reliability	The ability of a system to recover from failures and continue to function.
Security	Protecting applications and data from threats.



COST OPTIMIZATION

When designing a cloud solution, focus on generating incremental value early. Apply the principles of **Build-Measure-Learn**, to accelerate time to market while avoiding capital-intensive solutions. Use the pay-as-you-go strategy for the architecture, and invest in scaling out, rather than investing in a large initial version. Consider opportunity costs in the architecture, and the balance between first mover advantage versus "fast follow". Use the cost calculators to estimate the initial cost and operational costs. Finally, establish policies, budgets, and controls that set cost limits for the solution.

OPERATIONAL EXCELLENCE

This pillar covers the operations processes that keep an application running in production. Deployments must be reliable and predictable. They should be automated to reduce the chance of human error. They should be a fast and routine process, so they don't slow down the release of new features or bug fixes. It is equally important to be able to quickly roll back or roll forward if an update has problems.

PERFORMANCE EFFICIENCY

Performance efficiency is the ability of a workload to scale to meet the demands placed on it by users in an efficient manner. The main ways to achieve this are by using scaling appropriately and implementing PaaS offerings that have scaling built in.

There are two main ways that an application can scale. Vertical scaling (*scaling up*) means increasing the capacity of a resource, for example by using a larger VM size. Horizontal scaling (*scaling out*) is adding new instances of a resource, such as VMs or database replicas.

RELIABILITY

A reliable workload is one that is both resilient and available. Resiliency is the ability of the system to recover from failures and continue to function. The goal of resiliency is to return the application to a fully functioning state after a failure occurs. Availability is whether users can access workloads when they need to.

SECURITY

Think about security throughout the entire lifecycle of an application, from design and implementation to deployment and operations. The Azure platform provides protections against a variety of threats, such as network intrusion and DDoS attacks. But security still needs to be built into the applications and the DevOps processes.

Here are some broad security areas to consider.

- **Identity management:** Consider using Azure Active Directory (Azure AD) to authenticate and authorize users. Azure AD is a fully managed identity and access management service. Use it to create domains that exist purely on Azure, or integrate with on-premises Active Directory identities. Azure AD also integrates with Office365, Dynamics CRM Online, and many third-party SaaS applications. For consumer-facing applications, Azure Active Directory B2C lets users authenticate with their existing social accounts (such as Facebook, Google, or LinkedIn), or create a new user account that is managed by Azure AD.
- **Protecting the infrastructure:** Control access to the deployed Azure resources. Every Azure subscription has a [trust relationship](#) with an Azure AD tenant. Use [role-based access control](#) (RBAC) to grant users within the organization the correct permissions to Azure resources. Grant access by assigning RBAC role to users or groups at a certain scope. The scope can be a subscription, a resource group, or a single resource. [Audit](#) all changes to infrastructure.
- **Application security:** In general, the security best practices for application development still apply in the cloud. These include things like using SSL everywhere, protecting against CSRF and XSS attacks, preventing SQL injection attacks, and so on.
- Cloud applications often use managed services that have access keys. Never check these into source control. Consider storing application secrets in Azure Key Vault.
- **Data sovereignty and encryption:** Make sure that the data remains in the correct geopolitical zone when using Azure's highly available. Azure's geo-replicated storage uses the concept of a [paired region](#) in the same geopolitical region.
- Use Key Vault to safeguard cryptographic keys and secrets using keys that are protected by hardware security modules (HSMs). Many Azure storage and DB services support data encryption at rest, including [Azure Storage](#), [Azure SQL Database](#), [Azure Synapse Analytics](#), and [Cosmos DB](#).

Resources: <https://docs.microsoft.com/en-us/azure/architecture/framework>

Cloud-native architecture and design

Most of the traditional application designs and architectures that are commonplace in on-premises datacenters can run in the cloud without change. However, the cloud brings with it many new capabilities and features. Applications that make use of cloud capabilities are often referred to as “cloud-native” applications.

On the surface, designing applications for the cloud is not very different than designing for on-premises. All the same development tools, language, and frameworks can be used in the cloud. This enables all the familiar tools and existing skillsets of the development team to be used.

However, the cloud also offers a range of additional capabilities, and taking advantage of these requires some design changes. In addition, there are a wide range of cloud services and features available, and a variety of design approaches available. Cloud infrastructure partners are responsible for:

- Choosing the right cloud-native application architecture for the application.
- Incorporating proven best practices into cloud designs.
- Optimizing implementation by leveraging existing deployment templates for common architectures.

Microsoft has published extensive guidance on designing applications for the cloud. This guidance, found in the [Azure Architecture Center](#), provides a wealth of resources and proven cloud architecture best practices, based on real-world experiences gained from working directly with the largest Azure customers. This guidance is intended to accelerate the design process and ensure the designs follow proven best practices. The Architecture Center includes:

- The [Azure Application Architecture Guide](#), which presents several common architecture styles, technology choices, and design principles for Azure applications.
- [Azure reference architectures](#), which demonstrate recommended practices and include deployable solutions which can be used as the basis of deployments.
- [Azure architecture best practices](#) for a wide range of common topics, including API design and implementation, autoscaling, use of background jobs, monitoring, fault handling, and more.
- [Design review checklists](#) for [Availability](#), [Resiliency](#) and [Scalability](#), which can be used to validate and improve designs, and catch potential problems early to avoid expensive re-work later.

Enterprise-scale landing zones

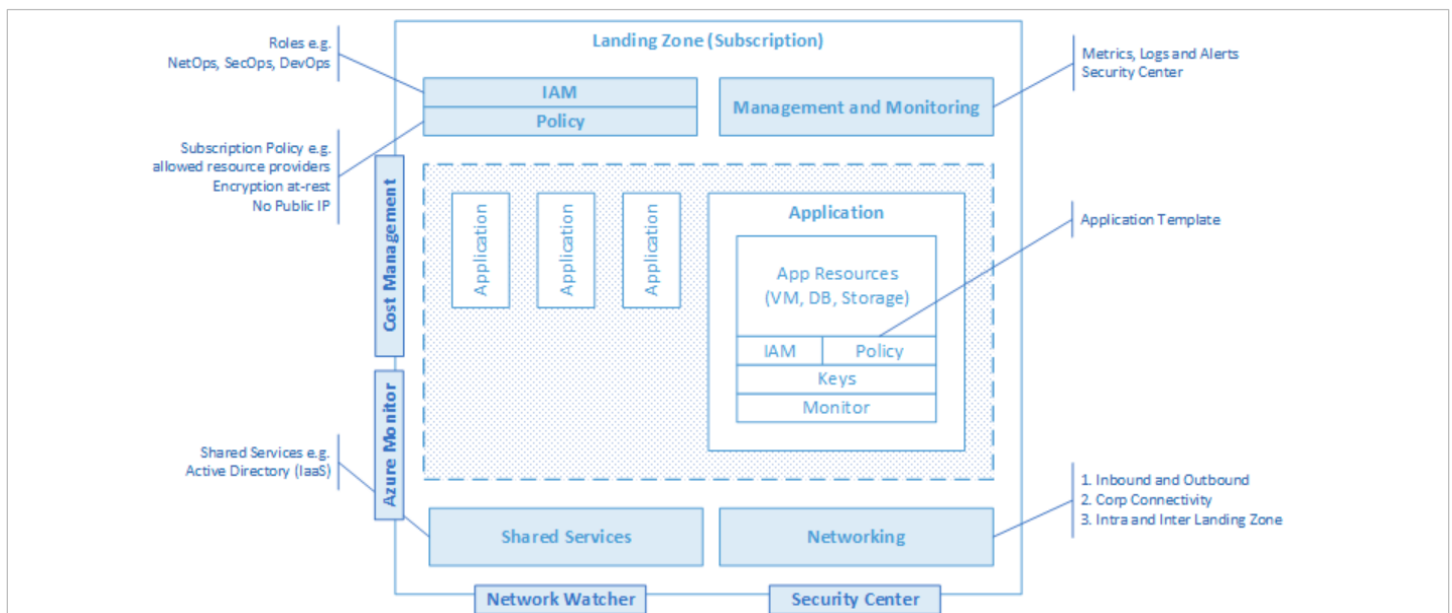
An Azure landing zone is an Azure subscription that accounts for scale, security, governance, networking, and identity. An Azure landing zone enables application migrations and cloud native application development by consider all platform resources that are required but does not differentiate between IaaS or PaaS-based applications.

What is Enterprise-Scale?

Enterprise-Scale is part of the Cloud Adoption Framework (CAF), or more specifically the Ready phase of CAF. The Enterprise-Scale architecture provides prescriptive architecture guidance coupled with Azure best practices, and it follows design principles across the critical design areas for an organization's Azure environment and landing zones. It is an architecture approach and reference implementation that enables an effective operationalization of landing zones on Azure. Enterprise-Scale is based on the success of large-scale migration projects and the architecture is based on the following five design principles:

- Subscription democratization
- Policy-driven governance
- Single control and management plane
- Application-centric and archetype neutral
- Align Azure-native design and roadmap

Furthermore, Enterprise-Scale within CAF lists many design guidelines, design considerations and recommendations. These eight design areas can help address the mismatch between on-premises data center and cloud-design infrastructure. It is not required to implement all the design recommendations, as long as the chosen cloud-design infrastructure is aligned with the five design principles.



The eight design areas are as follows:

- Enterprise Agreement (EA) enrollment and Azure Active Directory tenants
- Identity and access management
- Management group and subscription organization
- Network topology and connectivity
- Management and monitoring
- Business continuity and disaster recovery
- Security, governance, and compliance
- Platform automation and DevOps

In those design areas, topics covered are for example using Azure Active Directory Privileged Identity Management (PIM) for just in time access, Azure Virtual WAN for the global network, Azure Application Gateway and Web Application Firewall (WAF) to protect web applications, etc.

RESOURCES

- ➔ [Enterprise-Scale for Azure landing zones](#)
- ➔ [Enterprise-Scale as part of the Cloud Adoption Framework](#)
- ➔ [Enterprise-Scale design principles](#)

Choosing virtual machines

Helping customers choose the right virtual machines family and size, with the correct availability options, is an important value-add.

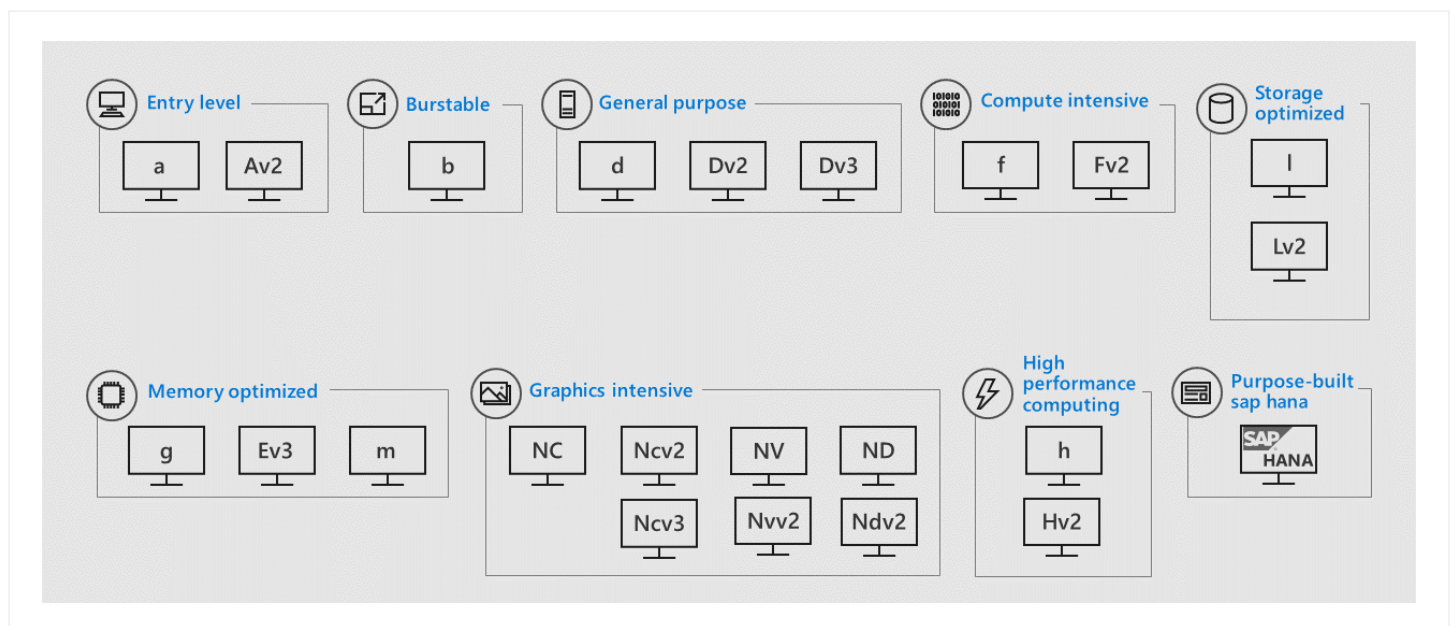
Azure supports a wide range of [virtual machine families](#), with a wide range of compute and memory capabilities. Some virtual machine families offer a balanced mix of CPU, memory, and storage, and are suitable for a wide range of general-purpose applications. Others are optimized for CPU, others for memory, and others for storage or networking, and suitable for specific, intensive workloads. There are also dedicated virtual machines for HPC workloads and for workloads that can be accelerated using additional processing power provided by an on-board graphics card.

Not every virtual machine family and size is available in every Azure region. Care should be taken when planning the deployment to ensure the desired virtual machine and region combination is available.

The family and size of each virtual machine used should be determined considering the capacity and performance requirements of the application.

Helping customers navigate the various VM compute series to ensure they are choosing the optimal size both for performance and for cost effectiveness for their workload is an incredible value add and will be critical to the success of any project.

Virtual machine costs vary significantly with virtual machine family and size. An optimal selection has the potential to enable significant cost savings. Virtual machines can be re-sized, so under-provisioning is not as much of a concern as when buying physical hardware. Users can scale up later as required or scale down if compute needs change.



Availability options

Beyond choosing the right family and size of virtual machine, choosing the right availability option is integral, as is understanding the native availability requirements for the workload (for example: SQL Server Always On). Partners plan and choose the right level of availability with Azure Virtual Machines, backed by a suitable [virtual machine availability SLA](#).

SINGLE INSTANCE VM

When any Azure virtual machine is backed by Azure Premium Storage, (for all disks), Microsoft provides a 99.9% availability SLA.

AVAILABILITY SETS

[Azure Availability Sets](#) are a logical grouping capability in Azure to ensure that the virtual machines are isolated from each other when they are deployed within an Azure datacenter.

Using availability sets helps protect against outages caused by local failures, such as a top-of-rack network switch, or by rolling system updates such as host OS patching.

Availability sets offer a 99.95% availability SLA and require that at least two virtual machines are deployed.

AVAILABILITY ZONES

[Azure Availability Zones](#) are fault-isolated locations within an Azure region, designed with independent power, cooling, and networking. They help protect mission-critical applications from failures of entire datacenters, caused by events such as power or cooling failures, fire, or flood.

Availability zones are designed to be sufficiently isolated to protect against coordinated failures, yet close enough for low network latency between zones, so that write operations to [zone-redundant storage](#) take place synchronously.

Availability zones also support zone-redundant networking. Zone-redundant load-balancers can be used to distributed traffic across virtual machine instances, both within and across Availability Zones. Zone-redundant public IP addresses enable a single public IP address to be shared across all zones, with traffic routed away from failed zones automatically.

Availability zones offer a 99.99% availability SLA. However, they are not yet supported in all Azure regions—see [Azure Regions](#) for details.

REGION PAIRS

Deploying applications to more than one Azure region helps protect against large-scale region-wide disasters (such as hurricanes) with the potential to impact all availability zones within a region. However, this comes at a significant cost—as well as the increased Azure consumption arising from the larger deployment footprint. The application design must account for data consistency between regions and traffic routing, both before and during a disaster.

Cross-region data replication can be achieved using a range of database technologies, including [Azure SQL Database](#). Cross-region traffic routing and failover is provided by [Azure Traffic Manager](#) or [Azure Front Door Service](#) which both support a variety of traffic-routing policies.

When deploying an application to more than one Azure region, take advantage of [Azure region pairs](#). Each Azure region has a 'paired' region, and Azure avoids deploying system updates to both regions at the same time. Spreading the load across paired Azure regions helps protect against unexpected outages caused by Azure system updates.

Customized virtual machine images

Many customers use virtual machine images in their existing virtualization environment complete with third-party and custom software ready for deployment. These images can be used in Azure as well, which can accelerate deployments by removing the need to change configuration settings and deploy software after the virtual machine is created.

CUSTOM IMAGES FOR WORKING TOOLS

Many partners create custom images (Windows and Linux) that contain their custom applications and third-party tools they commonly use as part of a migration or modernization project.

With this approach, they get the additional benefit of a common working environment which allows for consistent behavior and a common set of tools. New teams can get started much faster and with less confusion since all the environments have the expected set of tools and services when they start.

CREATING IMAGES

A first step should be to browse the [Azure Marketplace](#) to see if there is an existing virtual machine image that meets the needs. However, if a suitable image is not found in the Marketplace, a custom image can be created as a baseline for the virtual machines.

The easiest way to create a new image is to start by provisioning a VM from the Azure Marketplace and then customizing it by installing software and services. After the VM is configured, sysprep.exe must be run with the generalize and shutdown options selected. Once the VM is shutdown, use the Azure capture command to store the image for later use. For more information, see [Creating Custom VM Images for Windows](#) and [Linux](#).

Another option is to use the open source tool '[Packer](#)' to create custom virtual machine images. To build images, define a Packer template file specifying the build process for the image. Packer supports integration with Azure to define Azure resources such as service principal credentials. Running Packer will then deploy a virtual machine to Azure, perform the necessary build steps, create the image, and then clean up the virtual machine. This image can then be used as a baseline for more virtual machines. For more information, see [How to use Packer to create Windows virtual machine images in Azure](#) and [How to use Packer to create Linux virtual machine images in Azure](#).

UPLOADING EXISTING IMAGES

Use the Azure Command line tools or Storage Explorer to upload existing VHD files and register them as managed images that can be used to create new virtual machines in Azure.

For details, see [Migrating Disks to Azure](#).

Azure Virtual Datacenter

And the Enterprise Control Plane

Azure Virtual Datacenter (vDC) is an approach to making the most of the Azure platform's capabilities while respecting the customer's existing security and networking policies by implementing "secure-by-design" Azure deployments.

When deploying enterprise workloads to the cloud, all organizations must balance governance with service delivery and agility. Azure Virtual Datacenter provides models to achieve this balance with an emphasis on governance.

ADDRESSING CUSTOMER NEEDS

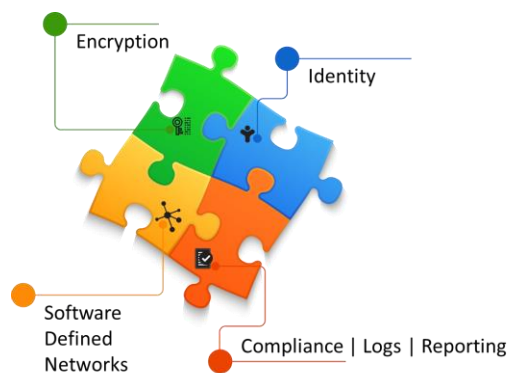
Customers look to Microsoft and its partners to reduce costs in Azure while reproducing the isolation, security policies, and audit models they have today. They also want partners to have access to mature tools for identifying workload suitability as well as the one-time deployment and ongoing operational costs of Azure.

As partners balance these needs, they also need to consider the needs of the developers who will need to do their work independently of a centralized IT organization while still adhering to organizational policies. By implementing the practices and tools of the vDC, partners can deliver services on the Azure platform to even the most sophisticated customers.

The vDC delivers:

- Tooling that automates Azure deployments that are isolated, secure, and policy driven.
- Suggested practices, tools, and models that support Azure migration decisions.
- Integration with well-known Microsoft developer tools to enable governed applications and CI/CD pipeline.
- Integration with Azure monitoring tools, including Log Analytics workspaces, Azure Security Center, and Azure Monitor.

There are four pillars that make the vDC possible: identity, encryption, software-defined networking (SDN), and compliance (including logging and reporting).



By adhering to these principles, partners can enable Azure to become a natural extension of their customers' existing environments. The components can be used to build a true virtual datacenter – fully isolated from other customers that supports the application of organization policies like security and compliance.

The remainder of this section explores the services that partners can implement to enable the vDC and the enterprise control plane for customers. Learn about deploying subscriptions, implementing identity management and role-based access controls, configuring Azure to meet compliance needs, and implementing secure deployments with encryption and software-defined networking abstractions. To learn more, see [Azure Virtual Datacenter and the Enterprise Control Plane](#).

Managing Azure subscription creation

RESOURCES

- ➔ [Licensing Azure for the Enterprise](#)
- ➔ [Enterprise Portal](#)
- ➔ [Direct Customer Onboarding Guide](#)

Subscriptions are the bedrock of the Azure Virtual Datacenter. Organizations can use subscriptions to manage costs and impose limits on the creation of resources by users, teams, projects, or using many other strategies.

Microsoft Azure Enterprise Portal

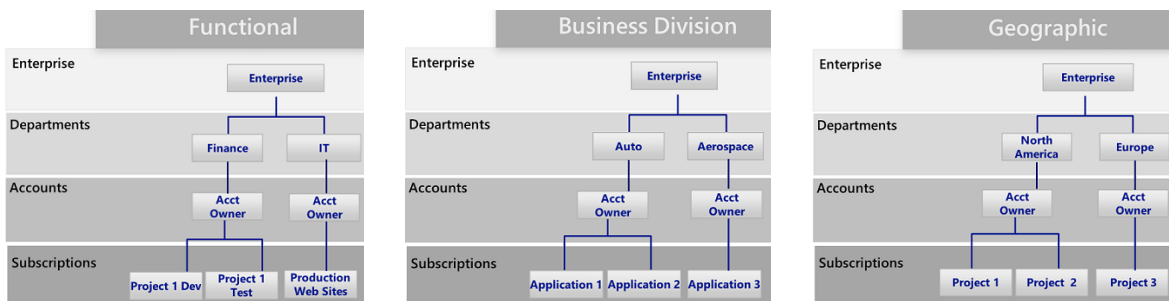
The Microsoft Azure Enterprise Portal for Enterprise Agreement customers (EA Portal) is where customers can administer the Azure subscriptions that are associated with their Enterprise Agreement, obtain billing and usage reports, and understand their current monetary commitment balance(s) and burn down. Within the portal, customers can create Account and Department Administrators. Account owners are then associated with one (or more) subscriptions where they also become the Service Administrator.

As customers setup their portal, customers divide their enrollment into Departments and Accounts, followed finally by subscriptions.



While the resources created in a given subscription are the most tangible aspects to Account and Service Administrators and managed in the [Management Portal](#), Enterprise Administrators and Department Administrators perform their tasks through the [Enterprise Portal](#). Depending on the user's role associations, they could perform management tasks in any of the three portals.

Account Owners are solely responsible for the lifecycle of a subscription, including its creation and, if needed, deletion. Subscriptions are created and managed within the hierarchy defined at the Enterprise and Department levels.



Partner Center

An Azure CSP customer must be created within Partner Center before partners place orders for a customer. When a customer is created, it also creates:

- An Azure Active Directory (Azure AD) tenant object for the customer.
- A relationship between the reseller and customer, which is used for delegated administrator privileges.
- A username and password for signing in as an administrator for the customer.

The screenshot shows the Microsoft Partner Center dashboard. The top navigation bar includes links for 'Partner with us', 'Learn more', 'Find a Partner', 'Get support', and 'Dashboard'. The left sidebar lists various sections: Dashboard, Overview, Customers, Service requests, Service health, Product analytics, Azure spending, Activity log, Billing, Pricing and offers, Promotions, Referrals, Account settings, Notification center, and Announcements.

The main content area is titled 'Azure spending'. It includes an 'Email notifications' section with a toggle switch set to 'On' and a 'Get emails' button. Below this, the 'Billing period' is shown as 'June 26 - July 25' with '20' days remaining. A section titled 'Customers with Microsoft Azure subscriptions' provides a report for 7/4/17 8:38 PM, noting that the data is an estimate and may be delayed by up to 48 hours.

Below the report, there is a 'Monthly budget' input field with 'Apply' and 'Remove budget' buttons, and a search bar. A table lists three customers with their respective budgets and current estimates:

Customer	Monthly budget	Current estimate	% used
SEATTLEIOT	\$100	\$123.39	123%
ANDREWS CONCERT TICKETS	\$1,000	\$244.11	24%
DAN INC	\$5,000	\$835.31	17%

Customers can be provisioned through the Web UI, PowerShell, C#, or the available REST API.

As the customer is created, partners can select the offers that will be provisioned for the customer. Note that there are separate offers for Enterprise, Small business, and Government. The Azure CSP offer can be found under the Enterprise category.

The initial admin user account and associated password are only available when the customer is created and the offer provisioned. Make sure to note them, especially when using the web user interface.

RESOURCES

- ➔ [Create an Azure CSP customer](#)
- ➔ [Partner Dashboard](#)
- ➔ [Azure in CSP](#)

Managing Azure subscription access

RESOURCES

- [Add an RBAC Owner admin for a subscription in the Azure portal](#)
- [Add or change Co-administrator](#)
- [Azure CSP subscription permissions management](#)

Accessing a customer's subscription and the delegation of management of a subscription is dependent on the type of subscription and how it was created.

AZURE ENTERPRISE ENROLLMENT AND PAY-AS-YOU-GO SUBSCRIPTIONS

To access a customer's existing enterprise enrollment, the customer will need to grant a partner rights within their Azure subscription. There are several ways they can accomplish this.

AZURE RESOURCE MANAGER SUBSCRIPTIONS

Azure Resource Manager (ARM) subscriptions provide support for role-based access control (RBAC) and offer fine-grained access management to the resources hosted in an Azure subscription with many built-in roles, flexible scopes, and custom roles. It is recommended that all Azure subscribers use RBAC for assessment management whenever possible, even if it requires reconfiguring existing access policies to accommodate RBAC.

Customers can following the instructions in the article at [Add an RBAC Owner admin for a subscription in the Azure portal](#) to add a partner user account to their subscription.

There may be customers who still utilize Azure Service Management (ASM) (otherwise known as Classic subscriptions). Classic subscriptions are managed through a different set of APIs and it is recommended that those customers redeploy existing resources through ARM. For customers that are still managing Classic resources, partners should consider offering services to assist those them in transitioning to the modern ARM APIs and deployment model. For more resources on Classic to Resource Manager migrations, see [Migrate from classic to Resource Manager](#).

AZURE CSP SUBSCRIPTIONS

Azure CSP subscriptions that have been created on behalf of a customer by a partner will not require additional intervention for the partner to gain access. In this case, it is the partner who must grant the customer rights to access the subscription if that the customer requires it or the partner has structured the service agreement in such a manner. The article at [Assign and manage permissions within an Azure subscription](#) contains the steps that show how this is done.

Identity and access management (IAM)

IAM Resources

Subscriptions provide the first layer of isolation in the vDC and robust role-based access controls provide the next with Azure Active Directory (Azure AD).

Azure AD manages user identities and creates intelligence-driven access policies to secure Azure resources within an Azure subscription. The roles created in Azure AD are used to control access to resources in Azure, including services, virtual machines, storage, and databases.

ROLE-BASED ACCESS CONTROL (RBAC)

Access to manage resources can be delegated to individual users, groups, service principals, and managed identities or a combination of all of them. It is important to remember that while RBAC can be used to control the access to the top-level resource, the internal configuration of a resource is not controlled through Azure AD and RBAC. For instance, access to a virtual machines' configuration in Azure can be delegated with RBAC, however the access to the underlying guest operating system is configured within the operating system itself.

Access to resources in Azure should always be explicitly granted to specific users, groups, or applications performing a function. The users and groups that are assigned to roles and resources can be created on-premises and synchronized to Azure AD with Azure AD Connect or created as cloud-only objects in Azure AD and managed exclusively in the cloud.

If a customer has existing security policies in place, including well defined security groups in an on-premises environment, they can be repurposed in Azure. By leveraging Azure AD Connect, group membership can be managed on-premises and surfaced in Azure through the application of a role assignment. This allows for a distributed approach to give customers access to specific workloads without impacting the services provided.

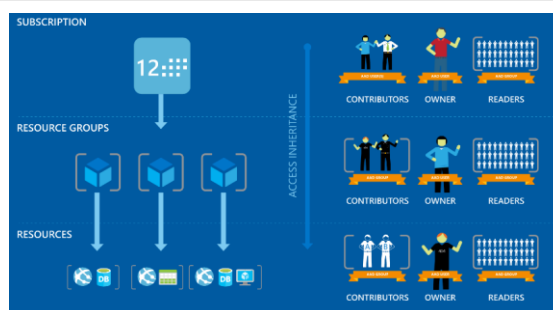
When planning roles in Azure, it is important to note that roles are comprised of two components:

- **Role definitions** describe the set of permissions allowed within a role. For instance, a role definition may include the Contributor permission to manage everything related to a resource except access to the resource.
- **Role assignments** allow users, groups, and service principals to be associated with role definitions at a scope. For instance, an application administrator can be granted Contributor rights to a resource group, allowing that user to manage all the resources within the group while the delegation of access control can remain with another group.

Also consider role-inheritance in the design of the roles. ARM provides a very granular RBAC model where management rights are assigned at a scope level. A scope is the boundary that access applies to.

There are four RBAC scopes in ARM:

- **Management group level** which grants permissions to all management groups, subscriptions, and resources under the management group where a role assignment is made.
- **Subscription level** which grants permissions to all resources in a subscription.
- **Resource group level** which grants permissions to all resources in the resource group.
- **Resource level** which grants permissions to a specific resource.



The goal should always be to follow the principals of least privileged access. By following this model, users will be able to do the tasks their job requires, but no more than that. For example, an IT operations manager may require access to read an activity log and view reports but will not need access to update the permissions for a networking component. By granting them access to only the resources they need, partners can ensure that resources are properly isolated and that the proper controls have been implemented.

BUILT-IN ROLES

Azure RBAC has many [built-in role definitions](#) that can be assigned to users, groups, and service principals. As a best practice, always try to leverage built-in roles whenever possible. There are 40-plus built-in roles today, and more are added all the time.

When considering built-in roles, there are four primary roles:

- **Owner** can perform all management operations for a resource and its child resources including access management and granting access to others.
- **Contributor** can perform all management operations for a resource including creating and deleting child resources. Contributors cannot grant access to other others.
- **Reader** has read-only access to a resource and its child resources but cannot read secrets.
- **User Access Administrator** can manage user access to resources.

Beyond the primary roles, there are more than 100 [resource-specific roles](#). These roles are permissions scoped to resources and actions that are commonly required by consumers of Azure. One example of this would be the Virtual Machine Contributor role. This role lets assignees manage virtual machines, but not the access to them or the virtual network or storage account to which they are connected.

CUSTOM ROLES

It is recommended that partners leverage the built-in roles whenever possible. When the built-in roles do not meet the needs of customers, [custom roles](#) can be created. Just as with built-in roles, custom roles can be assigned to users, groups, and service principals at the subscription, resource group, and resource scopes. Custom roles are stored in Azure AD and can be shared across subscriptions.

To create a custom role, start with a built-in role, edit it, and then finalized as a custom role. It is important to note that while using a built-in role as a template for a custom role, if that built-in role is ever updated, no updates will be made to the custom role. The more custom roles that are implemented, the more operational overhead is added to maintain them moving forward as new actions are introduced.

RESOURCE LOCKS

[Resource locks](#) are used to create policies within subscriptions which restrict operations on high-value resources where modifying them or deleting them could have a significant impact on the cloud infrastructure and applications.

Just as with roles, resource locks are applied at a subscription, resource group, or resource scope. Resource locks are commonly applied to resources related to core infrastructure such as virtual networks, gateways, storage accounts, and ExpressRoute circuits (if applicable).

Resource locks can be CanNotDelete or ReadOnly locks. CanNotDelete means that a resource can be read and/or modified by users with the appropriate access rights, but that resource cannot be deleted. A ReadOnly lock means that authorized users cannot delete or modify a resource.

When considering resource locks, the first place to look for practical application is the core networking resources. While resources like a virtual network cannot be deleted while in use, it is always helpful to have additional safeguards in place. Another strong candidate for resource locks are any recovery services vaults that contain backup items or that are providing active protection for machines with Azure Site Recovery.

ACTIVITY LOGS AND AUDIT

Even with a well-planned access management strategy in place, regular audits should be performed to ensure the integrity of subscriptions. The Azure Activity logs captures common operations related to RBAC changes and maintains the history of those operations for 90 days. For longer term retention, the Activity Log can also be sent to a Log Analytics workspace, sent to an Azure storage account, or streamed to an Azure Event Hub and exported to the preferred destination.

The entire lifecycle of RBAC is included in the Activity Log under the Administrative event category. This includes the creation and deletion of role assessments as well as the creation, updates, and deletion of custom role definitions.

The Activity Logs also capture all write operations performed the resources in a subscription. Read operations are not included in the log today. Using the activity logs, administrators can determine:

- **Who** initiated the operation (although operations initiated by a backend service do not return a user as the caller).
- **What** operations were taken on the resources in the subscription.
- **When** the operation occurred.
- The **status** of the operation.
- The **values** of other properties that might help research the operation.

The activity logs are a crucial resource for understanding the actions and operations that are occurring in the subscriptions, whether they are being used for audit controls or even basic troubleshooting.

The Activity Log can be queried through Azure Monitor and operational alerts and automation can be trigged from events that are written to the Activity Log as well. For example, for a virtual machine that always needs to be allocated, create an alert that automatically starts the VM even if another user stops the virtual machine.

AZURE POLICY

[Azure Policy](#) is a service that can be used to enforce different rules and effects over the resources in Azure subscriptions. Think of Azure Policy as a risk management and mitigation mechanism, keeping users on a defined path. Where RBAC grants access to the Azure platform, Azure Policy defines what users can do, regardless of their assigned roles, within Azure.

At the core, policies restrict, enforce, or audit certain actions within an Azure subscription. Policies have multiple actions that allow for a fine-grained approach to governance:

- **Deny:** Blocks the resource request.
- **Audit:** Allows the request but adds a line to the activity log (which can be used to provide alerts or to trigger runbooks.)
- **Append:** Adds specified information to the resource. For example, if there is not a "CostCenter" tag on a resource, add that tag with a default value.
- With actions such as Audit, partners can combine policy with the activity log to ensure compliance and governance needs are being enforced.

Policies can be defined to implement platform governance for many common use cases.

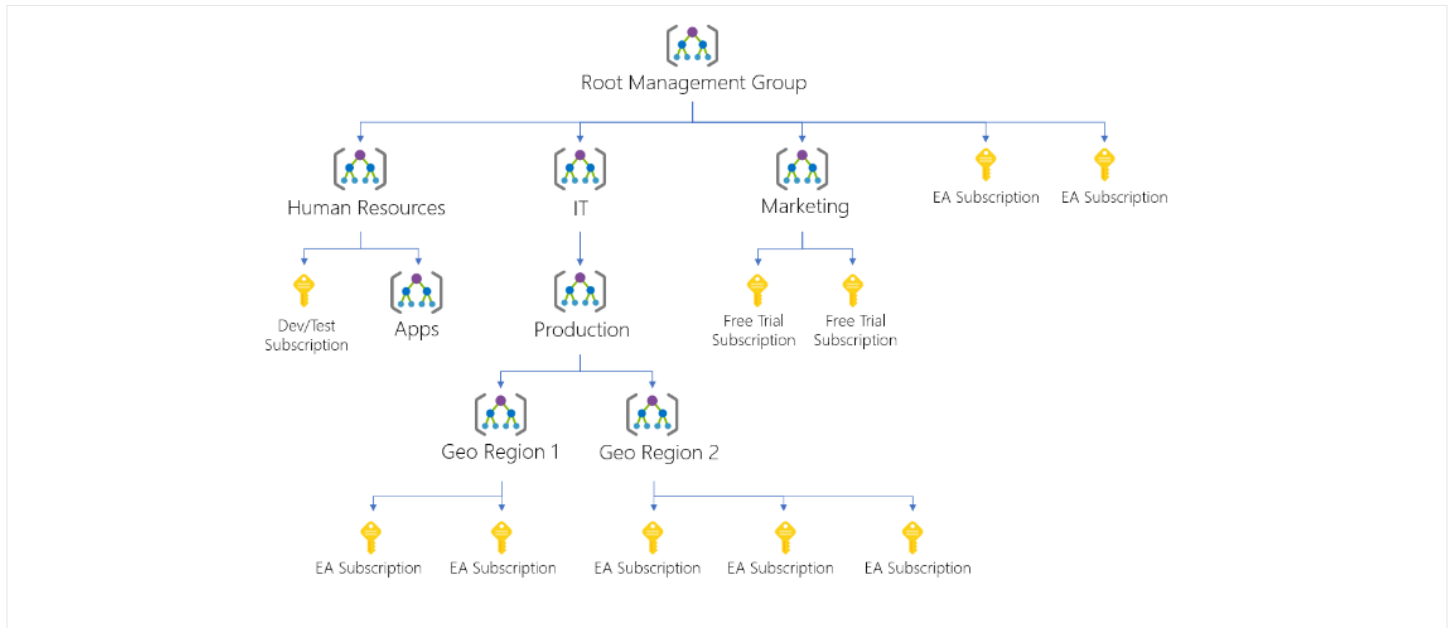
- **Geo-compliance/data sovereignty** by implementing policies which dictate the regions in which resources can be provisioned
- **Cost management** by restricting the types of resources that can be provisioned (e.g., do not allow Azure SQL Data Warehouse) and even the scale of resources (e.g., only allow certain VM sizes and SKUs)
- **Required tags to ensure** resources in Azure can be tracked, inventoried, and allocated properly in billing reports or other cost management tools

Consider where resources can be created and what types of resources can be created. Building policies that address these key items will allow partners to construct common sense policies that can be applied to their subscriptions as they are created.

MANAGEMENT GROUPS

It is quite common for customers to have more than one subscription as [management groups](#) can be used to build a hierarchy that organizes Azure Policies and RBAC controls across multiple subscriptions. Management Groups provide a level of scope above subscriptions to apply controls and governance conditions in a repeatable, automated fashion.

Management groups allow partners to organize subscriptions on their terms. For instance, they could create a hierarchy of customers or departments, apply policy to those groups, and then assign one or more subscriptions to each group.



Through a management group, administrators can make both role assignments and policy assignments. This allows for management of these governance mechanisms at the tenant level (in Azure AD) and ensures the controls are applied to existing subscriptions and to new subscriptions in an automated way.

For each tenant, there is a root management group and up to six levels of depth can be added to build a tree, or hierarchy of management groups and subscriptions that are all associated with the same Azure Active Directory tenant.

AZURE BLUEPRINTS

Azure blueprints are used to define a repeatable set of Azure resources that implement the standards, patterns, and requirements for Azure subscriptions. While management groups are used to model role assignments and policy assignments, blueprints add additional functionality through the application of artifacts, including:


- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Azure blueprints can be used to combine one or more of these artifacts and setup an entire environment rather than a single component. Where policy focuses on controlling resource properties during deployment and for existing resources, Azure Blueprints enable the creation of policy and application of policy patterns as Blueprint assignments are made and the policies included in a Blueprint definition can be combined with any of the other available artifact types.

In the case of Azure Resource Manager templates, Blueprints maintain the relationship between the Blueprint definition (what *should* be deployed) and the assignment of the Blueprint (what *was* deployed) which brings improved tracking and auditing support to Azure deployments.


Microsoft has several [sample blueprints](#) which are available directly from the Blueprint service in the Azure Portal.

Other Samples




Common Policies
A set of popular policies to apply to a subscription

[Use this sample](#)




ISO 27001: ASE/SQL Workload
Deploys and configures Azure App Service and SQL DB. Extends ISO Shared Service Blueprint. [Learn More.](#)

[Use this sample](#)




ISO 27001: Shared Services
Deploys and configures Azure infrastructure and policies mapped to specific ISO controls. [Learn More.](#)

[Use this sample](#)



Basic Networking (VNET)
Configures a virtual network with a subnet and an NSG.

[Use this sample](#)



Resource Groups with RBAC
Sets up two resource groups and configures a role assignment for each. [Learn More.](#)

[Use this sample](#)

For example, the [ISO 27001 Shared Services Blueprint sample](#) creates an entire environment with virtual networks, Azure Firewall, Azure Key Vault, and other core services which help to meet an ISO 27001 attestation.

IAM tools

These are the tools and licensing features of Azure Active Directory for implementing hybrid identity management and put additional security controls in place to better control access to the resources hosted in Azure subscriptions or other applications that use Azure AD as an identity provider.

Azure AD Connect

[Azure AD Connect](#) is used to integrate an existing Active Directory with Azure Active Directory and perform hybrid identity management. Partners can leverage their customer's existing Active Directory investments in Azure, including the use of on-premises users and groups in RBAC assignments.

Azure AD Connect also allows customers to use features such as single sign-on (SSO) to access resources in Azure with the same identities they use on-premises today. Azure AD Connect provides capabilities to support identity synchronization needs and replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

Identity management and synchronization between on-premises and Azure AD is enabled through:

- **Synchronization:** This component is responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for on-premises users and groups is matching the cloud. Password write-back can also be enabled to keep on-premises directories in sync when a user updates their password in Azure AD.
- **AD FS:** Federation is an optional capability provided by Azure AD Connect that can be used to configure a hybrid environment using an on-premises AD FS infrastructure. Federation can be used by organizations to address complex deployments, such as single sign on, enforcement of AD sign-in policy, and smart card or third-party MFA.
- **Health monitoring:** [Azure AD Connect Health](#) can provide robust monitoring and provide a central location in the Azure portal to view this activity.

MULTI-FACTOR AUTHENTICATION AND CONDITIONAL ACCESS

Azure AD can enable additional levels of validation such as [multi-factor authentication](#) and [conditional access policies](#). Monitoring suspicious activity through advanced security reporting, auditing, and alerting helps mitigate potential security issues.

In the public cloud, identity is the control plane to protect the identity of the users that consume Azure resources. One of the easiest steps to protect these, and other privileged accounts is enabling multi-factor authentication (MFA). Azure offers multiple verification options, including phone call, text message, or mobile app notification through the [Microsoft Authenticator app](#).

Conditional access policies, a feature available through Azure AD Premium licensing, allows admins to create policy-based access rules for any Azure AD-connected application (SaaS apps, custom apps running in the cloud or on-premises web applications). Azure AD evaluates these policies in real-time and enforces them whenever a user attempts to access an application. Azure identity protection policies can block access to users at high risk, enforcing multi-factor authentication, and resetting user passwords if it looks like credentials have been compromised.

PRIVILEGED IDENTITY MANAGEMENT

[Privileged Identity Management](#), included with the Azure Active Directory Premium P2 offering enables admins to discover, restrict, and monitor administrative accounts and their access to resources in the Azure Active Directory and other Microsoft online services. It also helps administer on-demand administrative access for the exact period needed.

Privileged Identity Management can enforce on-demand administrator rights so that administrators can request multi-factor authenticated, temporary elevation of their privileges for pre-configured periods of time before their accounts return to a normal user state, not only to privileged [roles in Azure AD](#) but also to [role assignments in Azure](#).

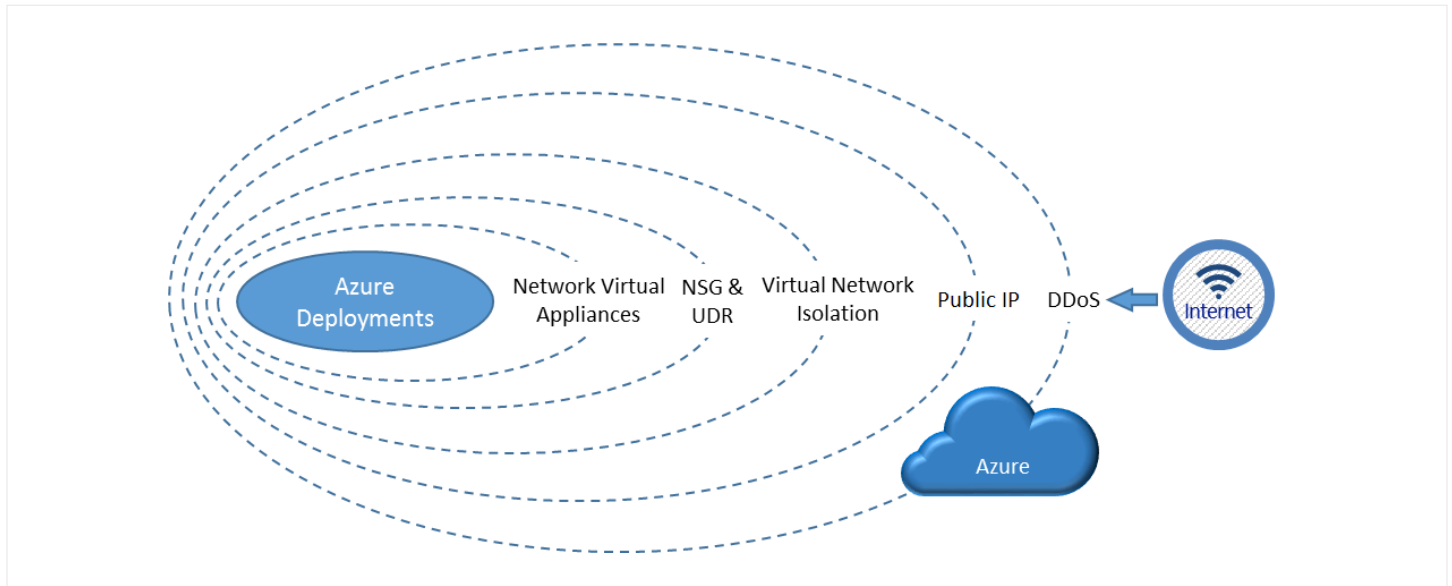
Security and networking

Azure's hyperscale networking and built-in security services extend the concept of the vDC to another layer.

Building on the foundation of subscriptions and access controls, partners must also put configurations and services in place that bring secure and private connectivity to the Azure workloads.

Networking resources

When approaching the design of networks in Azure, it is important to consider that Azure provides multiple layers of network security, some of which are native to the Azure platform and others which can optionally be implemented as customer needs changes.



VIRTUAL NETWORK

The core of a software-defined network in Azure is a [virtual network](#), an isolated portion of the Azure public network that is dedicated to a subscription. Within a subscription, one or more virtual networks can be segmented into subnets and then layered with network security groups, application security groups, and user-defined routes. In building out a vDC, consider how the design of the virtual networks will contribute to isolation and segmentation of workloads within subscriptions.

There are many questions to answer in the design of virtual networks, such as:

- Are there existing security requirements for isolating traffic into dedicated networks?
- Do the networks need to be isolated to specific subscriptions or regions?
- How many network interfaces and private IP addresses are required?
- Does the virtual network need to connect to another network, either virtual or on-premises?
- Are there administration or management requirements for resources in different networks?
- Have services in Azure which create their own virtual network been accounted for?
- Have the [networking limits](#) within an Azure subscription been accounted for?

The above questions will help determine where the networks will be provisioned and their potential address spaces. They will also show where policy and RBAC can be applied to allow for administration and management of the networks.

The address spaces allocated to virtual networks are a critical design decision, especially for hybrid connectivity through VPN and ExpressRoute Gateways or even virtual network peering within Azure. To design [network topologies](#) such as hub-spoke or hub-spoke-spoke in Azure, ensure that IP addresses spaces do not overlap in connected networks.

SUBNETS

An equally important consideration for the design of virtual networks will be how to segment them with subnets. Each subnet must have a unique address range within the address space of a virtual network and that subnet range cannot overlap with other subnets in the network.

There are some Azure service resources which may require (or even create) their own subnet and will need enough allocated space for them to do so. Planning for services like Service Fabric, HDInsight, Virtual Machine scale sets, and even VPN Gateways becomes a critical consideration. See [Services that can be deployed into a virtual network](#) for a full list of services which will consume address space within virtual networks. If there are no plans to use these services, consider restricting the ability to provision them with Azure Policy.

NETWORK SECURITY GROUPS

[Network security groups](#) (NSGs) can limit inbound and outbound traffic to resources in their virtual networks for both subnets and individual network interfaces on virtual machines. The security rules implemented in a network security group can limit traffic based on source or destination IP address, port, and protocol. NSGs can be shared between multiple subnets and network interfaces to create a single set of rules that can then be applied to multiple resources.

Consider that subnets and network interfaces can have zero, or one, associated NSG. A best practice is to ensure NSGs are in place for resources, even if only to deploy a minimal ruleset.

Microsoft also includes [service tags](#) which can be used when building NSGs. A service tag represents a group of IP address prefixes which can minimize the complexity of NSGs. Consider an NSG that needs to allow inbound access from an Azure Load Balancer. A single service tag can define an NSG which will automatically whitelist inbound connections from the Azure Load Balancer service when using the *AzureLoadBalancer* service tag. Without this tag, a whitelist of IP addresses (or address ranges) would need to be manually maintained and manually updated for all NSGs that need to allow access from the Load Balancer any time the public service changes.

Service tags are available for many Azure services, including the previously mentioned Azure Load Balancer, Azure Traffic Manager, Azure Storage, Azure SQL Database, Azure Cosmos DB, and Azure Key Vault. For the full list of service tags and their values, see [Service tags](#).

APPLICATION SECURITY GROUPS

[Application security groups](#) (ASGs) can be used to group virtual machines and define network security policies based on those groups. Much like NSGs, ASGs provide a further level of abstraction for network policy, simplifying management and deepening the control plane. ASGs can model and implement a set of rules that can be reused multiple times based on business requirements.

For example, consider a traditional two-tier application with a web and a data tier. ASGs can be used to create a rule that defines the inbound and outbound security for the web tier (e.g. traffic is allowed inbound from the internet on port 80 and outbound to the data tier on port 1433). A similar rule can be created for the data tier (e.g., traffic is allowed inbound on port 1433 from the web tier). With the security rules defined, apply them to the virtual machines, with the web rule applied to the web services and the data rule applied to the database servers. As new servers or applications come online that can make use of the same ruleset, they can have the same ASGs applied as needed.

USER-DEFINED ROUTES

By default, Azure routes network traffic between all subnets in a virtual network. Override Azure's default routing to prevent Azure routing between subnets, or to route traffic between subnets through a network virtual appliance by implementing user-defined routes (UDRs). UDRs can be used to implement additional security controls through network virtual appliances (NVAs) such as firewalls or other network filtering devices.

VIRTUAL NETWORK SERVICE ENDPOINTS

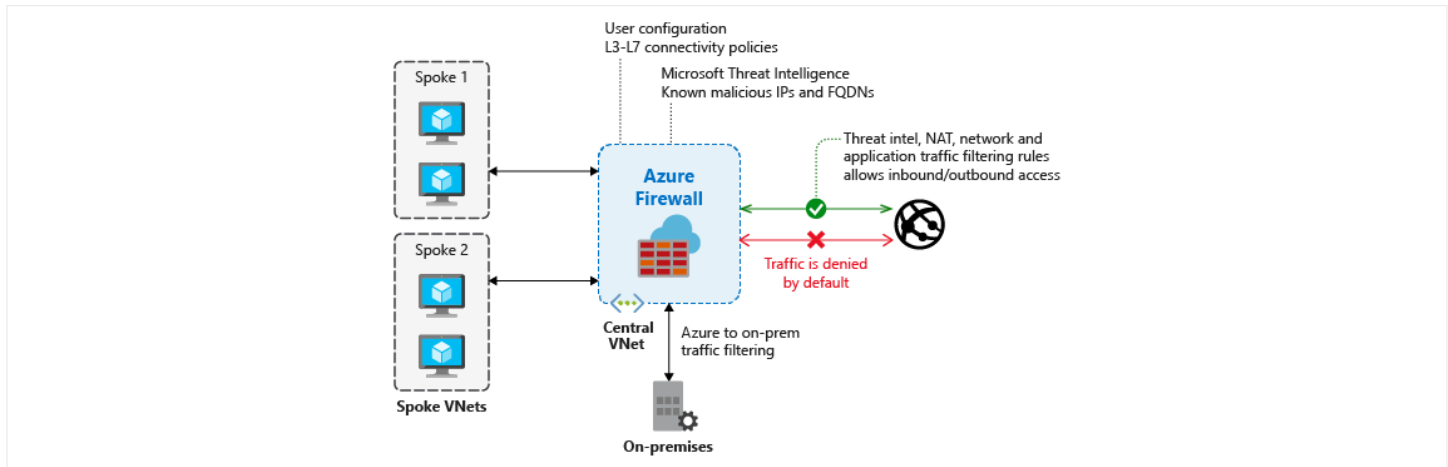
Limit access to Azure resources such as an Azure storage account or Azure SQL database, to specific subnets with a [Virtual Network Service Endpoint](#). Further deny access to the resources from the internet or create multiple subnets, and enable a service endpoint for some subnets, but not others.

Virtual network service endpoints extend the control plan for Azure PaaS services, improving the security for service resources by allowing traffic from only the virtual networks. Service endpoints also ensure that optimal routes are in place when using hybrid networking features such as forced tunneling.

Service endpoints are [available](#) for Azure Storage, Azure SQL Database, Azure SQL Data Warehouse, Azure Cosmos DB, Azure Key Vault, and many more Azure services with support for additional services always being added.

AZURE FIREWALL

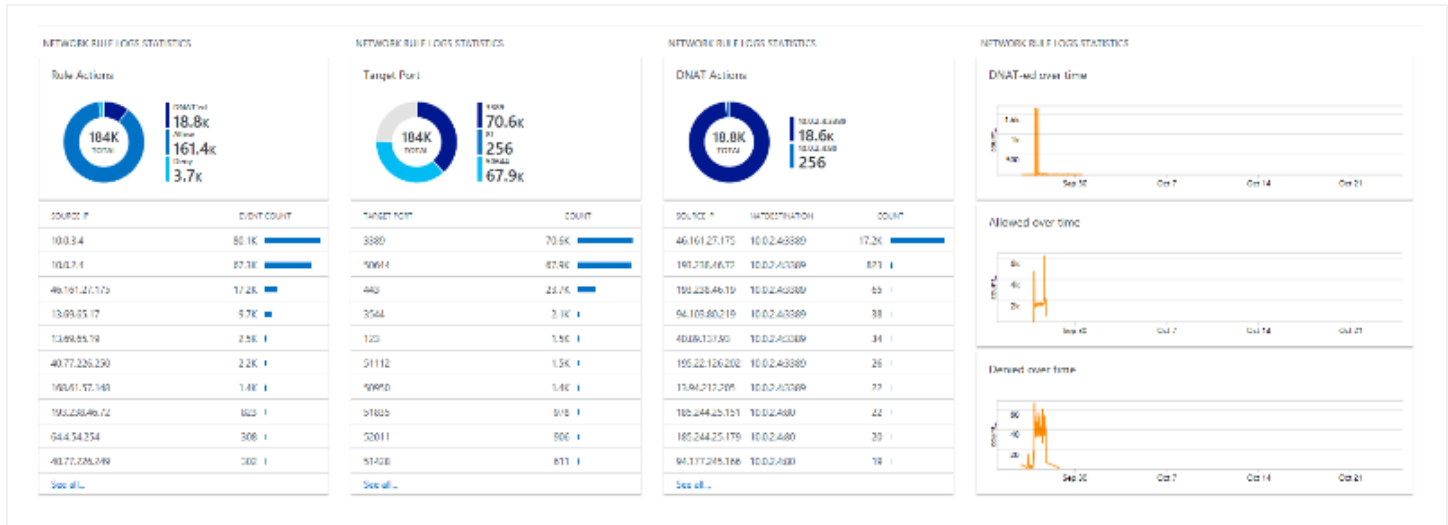
[Azure Firewall](#) is a managed, cloud-based network security service that protects Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.



Azure Firewall offers the following features:

- **Built-in high availability** requires no additional load balancers or configuration.
- **Unrestricted cloud scalability** allows Azure Firewall to scale out automatically to accommodate changing networking traffic flows.
- **Application FQDN filtering rules** allow for the management of outbound access to only allowed URIs, with support for protecting both HTTP/HTTPS sites and wildcards in domain names.
- **Network traffic filtering rules** allow for the management of allow or deny rule by source and destination IP address, port, and protocol.
- **FQDN tags** make it easier to manage access to well-known services such as Windows Update and Azure Backup.
- **Service tags** make it easy to allow well-known Azure service network traffic to flow through the firewall so applications can consume Azure services in a secure way without the overhead of monitoring the IP address space, ports, and protocols that Microsoft users for its services.
- **Threat intelligence**-based filtering leverages Microsoft's Threat Intelligence feedback to automatically block known malicious IP addresses and domains.
- **Outbound SNAT support** ensures that all outbound traffic from the firewall is translated to the public IP of the firewall to identify and allow traffic originating from the virtual networks to remote destinations outside of Azure.
- **Inbound DNAT support** protects resources in the virtual networks with Azure Firewall.
- **Azure Monitor logging** provides an integrated monitoring experience to archive firewall logs to storage accounts, an Event Hub, or to a Log Analytics workspace where they can be queried through Azure Monitor logs.

Microsoft provides samples for [creating Azure Firewall with PowerShell](#), [deploying using a template](#), and for [visualization of your firewall logs](#) through data stored in a Log Analytics workspace.



Azure Firewall also integrates with and supports other Azure networking resources such as [load balancers](#) and Network Security Groups.

NETWORK VIRTUAL APPLIANCES

There are hundreds of [Network Virtual Appliances](#) (NVAs) available in the [Azure Marketplace](#) that are easy to configure, scalable, and highly-available.

NVAs help execute even the most advanced networking scenarios in Azure when combined with native platform features like UDRs. NVAs are available for many functions, including next-generation firewalls (NGFW), web application firewalls (WAF), gateways and routers, application delivery controllers (ADC), and WAN optimizers.

The choice to use an NVA will depend on the specific requirements and security needs. For instance, there may be a requirement to inspect all outbound internet traffic from one or more virtual networks. Partners can deploy an NVA pair (for high availability) to a hub network and route traffic from the spoke networks through the hub. Another example would be the implementation of a third-party load balancer that has additional features beyond what Microsoft's native load-balancer or application gateway provide.

There are many considerations for deploying NVAs. Some are straightforward, such as the need for additional licensing, while others are less well known such as accounting for the additional operations overhead or maintaining additional virtual machines and appliance specific configurations. Ask the following questions prior to deploying NVAs:

- Is there an equivalent Azure service which meets the requirements?
- Does the NVA need to be highly available? If so, what are the cost and management impacts?
- How many NVAs are needed based on the network throughput? Azure limits will once again come into play as virtual machine network interfaces have a maximum throughput.
- What type of support will be needed from the NVA vendor in the event assistance is required?
- Is there a need for multiple NVAs in series? For example, an NVA implementing a firewall could be placed in series with an NVA performing ADC.

AZURE APPLICATION GATEWAY

[Azure Application Gateway](#) is a dedicated virtual appliance providing application delivery controller (ADC) as a service, offering various layer 7 load-balancing capabilities for applications hosted in Azure.

Application Gateway is provisioned in a subnet and is a part of the virtual network, so it respects both routing and Network Security Groups as well. As a layer 7 load balancing solution, Application Gateway supports:

- Secure Sockets Layer (SSL) termination
- Connection draining
- Custom error pages
- Web application firewall
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- WebSocket and HTTP/2 support

With the ability to host multiple sites behind a single Application Gateway, partners can implement more efficient topologies and still maintain segmentation of traffic by directing traffic from the gateway to well-defined backend pools, where pool members can include virtual machines, or even PaaS services such as Azure Web Apps.

SSL termination allows for offloading the potential overhead of managing SSL directly on the servers behind the gateway and the overhead of encrypting and decrypting traffic on those servers as well. This is an optional feature of the Application Gateway, which also supports end-to-end SSL encryption when it is required. This feature can be combined with redirection as well. For example, with the Application Gateway SSL can be configured and a redirection rule can be implemented to redirect traffic from HTTP to HTTPS automatically.

Connection draining is used to gracefully remove backend pool members during maintenance or planned service updates. This feature also allows for unhealthy pool members to be removed from a backend pool in a controlled manner in the event they are marked as unhealthy by a health probe.

Web application firewall (WAF) is a feature of Application Gateway that provides centralized protection of web applications from common exploits and vulnerabilities. WAF is based on rules from the [OWASP \(Open Web Application Security Project\) core rule sets](#) 3.0 or 2.2.9 and each rule within the ruleset can be customized. The WAF feature of Application Gateway provides both protection from malicious attacks such as SQL injection and cross-site scripting and rich monitoring through a real-time log that is integrated with Azure Security Center and Azure Monitor which allows for the easy creation and management of WAF alerts. The integration with Azure Monitor also brings support for visualization of the WAF log through Azure Dashboards.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

Distributed denial of service (DDoS) attacks are often one of the largest concerns customers surface when bringing their workloads to the cloud. DDoS attacks flood resources with network requests which exhaust an application's resources. This makes the application unavailable to legitimate users and leads to additional cost for application owners to remediate the attack.

[Azure DDoS Protection](#) is available in two tiers -Basic and Standard. Basic DDoS protection is built directly into the Azure platform and is available for no additional cost. This free coverage is included for both IPv4 and IPv6 Azure public IP addresses.

If additional protection is required, the Azure DDoS Protection Standard tier provides additional mitigation abilities for protecting Azure resources with public IP addresses such as Azure Load Balancer or Azure Application Gateway. The Standard tier provides mitigations for volumetric attacks, protocol attacks, and application layer attacks.

The Azure DDoS Protection service can be layered with other Azure services, including WAFs and NVAs providing layer 3 to layer 7 mitigation capabilities. The DDoS service also integrates with monitoring services, including Azure Monitor, Azure Log Analytics, Azure Storage, or third-party SIEM tools like Splunk.

PENETRATION TESTING

Microsoft [performs regular penetration testing of its networks](#), including Azure. They do not however provide penetration testing for the applications and workloads deployed into Azure. Customers can perform their own penetration testing as needed. It is recommended (but not required) to inform Microsoft of such activities by filling out the Azure Service Penetration Testing Notification form. Standard tests include:

- Testing internet endpoints for any of the [OWASP top 10 vulnerabilities](#)
- Fuzz testing of endpoints
- Port scanning of endpoints

There are tests which cannot be performed under any circumstance such as any kind of Denial of Service (DoS) attack. All pen testing must comply with the [Microsoft Cloud Unified Penetration Testing Rules of Engagement](#).

DEPLOYED ADVANCED SCENARIOS

By combining the networking features of Azure, partners can support even the most complex topologies, including rich segmentation of Azure networks from each other and from on-premises networks when implementing hybrid networking.

There are examples provided for:

- ➔ [Implement a DMZ between Azure and your on-premises datacenter](#)
- ➔ [Implement a DMZ between Azure and the Internet](#)
- ➔ [Deploy highly available network virtual appliances](#)
- ➔ [Implement a hub-spoke network topology in Azure](#)
- ➔ Implement a hub-spoke network topology with shared services in Azure

Security for virtual machines

There are many considerations for securing virtual machines in Azure beyond the network layer. Partners can add additional protections including anti-virus and antimalware solutions, disk encryption, and threat detection.

VIRTUAL MACHINE ACCESS CONTROL

There are two layers to controlling access to virtual machines – controlling access to the Azure resource (e.g., the VM configuration) and controlling access to the VM itself (e.g., local logon via SSH). There are several built-in Azure RBAC roles specifically for virtual machines:

- **Virtual machine contributor** can manage VMs, but not the virtual network or storage account to which they are connected.
- **Classic virtual machine contributor** can manage VMs created by using the classic deployment model, but not the virtual network or storage account to which the VMs are connected.
- **Security admin** can manage security components and security policies.
- **DevTest labs user** can view everything and connect, start, restart, and shut down VMs.

Grouping virtual machines with the same lifecycle together in the same resource group and using the built-in roles can simplify the management and improve the security posture of these Azure resources.

ANTIMALWARE PROTECTION

There are antimalware and anti-virus solutions available from Microsoft and other vendors in the Azure Marketplace. Considerations for selecting an antimalware solution include operating systems covered and any requirements for integrating with other Azure services such as Log Analytics or Azure Storage for event collection and aggregation.

When protecting compatible Windows workloads, Microsoft [Antimalware for Azure Cloud Services and Virtual Machines](#) is available at no additional cost as a native Azure virtual machine extension. For Linux workloads that require antimalware protection or have relationships with other antimalware vendors, there are multiple offerings in the Azure Marketplace from vendors like Symantec, Trend Micro, and Kaspersky.

DISK ENCRYPTION

Encrypting data in virtual machines can be considered a mandatory step, especially when considering needs for data privacy, compliance, and data sovereignty. Encrypting disks can reduce the threat of data theft or exposure from unauthorized access in the event a disk is moved.

By default, [Azure Storage Service Encryption](#) (SSE) is enabled for all new and existing storage accounts and cannot be disabled. This ensures that the data is encrypted at rest in all Standard and Premium storage accounts, both ARM and ASM, and for all storage services (blob, queue, table, and files).

To go a step further, [disk encryption](#) in Azure is available for both Windows and Linux operating systems, with Windows leveraging Bitlocker and Linux using DM-Crypt. This allows for the use of SSE for the virtual disks to encrypt the contents of those disk, providing protection at the resource level as well as within the configuration of the resource itself (in this case, a VHD). Encryption can be enabled for both the operating system and the data disks. Disk encryption in Azure is integrated directly with [Azure Key Vault](#) for the storage of encryption keys.

Azure Key Vault allows can store and manage the lifecycle of encryption keys for both SSE and Azure Disk Encryption. It can automate the end-to-end lifecycle of data in Azure, ensuring access control and the ability to revoke access as need by simply invalidating an encryption key.

UPDATE MANAGEMENT

Patching and maintaining virtual machines is critical to the security posture. Azure offers a patch management service as a part of Azure Automation to discover, inventory, track changes, and update both Linux and Windows workloads hosted in Azure, on-premises environments, and even other cloud providers.

[Update management](#) can quickly assess the state of patch installation (including the status of available updates), schedule required updates, and verify the installation of updates through change tracking.

To leverage update management, an Azure Automation account will need to be created to hold a watcher, the action runbooks, and a watcher task. Update management also leverages a Log Analytics workspace, where it stores the logs and metadata associated with the watcher.

Onboarding a virtual machine to Update management requires that the solution be enabled for a given virtual machine. The Update management solution can be enabled for individual machines, all current machines, all future machines, and all future machines, or only on a specific set of virtual machines.

There is no additional charge for Update management in Azure Automation beyond the charges for the metadata stored in Log Analytics. With Update management, partners can ensure that customers have a patch management tool in place for their entire Azure estate.

THREAT DETECTION

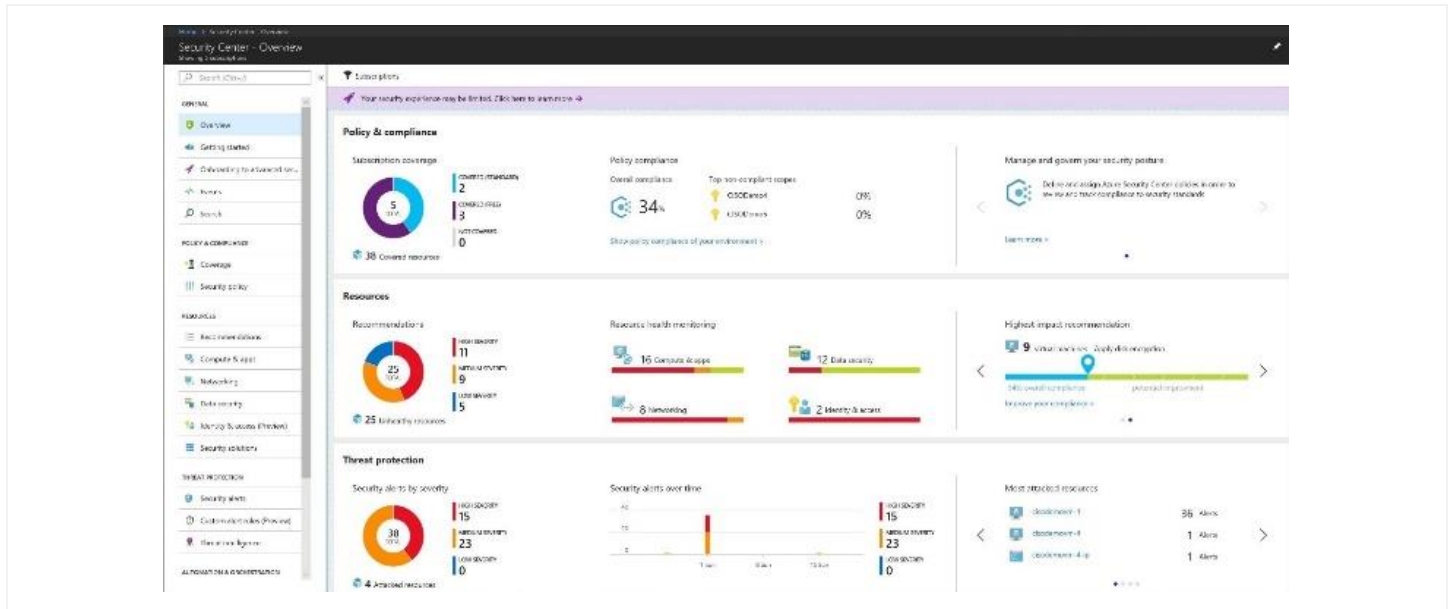
Implementing these controls is not enough. Partners also need to monitor their virtual machines and analyze their security posture on an ongoing basis.

[Azure Security Center](#) helps prevent, detect, and respond to threats with increased visibility into and control over the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Azure Security Center should be part of any Azure practice to assist with monitoring and support.

Security Center delivers effective threat prevention, detection, and response capabilities that are built into Azure. Some of its key capabilities are:

- Monitors the security state of Azure resources.
- Defines policies for Azure subscriptions and resource groups based on security requirements, the types of applications in use, and the sensitivity of the data.
- Uses policy-driven security recommendations to guide service owners through the process of implementing needed controls.
- Rapidly deploys security services and appliances from Microsoft and partners.
- Automatically collects and analyzes security data from Azure resources, the network, and partner solutions like antimalware programs and firewalls.
- Leverages global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
- Applies advanced analytics, including machine learning and behavioral analysis.
- Provides prioritized security incidents/alerts.
- Offers insights into the source of the attack and impacted resources.
- Suggests ways to stop the current attack and help prevent future attacks.

Security Center is available in two tiers – Free and Standard. Every Azure customer should be using the Free tier of Security Center and it is a powerful tool for demonstrating how partners can keep customers more secure in Azure.



JUST IN TIME VM ACCESS

A feature of the Standard pricing tier of Azure Security Center, Just in Time VM Access (JIT) brings both a security and access management feature to a virtual machine control plane. JIT can restrict inbound management traffic (e.g., RDP and SSH traffic) to the virtual machines and expose the required ports for access on an on-demand basis. JIT greatly reduces the amount of time these management ports are open which reduces the time windows for common attacks like brute force login attempts.

With JIT enabled, Azure Security Center can manage the NSG rules associated with the virtual machines.

Administrators and other operators can request access to the virtual machine through Security Center. It is at this time that RBAC is evaluated, and if the user has rights to request access the ports are opened for the specified amount of time. After the time has expired, Security Center automatically revokes access to the management ports by restoring the NSG to its previous state.

Just in time VM access can be audited and monitored through the Azure Activity Log which provides a full detail of all the operations for the VM, including the time, date, and subscription.

Activity log

Columns

Export

Log search

Gain insights into Azure activities using log search and visualization for FREE

<Subscription ID>

Subscription

ASC DEMO

Timespan

Last week

Apply

Reset

Resource group

Type to start filtering ...

Event category

All categories

Resource

vm2W1

Event severity

4 selected

Resource type

Type to start filtering ...

Event initiated by

Email or name or service principal name

Operation

All operations

Search

Insights (Last 24 hours):

0 failed deployments

0 role assignments

0 errors

0 alerts fired

0 outage notifications

Query returned 7 items.

Click here to download all the items as CSV

OPERATION NAME	STATUS	TIME	TIME STAMP	SUBSCRIPTION	EVENT INITIATED BY
JIT Network Access request ended	Succeeded	6 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	9 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	10 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	12 h ago	Thu Mar 02 2...	ASC DEMO	
JIT Network Access request ended	Succeeded	6 d ago	Sat Feb 25 2...	ASC DEMO	
JIT Network Access request initiated	Succeeded	6 d ago	Fri Feb 24 20...	ASC DEMO	
JIT Network Access request ended	Succeeded	7 d ago	Fri Feb 24 20...	ASC DEMO	

Configuration management

The ongoing management of Azure deployments should be grounded in automation. Azure offers several services which can help deploy Azure environments in a repeatable fashion and ensure that they are configured to the requirements from the start.

AUTOMATE THE CONFIGURATION OF VMS

There are many tools for creating and managing Azure virtual machines in a consistent manner at any scale. These solutions all contribute to the overall infrastructure management and deployment lifecycle of Azure workloads.

ANSIBLE, CHEF, AND PUPPET

[Ansible](#) is an automation engine for configuration management, VM creation, or application deployment. Ansible uses an agent-less model, typically with SSH keys, to authenticate and manage target machines. Configuration tasks are defined in playbooks, with several Ansible modules available to carry out specific tasks.

[Chef](#) is an automation platform that helps define how the infrastructure is configured, deployed, and managed. Additional components included Chef Habitat for application lifecycle automation rather than the infrastructure, and Chef InSpec that helps automate compliance with security and policy requirements. Chef Clients are installed on target machines, with one or more central Chef Servers that store and manage the configurations.

[Puppet](#) is an enterprise-ready automation platform that handles the application delivery and deployment process. Agents are installed on target machines to allow Puppet Master to run manifests that define the desired configuration of the Azure infrastructure and VMs. Puppet can integrate with other solutions such as Jenkins and GitHub for an improved DevOps workflow.

CLOUD-INIT FOR LINUX VMS

[cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. Use cloud-init to install packages and write files, or to configure users and security. Because cloud-init is called during the initial boot process, there are no additional steps or required agents to apply the configuration.

cloud-init also works across distributions. For example, don't use `apt-get install` or `yum install` to install a package. Instead, define a list of packages to install. cloud-init automatically uses the native package management tool for the distro selected.

There are even [cloud-init enabled VMs in the Azure Marketplace](#). These images make cloud-init deployments work seamlessly with VMs and Virtual Machine Scale Sets.

PUBLISHER	CLOUD-INIT READY
Canonical	Yes
Canonical	Yes
CoreOS	Yes
OpenLogic	Preview
RedHat	Preview

POWERSHELL DESIRED STATE CONFIGURATION

[PowerShell Desired State Configuration \(DSC\)](#) is a management platform to define the configuration of target machines. DSC can also be used on Linux through the [Open Management Infrastructure \(OMI\) server](#).

DSC configurations define what to install on a machine and how to configure the host. A Local Configuration Manager (LCM) engine runs on each target node that processes requested actions based on pushed configurations. A pull server is a web service that runs on a central host to store the DSC configurations and associated resources. The pull server communicates with the LCM engine on each target host to provide the required configurations and report on compliance.

AZURE CUSTOM SCRIPT EXTENSION

The Azure Custom Script Extension for [Linux](#) or [Windows](#) downloads and executes scripts on Azure VMs. Use the extension when creating a VM, or any time after the VM is in use.

Scripts can be downloaded from Azure storage or any public location such as a GitHub repository. The Custom Script Extension can be used to write scripts in any language that runs on the source VM. These scripts can be used to install applications or configure the VM as desired. To secure credentials, sensitive information such as passwords can be stored in a protected configuration. These credentials are only decrypted inside the VM.

AUTOMATE INFRASTRUCTURE MANAGEMENT

There are a suite of technologies and tools which can be used in Azure to perform infrastructure management and contribute to the principles of managing infrastructure as code.

PACKER

[Packer](#) automates the build process when creating a custom VM image in Azure. Use Packer to define the OS and run post-configuration scripts that customize the VM for specific needs. Once configured, the VM is then captured as a Managed Disk image. Packer automates the process to create the source VM, network and storage resources, run configuration scripts, and then create the VM image.

TERRAFORM

[Terraform](#) is an automation tool for defining and creating an entire Azure infrastructure with a single template format language – the HashiCorp Configuration Language (HCL). It helps define templates that automate the process to create network, storage, and VM resources for a given application solution. Existing Terraform templates for other platforms can be used with Azure to ensure consistency and simplify the infrastructure deployment without needing to convert to an Azure Resource Manager template.

AZURE AUTOMATION

[Azure Automation](#) uses runbooks to process a set of tasks on the targeted VMs. Azure Automation is used to manage existing VMs rather than to create an infrastructure. Azure Automation can run across both Linux and Windows VMs, as well as on-premises virtual or physical machines with a hybrid runbook worker. Runbooks can be stored in a source control repository, such as GitHub. These runbooks can then run manually or on a defined schedule.

Azure Automation also provides a Desired State Configuration (DSC) service to create definitions for how a given set of VMs should be configured. DSC then ensures that the required configuration is applied and the VM stays consistent. Azure Automation DSC runs on both Windows and Linux machines.

AZURE CLOUD SHELL

[Azure Cloud Shell](#) is an interactive, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way users work. Linux users can opt for a Bash experience, while Windows users can opt for PowerShell.

Azure Cloud Shell even includes pre-configured tools such as Ansible and Terraform which can accelerate the adoption of infrastructure automation.

Availability and business continuity

A control plane for Azure resources needs to provide coverage for the availability of the workloads hosted and account for the business continuity and disaster recovery needs of the applications.

Virtual machine availability

AZURE MAINTENANCE

When designing a virtual machine availability strategy, be sure to account for both maintenance in the Azure platform and downtime. There are three scenarios which can impact virtual machine availability: unplanned hardware maintenance, unexpected downtime, and planned maintenance.

Unplanned maintenance events occur when the Azure platform detects a pending failure in a virtual machine host, storage, or any other platform component associated with the physical platform. Microsoft uses Live Migration technology for virtual machines, allowing Microsoft to migrate virtual machines from the faulting hardware to a healthy physical host. Live Migration allows Microsoft to perform these migrations while keeping memory, files, and network connections open during the migration, but there may be performance impacts to virtual machines before, during, and after the event.

Unexpected downtime occurs when the physical host fails unexpectedly. This can be anything from a network failure, a disk failure, or even a rack-level failure. When these events are detected, the affected virtual machine is automatically migrated to a healthy physical host with minimal downtime. While minimal, there is downtime in these types of events, including a reboot of the virtual machine and a reset of any ephemeral storage such as a temporary drive/scratch disk.

Planned maintenance events occur as a part of regular and ongoing Azure datacenter maintenance. In the majority of cases, Microsoft attempts to use [VM Preserving Maintenance](#), where a VM is paused while the underlying host is patched and unpaused without any reboot once maintenance has completed. However, there are instances where a reboot of a VM will be needed. In these instances, use [Planned Maintenance](#) to schedule the reboot or redeployment of the VM to a new host.

IMPROVING AVAILABILITY

There are three financially backed [service level agreements for virtual machines](#) in Azure to select from based on the requirements.

- **99.9%** availability is guaranteed for single-instance virtual machines that use premium storage.
- **99.95%** availability is guaranteed for at least one virtual machine when two or more instances are deployed in the same availability set.
- **99.99%** availability is guaranteed for at least one virtual machine when two or more instances are deployed across two or more availability zones.

AVAILABILITY SETS

Availability Sets can be used to spread two or more virtual machines across up to twenty update domains (UDs) within an Azure datacenter. During planned maintenance, Microsoft guarantees that only one update domain is updated at any given time. As UD's are updated within the data center, there is a 30-minute recovery window before the next UD is updated. This guarantee is what provides the increased SLA of 99.95% on virtual machines.

The adoption of availability sets also increases availability by ensuring that virtual machines are placed into multiple fault domains (FDs). FDs ensure that virtual machines are grouped in a way that prevents them from sharing a common power source and network switch.

AVAILABILITY ZONES

Availability Zones offer even more resiliency than Availability Sets, hence the increased SLA of 99.99%. Availability Zones can be used to physically separate virtual machines within an Azure region, with updates to three Availability Zones supported per region. Each Availability Zone comes with its own power source, network, and cooling.

This makes Availability Zones a natural choice to guarantee the protection of applications in the event of the loss of an Azure datacenter.

Backup and recovery

Azure offers both backup and recovery services natively with Azure Backup and Azure Site Recovery. Both services can backup and restore data, but each serves a different purpose regarding business continuity and disaster recovery.

Azure Backup can backup and restore data at a very granular level, including file and folder recovery. Azure Site Recovery can be used to replicate virtual machines between datacenters, orchestrate failovers, and even perform migrations. At their most basic, Azure Backup protects data wherever it resides – in the cloud or on-premises while Azure Site Recovery coordinates virtual machine and physical server replication, failover, and failback.

Both services contribute to the business continuity and disaster recovery needs of workloads and applications by keeping the data safe (Azure Backup) and keeping the workloads available (Azure Site Recovery) when outages occur.

Consider the following when selecting backup and recovery services:

- **Recovery point objective (RPO):** The amount of acceptable data loss if a recovery is needed.
- **Recovery time objective (RTO):** The amount of time that it takes to perform a restoration or recovery.
- **Retention:** The amount of time the data needs to be stored.

Note that some workloads may require both backup and disaster recovery (e.g., local resiliency as first layer and geo-redundancy for additional protection).

	BACKUP	DISASTER RECOVERY
RPO	Workloads with variable RPO. Servers may be days while databases may be hours or even minutes.	Workloads with low RPOs where DR copies are only a few minutes behind their source.
RTO	Backup solutions typically have longer RTOs as wider RPO windows driver larger backup sets. This can lead to recovery times of hours or days.	DR solutions will have much smaller RTOs, sometimes less than a minute as data is constantly synchronized with the source.
RETENTION	Backup is suitable for workloads with both long and short term retention needs. Compliance often drives the retention window (e.g., financial records often need to be retained for years).	DR is not suitable for long term retention as it is capturing so many changes in a short period of time.

AZURE BACKUP

[Azure Backup](#) is the Azure-based service to use to back up (or protect) and restore data in the Microsoft cloud. Azure Backup replaces existing on-premises or off-site backup solutions with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components to deploy depending on what needs to be protected. All Azure Backup components (no matter whether they are protecting data on-premises or in the cloud) can be used to back up data to a Recovery Services vault in Azure.

Traditional backup solutions have evolved to treat the cloud as an endpoint, or static storage destination, like disks or tape. While this approach is simple, it is limited and doesn't take full advantage of an underlying cloud platform, which

translates to an expensive, inefficient solution. Other solutions can be inefficient and expensive when paying for the wrong type of storage, or unneeded storage, or administrative tasks require too much time. In contrast, Azure Backup delivers these benefits:

- **Automatic storage management** that offers automatic allocation and management of backup storage all in a pay-as-you-use model.
- **Unlimited scaling** with the built-in capabilities of Azure storage, including high availability, multiple storage sizes, and multiple storage tiers.
- **Multiple storage options** with access to both locally redundant storage and geo-redundant storage. Data is always protected with at least three copies in a region.
- **Unlimited data transfer** with no caps on the amount of inbound or outbound data transferred.
- **Data encryption** allows for the secure transmission and storage of data with full control of the encryption passphrase (or key)
- **Application-consistent backup** means recovery points have all the required data to restore the backup copy with no additional fixes required – reducing the restoration time.
- **Long-term retention** means keeping data in the Recovery Services vault as long as needed.

AZURE BACKUP COVERAGE

Azure Backup provides coverage for a wide range of workloads and applications. At a high-level, Azure Backup provides coverage for files and folders, Hyper-V virtual machines, VMware virtual machines, Azure virtual machines, and application consistent backup for Microsoft SQL Server, Microsoft SharePoint, Microsoft Exchange,

A complete matrix of the data and workloads that can be protected with Azure Backup can be found at [Which applications and workloads can be backed up?](#)

DATA RETENTION

The length of time that backups can be retained is determined by the instance being protected (protected instance) and the frequency of backup (recovery points). Each protected instance can have up to 9,999 recovery points and there is no expiration limit on a single recovery point. A protected instance is defined as a Windows computer, a service (physical or virtual), or SQL database. Therefore, the configuration settings of the backup policy ultimately determine how quickly recovery points are consumed.

RECOVERING FROM FAILURE

Test backups at a minimum monthly if not more often to ensure their integrity and to ensure a viable recovery plan in the event restoration is required.

The restoration method for protected data in Azure Backup will differ based on the type of backup (file and folders versus full server) and the restoration tool (Azure CLI, Azure PowerShell, or the Azure Portal).

File and folder recovery are performed by determining the desired recovery point, mounting that recovery point to the virtual machine, copying the needed files, and then unmounting the recovery point. Files and folders can be restored to the same VM they were backed up from or restored to any entirely different machine.

Virtual machines that are backed up can be restored to a whole new virtual machine or disks can be mounted as additional data disks to existing virtual machines. Just as with file and folder recovery, a recovery point must be selected along with the restore configuration (new VM or disk restore).

With support for Azure CLI and Azure PowerShell, partners can even execute advanced restorations which may require additional post-restore configuration such as the instantiation of multiple network interfaces or a specific mount order for data disks on a virtual machine.

Disaster recovery

AZURE SITE RECOVERY

[Azure Site Recovery](#) (ASR) helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at a primary site, it fails over to a secondary location to access apps from there. After the primary location is running again, it can be fail back. Azure Site Recovery also forms the cornerstone of a lift-and-shift migration strategy, with support for replicating virtual machines between Azure regions (Azure-to-Azure), on-premises VMs and physical servers to Azure (Site to Azure), and even on-premises VMs and physical servers to a secondary site (Site to Site).

Azure Site Recovery offers a host of features:

- **Simple BCDR solution:** Set up and manage replication, failover, and failback from a single location in the Azure portal.
- **Azure VM replication:** Set up disaster recovery of Azure VMs from a primary region to a secondary region.
- **On-premises VM replication:** Replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
- **Workload replication:** Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.
- **Data resilience:** Orchestrate replication without intercepting application data. Data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.
- **RTO and RPO targets:** Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. Reduce RTO further by integrating with Azure Traffic Manager.
- **Keep apps consistent over failover:** Replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
- **Testing without disruption:** Easily run disaster recovery drills, without affecting ongoing replication.
- **Flexible failovers:** Run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters.
- **Customized recovery plans:** Customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. Recovery plans can be integrated with Azure automation runbooks.
- **BCDR integration:** Site Recovery integrates with other BCDR technologies. For example, use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups.
- **Azure automation integration:** A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.
- **Network integration:** Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.

APPLICATION REPLICATION

As previously mentioned, ASR can meet extremely low RPOs. Due to its near-synchronous replication, recovery plans can be executed with RPOs as low as 30 seconds and low RTO network switchovers.

ASR is also suitable for single and multi-tier application recovery when properly configured. ASR is directly integrated with SQL AlwaysOn and supports other application-level replication as well, including Active Directory replication, Exchange Database Availability Groups, and Oracle Data Guard.

To better understand ASR and its application-consistent recovery, see how to [protect a multi-tier SharePoint farm with ASR and recover it to Azure](#) while calling out important considerations. This gives an example of how a complex, three tier application that does not have explicit disaster recovery built in can utilize ASR for its components to provide a disaster recovery solution.

By utilizing ASR, we can utilize connecting to the target virtual network in a failover region, utilize [Azure Traffic Manager](#) to automatically route the users, and Recovery plans to sequence failover of the tiers of the application for proper sequencing in the event of a failover. The recovery plans can also incorporate Azure Automation runbooks to perform tasks or sequences that need to happen as part of the failover as well.

Compliance and monitoring

Build out a strategy for collecting and analyzing the data in the Azure estate to determine the performance, health, and availability of workloads and the resources on which they depend.

Azure monitoring concepts

Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on telemetry from applications and the Azure resources that support them. They can also work to monitor critical on-premises resources in a hybrid monitoring environment. Understanding the tools and data that are available is the first step in developing a complete monitoring strategy.

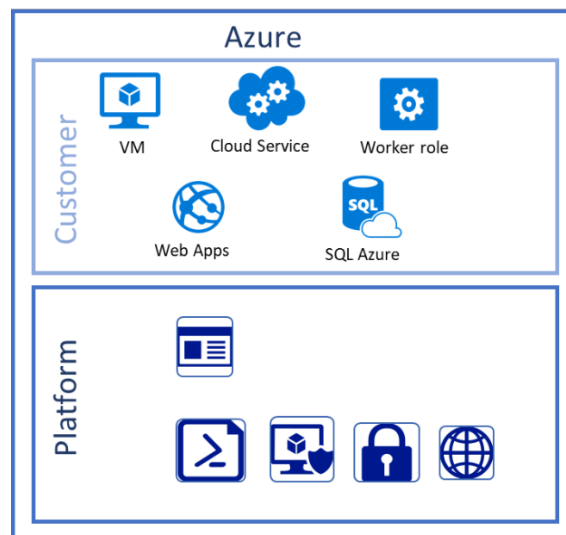
Many of the monitoring tools in Azure are integrated, offering a suite of shared capabilities such as alerts, dashboards, and metrics aggregation along with specific solutions for deep infrastructure and application monitoring.

AZURE SERVICE AND RESOURCE MONITORING

In Azure, monitoring and metrics are often available at multiple levels, including the service and resource level. For instance, virtual machines will rely on multiple Azure services like storage and networking.

APPLICATION MONITORING

The strategy must account for not only the Azure platform and resource level health, but also for the application-level audit logs and their potential ingestion into a centralized logging service such as Log Analytics.



SECURITY MONITORING

To improve the security posture and make monitoring easier when deploying virtual machines, leverage native gallery images which are consistently updated with the latest security patches and bug fixes. Then use these images to develop baselines, adopting services such as Azure Automation and DSC to perform configuration management.

Azure monitoring tools

ALERTS

[Azure alerts](#) proactively notifies when critical conditions occur and potentially take corrective action. Alert rules can use data from multiple sources, including metrics and logs. They use action groups, which contain unique sets of recipients and actions in response to an alert. Alerts can start external actions by using webhooks and integrate with existing ITSM tools.

METRICS EXPLORER

[Metrics](#) are numerical values generated by an Azure resource to help understand the operation and performance of the resource. Metrics Explorer can send metrics to Log Analytics for analysis with data from other sources.

DASHBOARDS

[Azure dashboards](#) can combine different kinds of data into a single pane in the Azure portal to share with other Azure users.

For example, a dashboard that combines:

- Tiles that show a graph of metrics
- A table of activity logs
- A usage chart from Application Insights
- The output of a log search in Log Analytics

Export Log Analytics data to [Power BI](#) to take advantage of additional visualizations and make the data available to others within and outside the organization.

AZURE MONITOR

[Azure Monitor](#) enables core monitoring for Azure services by allowing the collection of metrics, activity logs, and diagnostic logs. For example, the activity log shows when new resources are created or modified.

Azure Monitor provides the fastest metrics pipeline (5 minutes down to 1 minute) for time-critical alerts and notifications. Or send these metrics and logs to Azure Log Analytics for trending and detailed analysis or create additional alert rules to proactively notify of critical issues.

AZURE ADVISOR

[Azure Advisor](#) constantly monitors the resource configuration and usage telemetry. It then provides personalized recommendations based on best practices.

SERVICE HEALTH

[Azure Service Health](#) identifies any issues with Azure services that might affect the application. Service Health also helps plan for scheduled maintenance.

ACTIVITY LOG

Activity Log provides data about the operation of an Azure resource. This information includes:

- Configuration changes to the resource
- Service health incidents
- Recommendations on better utilizing the resource
- Information related to autoscale operations

View logs for a particular resource on its page in the Azure portal. Or view logs from multiple resources in Activity Log Explorer. Or send activity log entries to Log Analytics to analyze the logs by using data collected by management solutions, agents on virtual machines, and other sources.

APPLICATION INSIGHTS

Use [Azure Application Insights](#) to monitor availability, performance, and usage of the application, whether it's hosted in the cloud or on-premises. Quickly identify and diagnose errors without waiting for a user to report them. Application Insights has extensive tools for interacting with the data that it collects. It stores its data in a common repository and takes advantage of shared functionality such as alerts, dashboards, and deep analysis with the Log Analytics query language.

LOG ANALYTICS WORKSPACES

[Log Analytics](#) workspaces play a central role in Azure monitoring by collecting data from a variety of resources (including non-Microsoft tools) into a single repository to analyze the data with a powerful query language.

Application Insights and Azure Security Center store their data in the Log Analytics data store and use its analytics engine. Data is also collected from Azure Monitor, management solutions, and agents installed on virtual machines in the cloud or on-premises.

NETWORK MONITORING

There are several tools that work together to monitor various aspects of the network, whether in Azure or on-premises.

- [Network Watcher](#) provides scenario-based monitoring and diagnostics for different network scenarios in Azure. It stores data in Azure metrics and diagnostics for further analysis.
- [Network Performance Monitor \(NPM\)](#) is a cloud-based network monitoring solution that monitors connectivity across public clouds, datacenters, and on-premises environments.
- [ExpressRoute Monitor](#) is an NPM capability that monitors the end-to-end connectivity and performance over Azure ExpressRoute circuits.
- [DNS Analytics](#) is a solution that provides security, performance, and operations-related insights, based on DNS servers.
- [Service Endpoint Monitor](#) tests the reachability of applications and detects performance bottlenecks across on-premises, carrier networks, and cloud/private data centers.

SERVICE MAP

[Service Map](#) provides insight into an IaaS environment by analyzing virtual machines with their different processes and dependencies on other computers and external processes. It integrates events, performance data, and management solutions in Log Analytics to view this data in the context of each computer and its relation to the rest of the environment.

Service Map is similar to [Application Map in Application Insights](#). It focuses on the infrastructure components that support the applications

Multi-tenant management

Azure Lighthouse

Azure Lighthouse enables cross- and multi-tenant management, allowing for higher automation, scalability, and enhanced governance across resources and tenants.

With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust management tooling built into the Azure platform. Customers maintain control over who can access their tenant, what resources they can access, and what actions can be taken.



Benefits

- **Management at scale:** Customer engagement and life-cycle operations to manage customer resources are easier and more scalable. Existing APIs, management tools, and workflows can be used with delegated resources, including machines hosted outside of Azure, regardless of the regions in which they're located.
- **Greater visibility and control:** Customers have precise control over the scopes they delegate for management and the permissions that are allowed. They can audit service provider actions and remove access completely if desired.
- **Comprehensive and unified platform tooling:** Addresses key service provider scenarios, including multiple licensing models such as EA, CSP, and pay-as-you-go. Azure Lighthouse works with existing tools and APIs, licensing models, Azure managed applications, and partner programs such as the [Cloud Solution Provider program \(CSP\)](#). Integrate Azure Lighthouse into existing workflows and applications, and track the impact on customer engagements by linking the partner ID.

There are no additional costs associated with using Azure Lighthouse to manage Azure resources. Any Azure customer or partner can use Azure Lighthouse.

Capabilities

- **Azure delegated resource management:** [Manage customers' Azure resources](#) securely from within a tenant without having to switch context and control planes. Customer subscriptions and resource groups can be delegated to specified users and roles in the managing tenant, with the ability to remove access as needed.
- **New Azure portal experiences:** View cross-tenant information in the [My customers page](#) in the Azure portal. A corresponding [Service providers page](#) lets customers view and manage their service provider access.
- **Azure Resource Manager templates:** Use ARM templates to [onboard delegated customer resources](#) and [perform cross-tenant management tasks](#).
- **Managed Service offers in Azure Marketplace:** [Offer services to customers](#) through private or public offers, and automatically onboard them to Azure Lighthouse.

Management in any environment

Today, companies are struggling to control and govern an environment that becomes more and more complex.

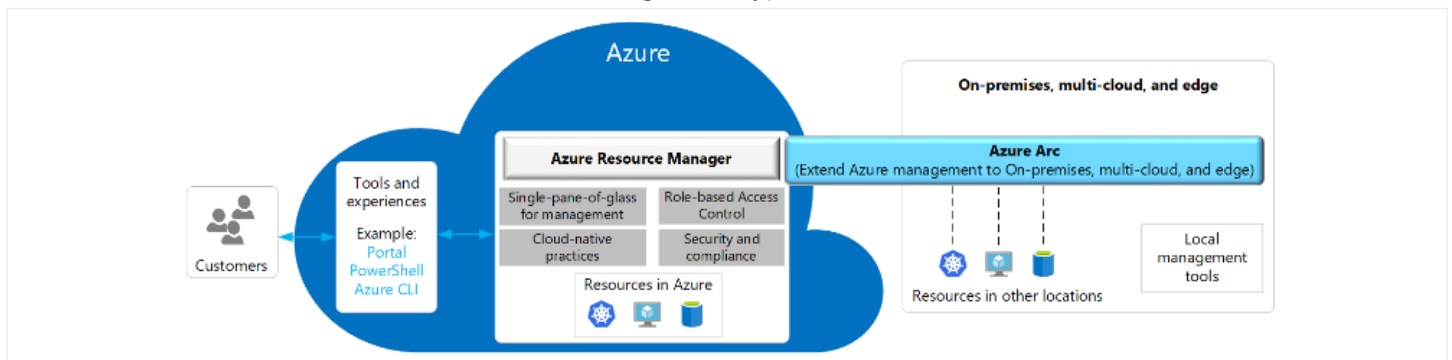
These environments extend across data centers, multiple clouds, and edge. Each environment and cloud has its own set of disjointed management tools. In parallel, new DevOps and ITOps operational models are hard to implement, as existing tools fail to provide support for new cloud native patterns.

Azure Arc

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform. Manage the entire environment with a single pane of glass by projecting the existing resources into Azure Resource Manager. Manage virtual machines, Kubernetes clusters, and databases as if they are running in Azure. Continue using traditional ITOps while introducing DevOps practices to support new cloud native patterns in the environment.

Today, Azure Arc can manage the following resource types hosted outside of Azure:

- Servers: both physical and virtual machines running Windows or Linux
- Kubernetes clusters: supporting multiple Kubernetes distributions
- Azure data services: Azure SQL Database and PostgreSQL Hyperscale services



KEY FEATURES OF AZURE ARC:

- Implement consistent inventory, management, governance, and security for servers across the environment,
- Configure Azure VM extensions to use Azure management services to monitor, secure, and update servers.
- Manage and govern Kubernetes clusters at scale.
- Use GitOps-based configuration as code management to deploy applications and configuration across one or more clusters directly from source control, such as GitHub.
- Zero touch compliance and configuration for Kubernetes clusters using Azure Policy.
- Run Azure data services on any Kubernetes environment, specifically Azure SQL Managed Instance and Azure Database for PostgreSQL.
- Hyperscale, with benefits such as upgrades/updates, security, and monitoring as if it runs in Azure.
- Leverage elastic scale, apply updates, without any application downtime, even if it doesn't have a continuous connection to Azure.
- A unified experience viewing Azure Arc enabled resources whether using the Azure portal, the Azure CLI, Azure PowerShell, or Azure REST API.

Azure Arc includes the following control plane functionality at no additional costs:

- Resource organization through Azure management groups and tags.
- Searching and indexing through Azure Resource Graph.
- Access and security through Azure RBAC and subscriptions.
- Environments and automation through templates and extensions.
- Update management.

Any Azure service that is used on Arc enabled servers will be charged as per the pricing for that service. For more information, see [Azure pricing page](#).

Currently in preview, Azure Arc enabled Kubernetes as well as Azure Arc enabled data services are offered at no additional costs.

Automated management of virtual machines

Azure Automanage (preview)

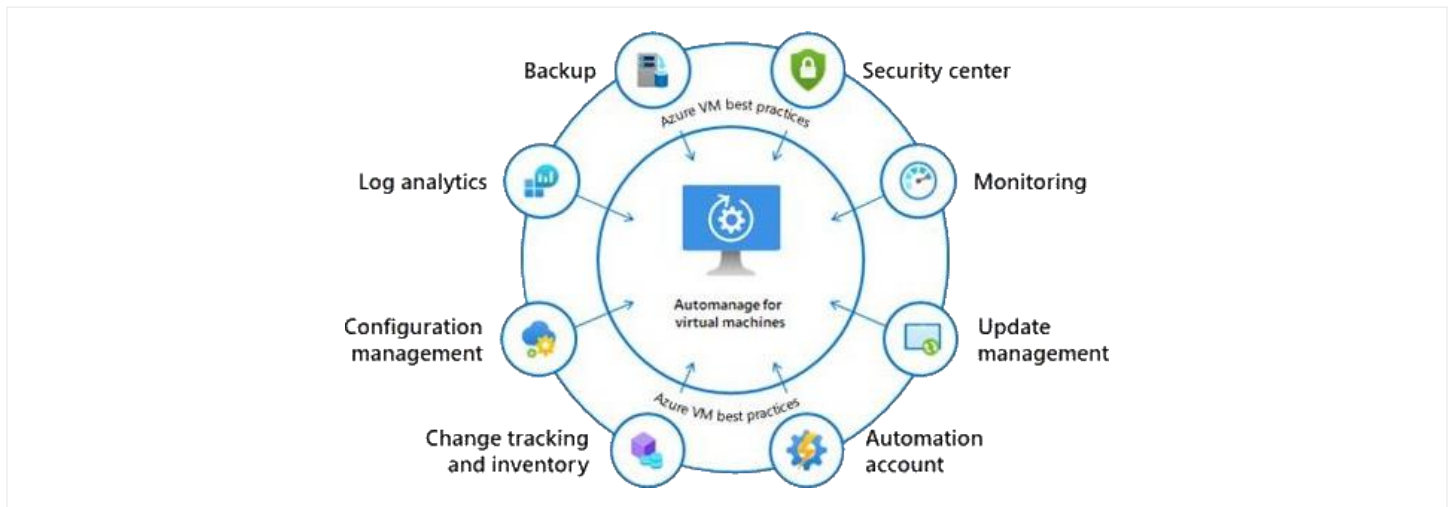
Azure Automanage for virtual machines is a service that eliminates the need to manually discover, onboard, and configure certain services in Azure. These services help enhance reliability, security, and management for virtual machines.

After onboarding virtual machines to Azure Automanage, it automatically configures best practice services to their recommended settings. Best practices are different for each of the services. An example might be Azure Backup, where the best practice might be to back up the virtual machine once a day and have a retention period of six months.

Azure Automanage also automatically monitors for drift and corrects for it when detected. This means that a virtual machine onboarded to Azure Automanage will be configured per Azure best practices and monitored to ensure that it continues to comply with those best practices across its entire lifecycle. If the VM does drift or deviate from those practices, it can be pulled back into the desired state.

Participating services

The following services participate in Azure Automanage and are automatically onboarded as part of the service. They are essential to the best practices found in the [Cloud Adoption Framework](#).



For a updated list of services including their supported configurations, see [Azure Automanage for Virtual Machines Best Practices](#).

Support and incident management

Supporting an Azure estate includes interactions with Microsoft. Here are the Partner options for engaging Microsoft support strategies for streamlining customer support.

Engaging support

COMMERCIAL SUPPORT

Microsoft offers several options via forum support or via paid options. Basic support services are included with every Azure subscription. This includes 24x7x365 access to Microsoft customer service, documentation, whitepapers, and support forums.

Considerations for the selection of a support model include the underlying requirements for basic needs like an SLA for response from Microsoft and the criticality of the workloads. Microsoft offers four support plans for Azure above the Basic tier:

- **Developer:** Suitable for trial and non-production environments.
- **Standard:** Suitable for non-critical production environments.
- **Professional Direct:** For critical production workloads.
- **Premier:** For customers who need support beyond Azure and have a substantial dependence across multiple Microsoft products.

The Developer support plan only includes business hours access to support, while the other plans include 24x7 access. Also consider the response times for different case severities. Microsoft [classifies severity](#) at three levels:

- **Severity A** for issues that involve a significant loss or degradation of services and require immediate attention.
- **Severity B** for issues which exhibit a moderate loss or degradation of services, but work can continue in a reasonable manner.
- **Severity C** for issues which have a minimal impact and only light impediments to service.

If it's likely that support cases will be opened with a Severity A or Severity B, select a Standard support plan or higher. Developer support plans do not include a response SLA for anything above a Severity C issue.

there is no mention of an SLA for how quickly an issue will be resolved under any support plan. This is by design as the time it takes to troubleshoot and resolve an issue in Azure can vary widely based on the specifics of the issue. Microsoft does commit to working to resolve each issue as fast as possible.

CSP SUPPORT

For CSPs or those who have sold support as part of their managed services solution, they are the front-line support for the customer. Azure CSP direct partners will provide all technical and account support services for their customers. This means many things, including:

- Describing the capabilities of different Azure services
- Providing answers to Azure pricing and usage questions.
- Providing billing and subscription support.
- Providing provisioning and deployment help.
- Resolving performance problems, service availability problems, incomplete software integration problems, or other deployment problems.

For Azure CSP indirect resellers, the responsibilities noted above are shared an Azure CSP indirect provider.

CSPs must provide customers with a clear description of how they will receive support, and that description must include an SLA. Keep this in mind when considering the [Azure CSP support plans](#).

The Azure CSP support plans use the same severity classification system as commercial support plans with the response SLA dictated by the support level purchased. All CSP direct partners have access to an included support plan or can optionally purchase a deeper level of support through the [Advanced Support for Partners \(ASfP\)](#) or the [Premier Support for Partners \(PSfP\)](#) plans.

Since customers cannot directly contact Microsoft for support, it is critical that to keep the organizational profile in the Partner Center updated. Specify the correct email and phone number for the helpdesk and if there is a ticket management system or other ITSM system, provide a link to the page where customers can submit a support a request.

Incident management

KNOWLEDGE MANAGEMENT

Building a knowledge base for the support staff and engineers is the first line of defense in addressing common customer issues and being able to fix issues quickly. A good knowledge base will integrate directly with the ITSM tooling.

The support, engineering, and operations team should all be encouraged to contribute to the knowledge base, and custom solutions for customers should always be documented in some fashion.

IT SERVICE MANAGEMENT (ITSM) TOOLS

Consider using ITSM tools which integrate directly with Azure services such as Azure Log Analytics and Azure Monitor. Leverage compatible tools to have bi-directional connectivity between the customer's Azure environment and the ITSM tooling.

The [IT Service Management Connection \(ITSMC\)](#) can be used to integrate a Log Analytics workspace with the following ITSM tools:

- ServiceNow
- System Center Service Manager
- Provance
- Cherwell

Another primary benefit of adopting an ITSM tool will be having the ability to offer customers self-service tools, including dashboards, reports, and the ability to create self-service requests. Self-service also includes the ability to notify customers of issue status and inform them of resolution when required.

HEALTHY SUPPORT CULTURE

An unhappy support staff will be known to customers and have a detrimental impact on the ability to deliver quality services. Be open to soliciting feedback from the support staff on where improvements can be made. Perform regular reviews of the workflows, escalation paths, and interaction metrics.

Also consider building post-mortems directly into the service delivery. This gives the staff an opportunity to improve over time and with a measured cadence.

Implementing these types of activities into the service delivery organization from the start will create a culture where staff members are open to learning from each other and where transparency is just the way it is.

Automation and DevOps

DevOps brings together people, processes, and technology, automating software delivery to provide continuous value by delivering software faster and more reliably.

AUTOMATE APPLICATION DEPLOYMENT AND DELIVERY

Azure supports a rich set of tools for going beyond the configuration and management of virtual machines, with tooling that brings automated builds and deployment, continuous integration, and testing into the DevOps lifecycle.

CONTINUOUS INTEGRATION (CI)	CONTINUOUS DEVELOPMENT (CD)	CONTINUOUS DEPLOYMENT WITH CI/CD
Take advantage of continuous integration to improve software development quality and speed. By using Visual Studio Team Services or Jenkins to build apps in the cloud and deploy to Azure, each time code is committed, it is automatically built and tested, so bugs are detected faster.	Ensure that code and infrastructure are always in a production-deployable state, with continuous delivery. Combining continuous integration and infrastructure as code (IaC) can achieve identical deployments and the confidence to manually deploy to production at any time.	With continuous deployment, partners can automate the entire process from code commit to production if the CI/CD tests are successful. Use CI/CD practices, paired with monitoring tools to safely deliver features to customers as soon as they're ready.

Deployment strategies

While deployment of code through continuous integration and deployment tools often comes to the forefront with DevOps, there is a precursor, and that is the automated deployment of the infrastructure (or infrastructure as code).

INFRASTRUCTURE AS CODE

Infrastructure as code (IaC) is the process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

Source: https://en.wikipedia.org/wiki/Infrastructure_as_Code

The primary goals of adopting Infrastructure as Code (IaC) are:

- **Cost reduction:** By focusing on automation, partners can invest staff time in the development and execution of repeatable processes.
- **Faster execution:** With repeatable processes, the time to execute builds drastically decreases and the time to provision resources becomes a known quantity.
- **Risk mitigation:** With a well-known and tested declarative provisioning model, be confident that the environments will be deployed the right way, the first time, reducing risk through manual intervention.

IaC ultimately leads us to a declarative provisioning model, where we define *what* we are going to provision. We then can use imperative provisioning to control *how* that infrastructure is configured.

Regardless of the technology, partners should have the ability to repeatedly deploy a solution throughout its lifecycle and have confidence it is deployed in a consistent state.

AZURE RESOURCE MANAGER TEMPLATES

[Azure Resource Manager \(ARM\) templates](#) can be used to create declarative JSON files that define the Azure infrastructure and the configuration of Azure resources. When an Azure resource is deployed through the Azure Portal, a template can be generated for later re-use. Microsoft maintains a GitHub repository with hundreds of [QuickStart Templates](#).

TERRAFORM

[Hashicorp Terraform](#) is an open-source tool for provisioning and managing cloud infrastructure. Much like ARM, it is used to create text-based templates called Terraform configurations to author the infrastructure and define its configuration. Configurations in Terraform follow a known syntax – the [Hashicorp Configuration Language \(HCL\)](#). Terraform can also recognize JSON files, and supports nesting in existing ARM templates.

There are several scenarios where Terraform may work best:

- Staff members have existing expertise in Terraform and can reuse their existing skills while they get up-to-speed on Azure.
- Terraform has multi-cloud support for customers not exclusively using Azure, Terraform can provide a consistent deployment model.

Microsoft has [invested deeply in the Terraform experience on Azure](#) is committed to bringing latest Azure resources to Terraform and ensuring Hashicorp can support them.

Microsoft has also announced a dedicated [Azure Terraform Resource Provider](#), which will allow partners and customers to provision Azure resources with native Terraform providers, deepening the integration between ARM and Terraform.

ANSIBLE

[Ansible](#) is an open-source product that automates cloud provisioning, configuration management, and application deployments. Ansible can provision virtual machines, containers, network infrastructures, and complete cloud infrastructures. In addition, Ansible can help automate the deployment and configuration of resources in the environment.

Like Azure Resource Manager templates and Terraform, Ansible playbooks are authored in YAML which define how resources in Azure are deployed and configured.

Ansible ships with modules that can be executed directly on remote hosts or through playbooks. There are modules available specifically for Azure, with coverage for resources across compute, storage, networking, databases, containers, and even PaaS services such as Azure Web Apps, and Azure Traffic Manager. To learn more, see [Ansible module and version matrix](#).

DEVOPS LIFECYCLE

Now it is time to think about how to integrate that code into an existing software development lifecycle (SDLC) and the DevOps lifecycle. This includes storing the templates and scripts in a source control repository, where a single version of truth can be maintained. All team members who need to interact with this code should have access to the repository with appropriate roles and rights. Also consider providing staff an area where they can develop and test these assets by deploying their own version of the defined infrastructure.

Managing the code in a repository means there will be a full audit trail of the infrastructure, showing who changed what, when, and why. Consider integrating the commits and check-ins of these infrastructure resources into a wider continuous delivery methodology using the tools mentioned below.

Deploying code

AZURE DEVOPS PROJECTS

[Azure DevOps Projects](#) presents a simplified experience for bringing existing code and Git repository (or choose from one of the sample applications) to create a Continuous Integration (CI) and Continuous Delivery (CD) pipeline to Azure. DevOps Projects has step-by-step tutorials for creating [Azure Pipelines](#) with many popular Azure services.

After creating a DevOps Project, developers can:

- Customize the build and release pipeline.
- Use pull requests to manage the code flow and keep the quality high.
- Test and build each commit before they merge the code to raise the quality bar.
- Track the backlog and issues right along with the application.

AZURE DEVOPS SERVICES

[Azure DevOps Services](#) (formerly [Visual Studio Team Services](#)) offers a platform to perform continuous integration and continuous delivery (CI/CD), source code repository hosting, workstream tracking, automated testing solutions, and package hosting for package feeds.

The services within Azure DevOps are:

- **Azure Pipelines:** Continuous integration and continuous delivery (CI/CD) that works with any language, platform, and cloud.
- **Azure Repos:** Unlimited cloud-hosted private Git and Team Foundation Version Control (TFVC) repos.
- **Azure Boards:** Work tracking with Kanban boards, backlogs, team dashboards, and custom reporting.
- **Azure Test Plans:** An all-in-one planned and exploratory testing solution.
- **Azure Artifacts:** Maven, npm, and NuGet package feeds from public and private sources.

Azure Pipelines is available as an individual service while the other services are purchased as a part of Azure DevOps.

JENKINS

[Jenkins](#) is a continuous integration server that helps deploy and test applications and create automated pipelines for code delivery. There are hundreds of plugins to extend the core Jenkins platform and integrate with many other products and solutions through webhooks. Jenkins can be manually installed on an Azure VM, run from within a Docker container, or use a pre-built Azure Marketplace image.

DevOps and containers

As customers adopt containers and container orchestrators such as Kubernetes there is a need to manage not only the orchestrator and the underlying container cluster resources with a service such as [Azure Kubernetes Service \(AKS\)](#), but also the lifecycle of containerized applications.

HELM

[Helm](#) is an open-source packaging tool that helps install and manage the lifecycle of Kubernetes applications. Like Linux package managers such as APT and Yum, Helm is used to manage Kubernetes charts, which are packages of preconfigured Kubernetes resources. To learn more about how to use Helm and Helm charts with AKS, see [Install applications with Helm in Azure Kubernetes Service \(AKS\)](#).

BRIGADE

[Brigade](#) is a Kubernetes-native tool for performing event-driven scripting directly in a Kubernetes cluster. Because Brigade runs within the Kubernetes cluster, there are no additional hosts to manage to leverage Brigade for CI/CD or general scripting of automation within a Kubernetes cluster. Because Brigade is built directly on Kubernetes APIs, it is supported in AKS.

The deployment of Brigade can also be orchestrated and managed with Helm and it integrates with developer workflows with tools like Draft. Brigade is also approachable for most developers, as configurations are authored in JavaScript

Brigade can not only be used for managing long running services, but it also makes it easy to leverage a Kubernetes cluster for any short-lived task such as batch processing, code quality testing, or any other event-driven programming.

Continuous integration/continuous deployment

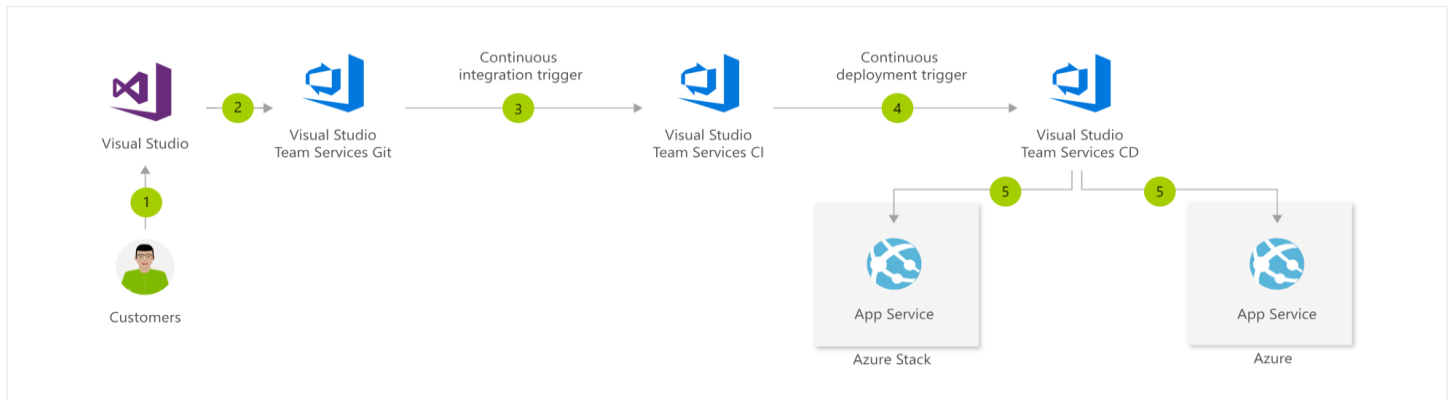
Building a rich pipeline for continuous integration and continuous deployment is an excellent way to add value by demonstrating an ability to execute advanced deployment scenarios.

Most organizations will approach their cloud deployments as singular entities, forgetting they can integrate even on-premises environments and existing applications into these pipelines.

Consider a customer that has an Azure App Service that they want to run on-premises in Azure Stack and in the Azure public cloud. Engineers can define the entire environment declaratively in one or more ARM templates. Azure Stack shares a common API surface with Azure, so the same template can be reused across hybrid environments. After the template is developed and tested, it is checked into Visual Studio Team Services (VSTS) where it can automatically be tested through continuous integration with application build and unit tests.

After the build passes its tests, VSTS will trigger a continuous deployment to orchestrate the deployment of the ARM template and the web app code to both environments, passing in environment specific parameters at the time of deployment.

In just a few steps, partners can empower their engineers and customers to deploy to multiple environments in a repeatable, testable, and known way.



For more examples of what can be accomplished with CI/CD and Azure, visit the [Azure Solution Architecture Center](#).

Key contracts and practice tools

Partners will require a complete set of legal documents to drive compliance, protect their IP, and produce consistent engagement deliverables. They also need a documented process to monitor project progress, in terms of both the project plan and budget.

KEY CONTRACTS

Leverage the [Key Contracts for Practice guide](#) to learn more about developing service level agreements, master services agreements, a statement of work, and a mutual non-disclosure agreement.

MICROSOFT TEAMS

[Microsoft Teams](#) should be used for every project for collaboration. Create a team for each project and invite the customer in as a guest user to collaborate and track the project. Build as much as possible into that team to demonstrate the value and expandability of Teams. The lifecycle of a project or duration of a managed services agreement is critical, especially when leveraging the technology and services they are selling them.

MICROSOFT PROJECT ONLINE

[Microsoft Project Online](#) is a flexible online solution for project portfolio management (PPM) and everyday work. Project Online provides powerful project management capabilities for planning, prioritizing, and managing projects and project portfolio investments—from almost anywhere on almost any device. Project Online can be used by administrators, portfolio managers and viewers, project and resource managers, and team leads and members.

AZURE DEVOPS

[Azure DevOps](#) provides various tools for tasks like running agile teams, providing support for Kanban boards, handling work item backlogs, scrum boards, source control, continuous integration, and release management. Source control functionality provides Git support, which enables integration with GitHub if such integration is desired. While Azure DevOps helps to manage the technical aspects of a project, cost-containment requires a different set of tools.

GITHUB

[GitHub](#) provides the hosted environment for the business application implementation team to version control and share their source code, notebooks and other artifacts both privately (e.g., internally to a team) and publicly (e.g., an open source project), and collaborate on development projects.

OTHER COLLABORATION TOOLS AND FILE SHARING

[Yammer](#) is an enterprise social network collaboration offering to help teams collaborate and share files with each other.

[OneDrive for Business](#) is an enterprise file sharing service that is designed for automatic synchronization of files between their computer and the cloud. OneDrive makes it easy to share files with their customers or partners.

[Microsoft Dynamics 365 for Project Service Automation](#) provides users with the capabilities required for setting up a project organization, engaging with customers, project scheduling and costing, managing and approving time and expenses, and closing projects. It is specially targeted to address the needs of a project services-based practice, as it is designed for professionals who manage projects and the associated customer engagement process end-to-end.

[Microsoft Surface Hub](#) is a Teams-integrated collaborations device, or “meeting room in a box.” In addition to the built-in team experiences like Teams, Microsoft Office, and Whiteboard, Microsoft Surface Hub is customizable with a wide array of applications. Universal apps built for Windows 10 shine on Microsoft Surface Hub, and scale to the large screen. They can also connect apps from their personal device and drive them from Microsoft Surface Hub.



Go-To-Market and Close Deals

Cloud Infrastructure



Microsoft
Partner
Network

aka.ms/practiceplaybooks

Introduction

Discover strategies to compel potential customers that may be sitting on the fence to buy, from creating a good value proposition to building marketing and sales materials that tell the story.

Get started by building foundational marketing materials such as marketing personas, points of differentiation, value propositions, and customer business needs. Then learn how to put those materials to work.

Discover best practices for attracting new customers and see how successful partners put it all together? Learn why integrated marketing campaigns work the best, and the tools needed to run them, such as a CRM system and marketing automation.

See how the marketing and sales teams work together and what marketing can do to support sales. The job of the marketing team is to build out not only customer-facing materials, but also compelling materials that can be used to train and arm their sales team.

The sales end of the bargain is to close the sale. One way to do this is by writing a winning proposal. Another way is to build a proof of concept or prototype of the product or service offering, which could help a prospect understand the offering or solidify their vision of what is possible. Microsoft is committed to helping partners businesses grow and provides both co-selling and co-marketing opportunities.

Go-To-Market and Close Deals Guide

Leverage the Microsoft resources available in the [Go-To-Market and Close Deals guide](#), for these additional sections:

MARKETING TO THE CLOUD BUYER

Technology buyers buy differently than in the past. By the time they engage with sales, they have already made some decisions.

ALIGN MARKETING GOALS WITH BUSINESS GOALS

What should the marketing efforts try to accomplish?

CREATING MARKETING FOR EVERY PHASE OF THE JOURNEY

Messaging and content should be available at each stage of the customer journey.

MARKETING TACTICS

Understand strategies for websites, SEO and SEM, social media, email, blogs, and webinars.

SALES

Find selling tips, sales training materials, best practices, sales incentives, and sales compensation advice.

CLOSING THE SALE

Write winning proposals and negotiate the offer.

Marketing is the toolset that addresses all these changes. Marketing today is digital and has the power to reach more people. Again, it is not to say that more traditional, non-digital marketing is ineffective. But to be found by prospective buyers with no prior relationship, employ digital marketing techniques. Modern marketing is focused on the prospects' and clients' views of the world.

Identify potential customers

Build the list of prospects that could potentially turn into customers with an awareness campaign and use past deployment success to earn additional business. Use these awareness activities to help generate new customers:

WEBINARS AND PODCASTS

A great way to transfer knowledge, establish a practice as an expert, and pique the interest of potential customers.

REFERRALS

Ask for referrals in email and phone calls when talking with existing customers, partners, and vendors who might know someone who is ready for similar services.

WHITE PAPERS

These are a great way to build credibility with decision makers with thought leadership and technical information. Technical staff often expect a white paper to help them understand underlying architecture and technology.

NEWS ARTICLES

Leverage public relation efforts to drive publicity around the technology, market activities, and other topics of current interest.

SOCIAL MEDIA

Social media such as Twitter, LinkedIn, etc., is a place to build awareness, reputation, and customer satisfaction — and gain new customers.

REVISIT EXISTING CUSTOMERS

When offering a new practice within an existing business, the easiest way to acquire new customers is to introduce the practice to existing customers.

Engage existing customers

As always, the best potential customers are existing customers. When relationships are good, customers are more open to ideas for helping improve their business processes. To start, dig deep into their needs, challenges, business objectives, and priorities. Then work with them to create a vision that combines tactical projects with strategic initiatives that include a clear definition of customer experience goals.

Partners that have done this recommend starting this conversation with a planning engagement that builds confidence that there is a way forward and what it might look like. Ask big picture questions. For example, ask the customer *"If one of your staff wanted to go into competition with you, what could they do to disrupt your business?"* Help executive-level leadership realize the vision and its potential, and how it can help fill their technical and business gaps.

PROVIDE CUSTOMER LIFETIME VALUE

Lifetime value does not happen without a plan. Map out the cloud journey in collaboration with the customer. What should they do first? Where will they be in two, three or five years? With a plan in hand, work with the customer to make potential business benefits a reality. Everything does not need to happen at once, but it does need to happen in a thoughtful and logical way. Always be thinking about what is next. Would complementary or incremental functionality be a good fit at the customer's stage in cloud maturity?

The digital partner of record on the customer's Microsoft subscriptions has access to their cloud solution usage and consumption data via the Cloud Services Partner Dashboard. Use it to identify where to encourage deeper and wider usage, as well as areas where the customer may benefit from incremental project or advisory services. For example, if SharePoint usage is low, try launching an outreach campaign about best practices in organizing projects and teams.

Consultative selling and technical pre-sales

Discovering the art of the possible

More than ever before, technical staff are a part of the decision-making process as they help envision a solution to solve a customer need.

The technical pre-sales staff should be very experienced users of the products and services. For that reason, former support employees often make good technical pre-sales staff. The technical pre-sales staff is in place to explain technology, how it works, how it meets a business need and to answer any other questions. They should excel at the more complex issues that come from prospects, and be focused on pre-sales, working together with sales and marketing, who address the business benefits. One without the other cannot be effective.

Examples of technical probing questions to ask during pre-sales conversations supporting cloud infrastructure, migration and modernization, and operations and management:

- What are your thoughts on your current application environment? How would you describe how you manage and maintain your global infrastructure?
- What does your ideal operation strategy look like?

BEST PRACTICES – CONSULTATIVE SELLING

- Combine solution selling with insights. To gain credibility in the eyes of the buyer, the solutions sales rep must introduce content and data that adds value to the sales call.
- Ask good questions. The successful solutions seller remains sensitive to the buyer's needs and asks important questions at the right moment.
- Listen actively. Solution selling requires considerable understanding of the buyer's needs, which will only come from listening attentively. Solution sellers should actively listen as the buyer details their organizational needs, taking notes and asking considerate questions in the process.

Offer guidance. Solution sellers must guide the buyer towards the solution being offered. This guidance comes as the solution seller adopts something of a teaching role, helping the buyer to overcome business challenges by utilizing their deep knowledge of industry pain points and trends.

Discovery

The goal of the discovery phase is to fully understand the existing infrastructure and applications, and the business context and goals surrounding those applications and their move to the cloud. This informs the planning and evaluations phases which follow.

It is important to understand how each application contributes to the business. What does it do? Who uses it? What is the impact of an outage? How important is business continuity and business assurance to the workloads being migrated? Placing the existing applications in their business context is essential to making informed decisions regarding prioritization, design, and indeed every aspect of the migration project.

Equally important is an understanding how customers use the application. In some cases, cloud migration will be a seamless change, of which users will be unaware. In other cases, users may experience significant changes, and may need to access applications differently, or perform specific tasks in new ways. To help customers embrace rather than resist this change, it's important to understand the user experience, and to keep the customer informed and engaged throughout the migration process.

Existing pain points (such as reliability, performance, or issues with functionality) should be identified. Migration to cloud is often an opportunity to reduce or remove such problems. These kinds of positive changes make it easier to get buy-in from both decision-makers and end users.

Non-functional requirements, such as reliability, performance, and forecasted scale must be understood so they can be factored into the design. The cloud offers far greater flexibility than on-premises infrastructure and is therefore able to adapt quickly to changes in demand. Even so, some requirements—such as very high availability delivered through redundancy across more than one Azure region—have design and cost implications that need to be captured up-front.

Likewise, security and compliance requirements must be captured. Azure supports an extremely wide range of compliance certifications spanning many international, national, and industry-specific standards. Delivering an application that is compliant with a specific set of standards requires that the design be reviewed against the Azure guidance for those standards.

Of course, the discovery phase must also capture the details of the existing application implementation. The hardware, network, and storage infrastructure must be documented. It is important to capture the actual usage as well as the physical specifications. Traditional infrastructure is often over-provisioned to handle expected future demand or worst-case scenarios. The agility and elastic scale of the cloud offers the opportunity to optimize significantly on this approach. Usage should be measured at both normal and peak expected load. Data should be gathered on CPU, memory, network (latency and bandwidth) and storage (capacity, IOPS and throughput).

Any dependencies between components and systems, such as between applications and databases, must be identified and mapped. Understanding these dependencies is important when grouping and sequencing migrations during the planning phase.

Capture the current version of all software, and all operating systems—in some cases, updating the software to more recent, supported versions may be required as a pre-requisite to migration. Where software is developed in-house, the availability of source code and skilled staff familiar with the code must be established. Where software is licensed, vendor support for cloud technologies must be understood. For example, does the vendor already offer a cloud-based version of the software? If the software uses Microsoft SQL Server, has the vendor certified use with Azure SQL Database?

UNDERSTAND THE TOTAL COST OF OWNERSHIP

Having mapped the existing infrastructure and applications, the total costs of delivering those applications can then be analyzed. The [Azure Total Cost of Ownership \(TCO\) calculator](#) can help estimate on-premises costs but cannot capture all costs such as 3rd-party software licenses. Building a complete business case for the cloud requires building a full view of these costs. Some costs, such as servers and software licensing, are specific to each application; other costs such as operations staff and buildings are spread across applications and therefore may need to be apportioned appropriately. Remember to include backup, disaster recovery, software licensing, power, space, operations staff, support agreements, networking equipment, warranties, and Internet access. It is also important to understand the renewal dates for any leasing, licensing, warranty or support agreements, and the refresh cycle for all hardware, since this may create hard deadlines for migration, or impact prioritization to better leverage existing assets.

DISCOVERY TECHNIQUES AND TOOLS

A variety of methods must be employed to gather all this information. First, it is important to identify key stakeholders, such as application owners, relevant executives, technical staff, and end users. Interviews with each stakeholder will be necessary to understand their perspectives and priorities, and to gather their input on the topics listed above.

Various tools are also available to assist with gathering technical data on the existing infrastructure. In many cases, these tools can also help with the subsequent migration planning, costing, and even with the migration execution.








One such tool, CAST Highlight from [CAST Software](#) helps quickly assess migration readiness of an entire application portfolio. It segments and prioritizes applications using the company's "Cloud Ready Index" metric that measures specific patterns in source code that could block or accelerate a cloud migration. Users can visualize application dependencies that could break migration, detect all open-source components in use and their associated risk. The cloud readiness assessment performed by CAST Highlight can automatically build an objective migration roadmap across hundreds of applications in just days.



In addition, CAST provides an architectural blueprint capability in its CAST Imaging tool to analyze all application components and their dependencies to transform apps into microservices. It can be used to reverse-engineer any database structures, code components and interdependencies to create accurate architecture blueprints.

Examples of other available tools, from both Microsoft and third-party vendors, include:

MICROSOFT OFFERINGS	
	<p>Azure Migrate: The Azure Migrate tool can be used to assess on-premises workloads for suitability, as well as offering advice on performance-based VM sizing and cost estimations. The initial release of Azure Migrate only supports assessment for VMware VMs. Support for Hyper-V assessment and VMware migration is coming soon. Azure Migrate offers the following capabilities:</p> <ul style="list-style-type: none"> • Discover and assess on-premises VMs • Confidently plan the migration • Easily migrate customer workloads to Azure <p>More resources:</p> <p>Assess on-premises workloads for migration to Azure</p> <p>Watch a Demonstration of Azure Migrate</p> <p>Azure Migrate hands-on lab</p>
	<p>Azure App Service Migration Assistant: The Azure App Service Migration site is a dedicated site to support migrating application to Azure App Service. For Internet-facing sites, an online assessment provides an initial migration compatibility report in seconds.</p> <p>Then download the App Service Migration Assistant for an in-depth assessment of both on-premises and Internet-facing applications, and automated migration of most modern ASP.NET applications.</p>
	<p>Azure Database Migration Service: The Azure Database Migration Service is a fully managed service designed to enable seamless migrations from multiple database sources to Azure Data platforms with minimal downtime.</p>
	<p>SQL Server Data Migration Assistant (DMA): Upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in a new version of SQL Server and Azure SQL Database. DMA recommends performance and reliability improvements for the target environment and moves the schema, data, and uncontained objects from the source server to the target server.</p>
	<p>Azure SQL Database DTU Calculator: A Database Transaction Unit (DTU) is a blended measure of CPU, memory, and I/O used by an Azure SQL Database. Within each SQL Database service tier, Microsoft guarantees performance in terms of DTUs. The SQL Database DTU Calculator can be used to analyze the performance of existing on-premises databases, to calculate the number of DTUs (and hence service tier) required after migration to Azure SQL Database.</p>
	<p>Virtual Desktops: Assess the on-premises virtual desktop infrastructure (VDI) and migrate it to Azure Virtual Desktop.</p>
	<p>Data: Migrate large amounts of data to Azure quickly and cost-effectively using Azure Data Box products.</p>

THIRD-PARTY OFFERINGS

	<p>Turbonomic</p> <p>Turbonomic plans reflect what the workloads need to run in the cloud—no more, no less. Get to the cloud quickly and safely, while avoiding cost-overruns or performance issues.</p>
 	<p>Cloudamize</p> <p>The Cloudamize cloud infrastructure analytics platform helps make data-driven decisions with ease and confidence throughout the entire cloud journey.</p> <ul style="list-style-type: none"> • Assess: Which cloud is right for me and what will it cost? • Plan: How do I prioritize my applications for migration? • Migrate: How do I ensure my migration execution is right on the first try? <p>CAST Highlight</p> <p>Quickly assess migration readiness of an entire application portfolio in days instead of weeks. Segment and prioritize applications to migrate using the “Cloud Ready Index” to measure patterns and dependencies that could block or accelerate a cloud migration and build a migration roadmap across hundreds of applications.</p>
	<p>Movere</p> <p>More than just a point-in-time assessment, Movere enables a depth of monitoring, analysis and optimization unseen in any other platform. Movere organically scans environments globally at a rate of up to 1,000 servers per hour and multiple instances/environments in less than one day.</p>
	<p>RISC Networks</p> <p>RISC Networks CloudScape provides IT professionals with the most relevant infrastructure performance analysis needed to properly prepare for cloud, data center, and infrastructure projects. Agentless discovery of Network Devices, routers, switches, Windows and Linux Servers and more. Review the Asset Report in the RISC Networks Portal or download an excel spreadsheet.</p>
	<p>BitTitan Azure Assessments</p> <p>Provide detailed readiness reporting using cost analysis and planning tools to convince customers to adopt Azure. Take advantage of massive opportunities to move data out of SQL servers at end of life or support. Even uncover security concerns in customer infrastructure.</p> <ul style="list-style-type: none"> • Readiness check • Cost analysis • Detailed planning
	<p>TSO Logic</p> <p>The TSO Logic Platform provides the industry’s most accurate data-driven analysis of total cost of ownership and cost modelling for an ideal future state. It ingests millions of data points from the current environment, including age, generation and configuration of all hardware and software running, and each instance’s historical utilization. The Platform creates a fine-grained statistical model of compute patterns for all OS instances, showing how much is being spent, where a customer is over-provisioned, and where there are opportunities to realize significant savings both now and in the future.</p>

	<p>Corent</p> <p>Corent's SurPaaS® Platform is an Azure SaaS service that automates the scan, assessment, planning and cost modeling for customers workloads. It automatically migrates them to the cloud, and then monitors, manages, optimizes, and operates those workloads in the cloud.</p>
	<p>BMC Discovery for Multi-Cloud</p> <p>BMC Discovery for Multi-Cloud automates asset discovery and application dependency mapping to build a holistic view of all data center assets, multi-cloud services, and their relationships.</p>

Resources: <https://docs.microsoft.com/en-us/azure/migrate/migrate-services-overview>

Agile as a pre-sales tool

For projects in cloud infrastructure, migration and modernization, and operations and management, agile methodologies are not only a means for executing project delivery, but also a pre-sales tool. Consider taking the following approach:

- Qualify the customer to ensure there is budget, interest, and involvement of the appropriate stakeholders. This is not something to offer to every lead as it incurs costs. Focus on potential customers who are further along in their purchasing evaluation.
- For qualified customers, consider performing rapid prototyping to ideate with the customer and create a vision of what the results could be like.
- Take an agile approach to developing the prototype. Leverage short sprints during the prototype development by implementing the minimal set of requirements that will help clarify the vision with the customer, collecting feedback from the customer and refining the prototype.
- The tangible outcome of a prototype or proof of concept demonstrates an understanding of their requirements.
- The ability to quickly deliver tangible results builds trust in the ability to execute. It is a great opportunity to highlight the practice's unique capabilities and identify potential follow-on projects to assist the customer.
- The process of iterating on the prototype with the customer is a great way for the customer to experience what it would be like to work on the larger project.
- Once a customer has the sense of a tangible, working prototype in hand, it becomes more difficult for them to select competitors who have only provided written proposals.

Sales compensation planning

Compensation for sales executives is an area all partners grapple with. Our research revealed three core principles of sales compensation.

REWARDING SALES ACTION

Reward an array of sales activities, not just the final close. Sometimes this can be challenging. The reward does not have to be big, but there must be something to reward the right sales behavior that will lead to the final sale.

THE LEVEL OF INCENTIVE VERSUS REQUIRED SELLING EFFORT

Not all sales are created equal. Sometimes a renewal, for instance, can be much easier than acquiring a new customer. Consider the effort put in when setting up a compensation model. Reward the right behavior that gets the result. Do not over-compensate for routine activities that require less effort and expertise. Always consider how much of the sales process can be done by lower-level sales staff versus the sales executive. This is also a way to keep sales compensation costs manageable.

SIMPLE ENOUGH TO BE UNDERSTOOD AND DRIVE ACTIONS

Always keep it simple. Salespeople are brought on for their ability to communicate, engage and educate customers, and the always-important act of closing. Do not overly complicate the sales actions required for compensation. Drive the behavior that leads to closing business. Reward that behavior and get sales reps to see it through to the close of business.

Remember that everyone is a seller in most companies. Train all employees in appropriate sales techniques. Everyone should be on the lookout for existing customer opportunities as well as new ones. Teach them the signs and how to react. Reward everyone in the company for positive sales behavior.

SALES COMPENSATION VARIABLES

When deciding how to calculate the compensation for the sales incentives, consider the variables that help describe the magnitude of the benefit of the sale to the company and the effort required to close the sale. Examples include:

- **Expected duration:** How long is the contract for? Longer contracts are more lucrative to the company and should have higher valued incentives.
- **Expected number of units:** How much of the service is purchased? Higher quantity purchases deliver more value to the company and should have higher valued incentives.
- **Feature options:** Some features are more profitable to the company than others. Consider incentivizing the higher profit margin features with higher valued incentives to drive sales.

POSITIONING THE OFFER VIA INCENTIVES

Depending on the maturity of the practice, it may require different incentives to encourage the selling of the offer. This diagram illustrates a decision-making process to finetune incentives based on how the offer's incentives compete with other company incentives.

Microsoft Technology Centers

With more than 40 locations around the globe, The [Microsoft Technology Center](#) (MTC) bring together the right resources to help accelerate a customer's digital transformation.

- **People:** The MTC staff is comprised of experts in Microsoft solutions. Their tenure in the industry ensures they will effectively guide partners in finding solutions.
- **Partners:** The MTCs have formed alliances with industry leaders who provide comprehensive resources, including hardware, software, and services.
- **Place:** The MTC environment provides rich interactive and immersive experiences to learn first-hand Microsoft and partner technologies.

The MTC can help close sales with these engagement offerings:

- **Strategy Briefing:** This one-day briefing starts by examining the current IT environment and business objectives. Then it moves into the Envisioning Center, showcasing Microsoft solutions in action through powerful demos and customized scenarios. The day includes mutual discovery, tailored product and technology drilldowns, and expert presentations. It culminates with the delivery of a clear and actionable picture of how Microsoft and partner technologies can help reach business goals.
- **Architecture Design Session:** This custom session aligns business objectives with specific applications of Microsoft software. It provides architectural guidance, consultation on preferred practices, and risk analysis to chief technology officers, architects, and senior members of the development team.
- **Workshops:** If seeing is believing, then imagine what a hands-on immersive experience can do. Attend a custom briefing that includes a facilitated, hands-on environment to experience the vision of Microsoft's platform and solutions firsthand.

Architecture design session (ADS)

An architecture design session is a working session that follows the envisioning session and builds on the customer's already established vision.

This intensive, one to two-day session delivers in-depth technical information on integrating data from across a customer's entire organization and delivering it in an analysis-ready form. Presentations, demonstrations, and whiteboard discussions are customized to address the customer's needs. In many cases, the design session is used to identify candidate proofs of concept.

Here are some potential topics that are covered during an architecture design session:

- **Server topology:** To plan and deploy a customer's business productivity solution, it is necessary to understand the required server topology.
- **Integration platform:** The Azure services work seamlessly together and can also be integrated with third party and LOB applications. The ADS will endeavor to fit diverse systems together.
- **Social computing:** Companies need to leverage their employees' ability to make business connections and create, share, and evaluate content in a natural way.
- **Secure framework:** Companies can create experiences that are both user-based and role-based. Choose from a range of options for restricting sensitive information and deliver the most relevant experience while meeting industry standards and enterprise security requirements.
- **Virtualization and cloud computing:** Extending a customer's enterprise by leveraging cloud resources or virtualization reduces the cost of hardware and additional resources.

PRIMARY AUDIENCE

- Architects
- Developers
- Test and quality assurance (QA) engineers
- Technical staff

Note that an architecture design session is not always an appropriate engagement with the customer. They may have very little to no knowledge about Azure or cloud technologies in general. If this is the case, then they are not ready for an ADS. A technical briefing or hands-on-labs may be needed to build the customer's confidence in cloud technologies.

Phases of a successful ADS

BEFORE THE ARCHITECTURE DESIGN SESSION

Before performing the architecture design session, it is important to conduct a simple session with the customer to establish the scenario. This session is oftentimes referred to as ideation or opportunity definition. The goal is to establish the five Ws (who, what, when, where, and why) of their needs, which can be used as a guide for the ADS, streamlining the brainstorming process, and informing the agenda and milestone goals.

- Schedule a time for the design session: Normally 1-2 days.
- Schedule a location: Ensure there are whiteboards and a projector.
- Schedule resources: Experts from the team, and a cross-cutting panel of technical and business stakeholders from the customer.
- Build an agenda: Establish milestone goals in advance so that the ADS do not get consumed discussing a single topic.
- Prepare preliminary documentation and architectural diagrams: Even with only the basic building blocks, it is good to come prepared with something to modify during or after the session.

DURING THE ARCHITECTURE DESIGN SESSION

Begin by reviewing requirements with the customer. Whiteboard the requirements, proposed solutions, and arrive at a consensus for each major topic. Be sure to capture photos of the whiteboard.

There are typically the following phases during an architecture design session: Discovery, Envisioning, and Planning.

DISCOVERY

- Review the customer background and business technology strategy
- Project background and its drivers/aims
- Functional and non-functional requirements
- Usage scenarios
- Technology landscape

ENVISIONING

- Key functions and capabilities
- Components of the solution
- External connections and integration points
- Security considerations
- Abilities considerations
- Map requirements and scenarios to components

PLANNING

- Establish proof points
- Exclusions, risks, and issues
- Pre-requisites
- Deliverables
- Resources
- Escalation, communication, and long-term plans

AFTER THE ARCHITECTURE DESIGN SESSION

In addition to a summary of the engagement, deliver information about:

- Special areas of concern to the customer's organization, such as security, compliance, and compatibility.
- Deployment scenarios that map to established deployment and practices and that cite specific examples where applicable.
- Familiarity with the Microsoft technologies proposed for the solution, in addition to any trade-offs among the differing technology options.
- The capabilities to deliver business performance on premises or in the cloud.

The outcome should be polished architecture diagrams that can be reviewed and signed off on by the customer. If one or more proof of concepts is desired, provide a plan and a timeline to deliver.

Implement a proof of concept (PoC)

If one of the outcomes of the ADS is a PoC, there are some basic guidelines to keep in mind.

The key to developing a successful PoC is to avoid common traps, such as premature optimization, and spending too much time hardening the application for rock solid performance and stability. The proof of concept is a level of complexity and usability below a minimum viable product (MVP), as it is used to validate the customer requirements and the proposed solution. Try to start a PoC from an available template, such as a Visual Studio project template, or from pre-existing code from other projects. This is a great way to jump start a development process. Bear in mind that the PoC lacks a lot of the functionality of the final delivered software. User interface elements, for instance, may be there just for illustrative purposes and lack functionality. APIs may have desired endpoints stubbed out that define the methods and functionality that it will provide, but the implementations are missing. Resist the urge to develop the final product atop the PoC, as it could alter the use of technology and the requirements could change. Start from a more stable development foundation.

The benefits of developing the PoC are twofold: it helps the development team fully understand the customer requirements, instead of just reading through the documents, and it also helps the customer truly understand what they want. Oftentimes, customers will have a concept in mind of what they want, but they are not aware of what they do not know, that can influence their concept later in the development process. The PoC helps identify these issues early on. Having a PoC on hand provides the opportunity to communicate to the user the look and feel of the final product much more vividly than using design documents and design reviews. Seeing the PoC allows the customer to adjust their requirements to match exactly what they want, and to better define their expectations for the final deliverable.



Optimize & Grow

Cloud Infrastructure



aka.ms/practiceplaybooks

Microsoft
Partner
Network

Introduction

Optimize and Grow Guide

Leverage the Microsoft resources available in the Optimize and Grow guide, for details on optimization strategies, engaging customers for life, and monitoring and measuring results. The guide contains the following additional sections:

OPTIMIZE THROUGH BOTTOM-LINE EFFICIENCIES

Optimize for operational excellence, using bottom-line levers.

MEASURE RESULTS

Benchmark and create scorecard to measure improvement against key performance indicators.

UNDERSTANDING CUSTOMER LIFETIME VALUE

A lifelong customer is of far greater value than any one-off transaction. And not all customers are equal in value.

CUSTOMER EXPERIENCE AND SATISFACTION

Continually improve the customer experience by establishing CX related metrics.

COLLECT FEEDBACK

Solicit feedback from customers on a regular basis and act on that feedback.

PERFORM A POST-MORTEM

Establish a formal process for evaluating a project.

GROWTH THROUGH TOP-LINE STRATEGIES

Without a strategic plan for growth and revenue generation, the impact will be felt on the bottom line.

POST-SALE ACTIVITIES

Building and nurturing positive customer outcomes post-deployment is critical to secure recurring and renewal-based revenue.

GROW PARTNERSHIPS

Identify partnership opportunities, assess readiness, and grow relationships to differentiate offers, expand markets, or enter verticals.

Partnering with Microsoft

One of the first steps to partnering with Microsoft is to join the [Microsoft Partner Network](#). Partners gain access to resources like the training, whitepapers, and marketing material described in this playbook. It is also where partners set up their users to gain Microsoft Partner competencies and access to other partner benefits.

TO BECOME A MICROSOFT PARTNER

The Microsoft Partner Network provides three types of memberships. Partners can participate in the program at the level that suits their unique needs.

- **Network member:** Receive a set of no-cost introductory benefits to help save time and money. Use our resources to help build business and discover the next steps.
- **Microsoft Action Pack (MAP):** This affordable yearly subscription is for businesses looking to begin, build, and grow their Microsoft practice in the cloud-first, mobile-first world through a wide range of software and benefits.
- **Competency:** Demonstrate a capability with a specific product or solutions and receive increased support, software, and training.

What is the Microsoft Partner Network?

The Microsoft Partner Network is a hub of people, resources, and offerings brought together to give you everything you need to build and deliver successful solutions for your customers.



The power of partnership

Together, we can accomplish more. When you join the network, you become part of a community with a shared goal to do more for our customers.



Investing in you

The resources, programs, and tools we offer help you train your team, build innovative solutions, differentiate in the marketplace, and connect with customers.



Your launchpad for growth

With access to a broad range of products and services, our partners are empowered to build and deliver solutions that can address any customer scenario.

Best practices

Ensure that the team is aware of and takes advantage of established best practices from Microsoft where possible.

Here is a list of best practice resources as it relates to developing Cloud Infrastructure solutions.

DOCUMENT	OVERVIEW
Cloud Adoption Framework	The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate the cloud adoption journey. https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/
Well Architected Framework	The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architecture excellence: Cost Optimization, Operational Excellence, Performance Efficiency, Reliability, and Security. https://docs.microsoft.com/en-us/azure/architecture/framework/ Partners can also request a Microsoft Azure Well-Architected Review .
Azure Architecture Center	Architecture diagrams, reference architectures, example scenarios, and solutions for common workloads on Azure. Azure Architecture Center provides guidance for architecting solutions on Azure using established patterns and practices. https://docs.microsoft.com/en-us/azure/architecture/
Azure Migrate	Get the Azure migration tools and guidance needed to plan and implement a move to the cloud—and track the project's progress using a central dashboard that provides intelligent insights. https://azure.microsoft.com/en-us/services/azure-migrate/

Playbook Summary

Thank you for taking the time to review this playbook. The research, guidance, and best practices outlined in this playbook provide insights from successful partners on how to build a cloud infrastructure, migration and modernization, and operations and management practice.

The goal was to organize resources and provide insight on business strategies and technical topics to capitalize on the cloud application development opportunity.

- The first section, **Define the Strategy**, helped partners define the practice strategy by identifying the unique value proposition and building a business plan.
- The second section, **Hire & Train**, focused on the importance of hiring the right team, and providing appropriate and ongoing training.
- The third section, **Operationalize**, detailed the solution delivery process, the Microsoft-provided support options, and tips for implementing IP in a security offering. It ended with a customer engagement checklist to use for creating repeatable processes.
- The fourth section, **Go-To-Market & Close Deals**, covered the sales and marketing process, finding new customers, and then nurturing and investing in them to build lasting relationships.
- The final section, **Optimize & Grow** the practice, stressed the importance of building customer lifetime value and the key elements of a customer adoption approach.

FEEDBACK

Share feedback on how to improve this and other playbooks by emailing playbookfeedback@microsoft.com.