Microsoft Corporation - Microsoft Azure

(Azure & Azure Government)

SOC 3 Report

January 1, 2017 - December 31, 2017

Table of contents

Section I:
Independent Service Auditors' Report

Deloitte & Touche LLP
925 Fourth Avenue, Suite 3300,
Seattle, WA 98104-1126
Tel: +1 206 716 7000

Section I: Independent Service Auditors' Report

Microsoft Corporation
One Microsoft Way
Redmond, WA, 98052-6399

We have examined the effectiveness of Microsoft Azure and Microsoft datacenters (the "Service Organization" or "Azure") controls related to Azure's in-scope services, for Azure and Azure Government cloud environments, to meet the criteria for the security, availability, processing integrity and confidentiality principles ("applicable trust services criteria")[1], during the period January 1, 2017 to December 31, 2017[2], based on the American Institute of Certified Public Accountants' (AICPA) 2016 edition of TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Azure's management is responsible for maintaining the effectiveness of these controls. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the AICPA, and accordingly, included (1) obtaining an understanding of the controls related to Azure's in-scope services, for Azure and Azure Government cloud environments, to meet the applicable trust services criteria (2) testing and evaluating the operating effectiveness of the Service Organization's controls, and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, the Service Organization's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent or detect and correct error or fraud, unauthorized access to systems and information, and failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion, the Service Organization maintained, in all material respects, effective controls to meet the applicable trust services criteria during the period January 1, 2017 to December 31, 2017 to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as "confidential", was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the AICPA's trust services principles and criteria for security, availability, processing integrity and confidentiality.

Deloitte & Touche LLP

January 31, 2018

---

[1] Applicable Trust Services Principles for Microsoft datacenters are Security and Availability.

[2] In-scope services and coverage periods are defined in the *Azure and Azure Government Report Scope Boundary* and *Azure Supporting Infrastructure Services* subsections in Section III of this SOC 3 report. Applicability of the Processing Integrity Trust Services Principle is defined in *the Azure and Azure Government Report Scope Boundary* subsection. In-scope datacenters and coverage periods are defined in the *Locations Covered by this Report* subsection in Section III of this SOC 3 report.

Section II:
Management's Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Section II: Management's Assertion

Microsoft Azure and Microsoft datacenters ("Azure") maintained effective controls over the security, availability, processing integrity, and confidentiality ("applicable trust services criteria")[3] of the system relating to Azure's in-scope services, for Azure and Azure Government cloud environments, throughout the period January 1, 2017 to December 31, 2017[4], to provide reasonable assurance that:

- the system was protected against unauthorized access, use or modification,
- the system was available for operation and use as committed or agreed,
- information within the system, designated as "confidential", was protected as committed or agreed, and
- the system processing was complete, valid, accurate, timely, and authorized

based on the 2016 edition of TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) for security, availability, processing integrity and confidentiality.

The following description of the system identifies the aspects of the Azure's in-scope services covered by this assertion.

Microsoft Azure

[3] Applicable trust services criteria for Microsoft datacenters are Security and Availability.

[4] In-scope services and coverage periods are defined in the *Azure and Azure Government Report Scope Boundary* and *Azure Supporting Infrastructure Services* subsections in Section III of this SOC 3 report. Applicability of the Processing Integrity Trust Services Principle is defined in the *Azure and Azure Government Report Scope Boundary* subsection. In-scope datacenters and coverage periods are defined in the *Locations Covered by this Report* subsection in Section III of this SOC 3 report.

Section III: Description of the Microsoft Azure System

Section III: Description of Microsoft Azure System

Overview of Operations

Business Description

Microsoft Azure is a cloud computing platform for building, deploying and managing applications through a global network of Microsoft and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models, and enables hybrid solutions that integrate cloud services with customers' on-premises resources. Microsoft Azure supports many customers, partners, and government organizations that span across a broad range of products and services, geographies, and industries. Microsoft Azure is designed to meet their security, confidentiality, and compliance requirements.

Microsoft datacenters support Microsoft Azure and many other Microsoft Online Services ("Online Services"). Online Services such as Intune, Power BI, and others are Software as a Service (SaaS) services that leverage the underlying Microsoft Azure platform and datacenter infrastructure. See section titled Azure and Azure Government Report Scope Boundary for the Microsoft Azure services and Online Services that are in scope for this report.

"Azure", when referenced in this report, comprises of "Microsoft Azure", "Online Services", and the supporting datacenters listed in this report.

Azure and Azure Government Report Scope Boundary

Azure is a global multi-tenant cloud platform that provides a public cloud deployment model. Azure Government is a US Government Community Cloud (GCC) that is physically separated from the Azure cloud. The following Azure and Azure Government services are in scope for this report:

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Microsoft Datacenters							
Microsoft Datacenter and Operations Service		✓	✓	✓	✓	✓	✓
Azure							
Compute	Batch	✓	✓	✓	✓	✓	✓

[5] Examination Period scope Q1 2017 extends from January 1, 2017 to March 31, 2017.
Examination Period scope Q2 2017 extends from April 1, 2017 to June 30, 2017.
Examination Period scope Q3 2017 extends from July 1, 2017 to September 30, 2017.
Examination Period scope Q4 2017 extends from October 1, 2017 to December 31, 2017.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q1 2017	Q2 2017	Q3 2017	Q4 2017
	Cloud Services	✓	✓	✓	✓	✓	✓
	Functions	✓	-	✓	✓	✓	✓
	Service Fabric	✓	✓	✓	✓	✓	✓
	Virtual Machines (including SQL VM)	✓	✓	✓	✓	✓	✓
	Virtual Machines Scale Sets	✓	✓	✓	✓	✓	✓
	Azure Reserved Virtual Machine Instances	✓	-	-	-	-	✓
Containers	Azure Container Registry	✓	-	-	✓	✓	✓
	Azure Container Service	✓	-	✓	✓	✓	✓
Networking	Application Gateway	✓	✓	✓	✓	✓	✓
	Azure DNS	✓	-	✓	✓	✓	✓
	Azure Network Watcher	✓	-	-	-	✓	✓
	ExpressRoute	✓	✓	✓	✓	✓	✓
	Load Balancer	✓	✓	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓	✓	✓
	Virtual Network	✓	✓	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓	✓	✓
Storage	Backup	✓	✓	✓	✓	✓	✓
	Cool Storage	✓	✓	✓	✓	✓	✓
	Data Lake Store	✓	-	✓	✓	✓	✓
	Import/Export	✓	✓	✓	✓	✓	✓
	Premium Storage	✓	✓	✓	✓	✓	✓
	Site Recovery	✓	✓	✓	✓	✓	✓
	Storage (Blobs, Disks, Files, Queues, Tables)	✓	✓	✓	✓	✓	✓
	StorSimple	✓	✓	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Web + Mobile	App Service	✓	✓	✓	✓	✓	✓
	App Service: API Apps	✓	✓	✓	✓	✓	✓
	App Service: Mobile Apps	✓	✓	✓	✓	✓	✓
	App Service: Web Apps	✓	✓	✓	✓	✓	✓
	Azure Search	✓	-	-	-	✓	✓
	Media Services	✓	✓	✓	✓	✓	✓
Databases	Azure Cosmos DB	✓	-	✓	✓	✓	✓
	Azure Database for MySQL	✓	-	-	✓	✓	✓
	Azure Database for PostgreSQL	✓	-	-	✓	✓	✓
	Redis Cache	✓	✓	✓	✓	✓	✓
	SQL Database	✓	✓	✓	✓	✓	✓
	SQL Data Warehouse	✓	✓	✓	✓	✓	✓
	SQL Server Stretch DB	✓	✓	✓	✓	✓	✓
Data + Analytics	Azure Analysis Services	✓	-	-	✓	✓	✓
	Data Lake Analytics	✓	-	✓	✓	✓	✓
	HDInsight	✓	✓	✓	✓	✓	✓
	Machine Learning Studio	✓	-	✓	✓	✓	✓
	Stream Analytics	✓	-	✓	✓	✓	✓
Internet of Things	Event Hubs	✓	✓	✓	✓	✓	✓
	Internet of Things (IoT) Hub	✓	-	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓	✓	✓
Enterprise Integration	API Management	✓	-	✓	✓	✓	✓
	Data Catalog	✓	-	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q1 2017	Q2 2017	Q3 2017	Q4 2017
	Logic Apps	✓	-	✓	✓	✓	✓
	Service Bus	✓	✓	✓	✓	✓	✓
Security + Identity	Azure Active Directory (Free, Basic)	✓	✓	✓	✓	✓	✓
	Azure Active Directory (Premium)	✓	-	-	-	✓	✓
	Azure Active Directory B2C	✓	-	✓	✓	✓	✓
	Azure Active Directory Domain Services	✓	-	-	-	✓	✓
	Azure Information Protection (including Azure Rights Management)	✓	✓	✓	✓	✓	✓
	Key Vault	✓	✓	✓	✓	✓	✓
	Multi-Factor Authentication	✓	-	✓	✓	✓	✓
	Security Center	✓	-	-	✓	✓	✓
Developer Tools	Application Insights	✓	-	✓	✓	✓	✓
	Azure DevTest Labs	✓	-	-	-	✓	✓
Monitoring + Management	Automation	✓	✓	✓	✓	✓	✓
	Azure Advisor	✓	-	-	-	✓	✓
	Azure Monitor	✓	-	-	-	✓	✓
	Azure Resource Manager[6]	✓	✓	✓	✓	✓	✓
	Log Analytics	✓	✓	✓	✓	✓	✓
	Microsoft Azure Portal[6]	✓	✓	✓	✓	✓	✓
	Scheduler	✓	✓	✓	✓	✓	✓

[6] Services for which AICPA Processing Integrity trust principle was examined: Azure Resource Manager, Microsoft Azure Portal, and RDFE.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q1 2017	Q2 2017	Q3 2017	Q4 2017
Azure Supporting Infrastructure Services[6,7]		✓	✓	✓	✓	✓	✓
Microsoft Online Services							
Microsoft Cloud App Security		✓	-	✓	✓	✓	✓
Microsoft Flow		✓	-	✓	✓	✓	✓
Microsoft Graph		✓	-	✓	✓	✓	✓
Microsoft Intune		✓	-	✓	✓	✓	✓
Microsoft Power BI		✓	✓	✓	✓	✓	✓
Microsoft PowerApps		✓	-	✓	✓	✓	✓
Microsoft Stream		✓	-	-	✓	✓	✓

Locations Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters deliver the core physical infrastructure that includes physical hardware asset management, security, data protection, networking services. These datacenters are managed, monitored, and operated by Microsoft operations staff delivering online services with 24x7 continuity. The purpose-built facilities are part of a network of datacenters that provide mission critical services to Azure and other Online Services. The datacenters in scope for the purposes of this report are:

[7] Azure Government scope boundary for internal services: ADRS, ADGateway, Azure Watson, Azure Active Directory Connect Health, IAM - Data Insights and Reporting Service, Azure Monitor - IDC, Azure Notification Services, Backend Health Management, Cloud App Discovery, Custom Speech Service, DNS (AzDNS, iDNS/RR), dSMS, Fabric / Compute Manager, Hybrid Identity Service, IAM - Information Worker UX, Jumpboxes, MSODS, OneDDoS, OneDeploy Express v2, PhyNet, PAS, RDFE, RDOS, Resource Providers (Compute, Networking, Storage), Service Fabric - RP Clusters, WANetMon, and Workflow. The coverage period for internal services for both Azure and Azure Government is Q1 2017 through Q4 2017 except for those specified with shorter coverage periods in the *Azure Supporting Infrastructure Services* subsection herein.

Domestic

- Phoenix, AZ (PHX20[8])
- Santa Clara, CA (BY1/2/3/4/22)
- Des Moines, IA (DM1/2/3, DSM05)
- Chicago, IL (CH1/3, CHI20[8])
- San Antonio, TX (SN1/2/3/4/5/6[11])
- Ashburn, VA (BL2/3/5/7[11])
- Boydton, VA (BN1/3/4/6)
- Dallas, TX (DAL[9])
- Bristow, VA (BLU)
- Reston, VA (BL4/6/30)
- Tukwila, WA (TK5)
- Quincy, WA (CO1/2, MWH01)
- Cheyenne, WY (CYS01/04)
- San Jose, CA (SJC31)
- New York, NY (NYC[10])
- Stirling, VA (BL20[11])

International

North America
- Toronto, Canada (YTO20, YTO01[10])
- Quebec City, Canada (YQB20)
- Mexico City, Mexico (MEX30)

Australia
- Macquarie Park, Australia (SYD03)
- Melbourne, Australia (MEL01)

Europe
- Vienna, Austria (VIE)
- Vantaa, Finland (HEL01)
- Amsterdam, Netherlands (AM1/2/3, AMS04/05/20[11])
- Billingham, United Kingdom (MME20)
- Chessington, United Kingdom (LON20/21)
- Cardiff, United Kingdom (CWL20)
- Dublin, Ireland (DB3/4/5, DUB06)
- Paris, France (PAR02[10]/21[11]/22[11])
- Marseille, France (MRS20[11])
- Copenhagen, Denmark (CPH30[9])
- Milan, Italy (MIL30[9])
- Stockholm, Sweden (STO[9])

South America
- Campinas, Brazil (CPQ01/02)
- Fortaleza, Brazil (FOR01)
- Rio de Janeiro, Brazil (RIO01)
- Sao Paulo, Brazil (GRU)
- Santiago, Chile (SCL01)
- Humacao, Puerto Rico (PR1)

Asia
- Hong Kong (HK1/2/20[11])
- Mumbai, India (BOM01)
- Dighi, India (PNQ01)
- Ambattur, India (MAA01)
- Osaka, Japan (OSA01/02)
- Tokyo, Japan (KAW, TYO01/21[11]/22[11])
- Cyberjaya, Malaysia (KUL01)
- Singapore (SG1/2/3, SIN20[11])
- Busan, South Korea (PUS01, PUS20)
- Seoul, South Korea (SEL20[12])

In addition to datacenter, network, and personnel security practices, Azure also incorporates security practices at the application and platform layers to enhance security for application development and service administration.

[8] The examination period for this datacenter was from July 1, 2017 to December 31, 2017.

[9] The examination period for this Edge site was from October 1, 2017 to December 31, 2017.

[10] The examination period for this Edge site was from April 1, 2017 to December 31, 2017.

[11] The examination period for this datacenter was from October 1, 2017 to December 31, 2017.

[12] Datacenter was placed into operation from February 1, 2017.

People

Azure is comprised and supported by the following groups who are responsible for the delivery and management of Azure services:

Online Services

Online Services teams manage the service lifecycle of the finished SaaS services that leverage the underlying Azure platform and datacenter infrastructure. They are responsible for the development of new features, operational support, and escalations.

Cloud and Enterprise Security

The Cloud and Enterprise Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud and Enterprise Security team is involved in the review of deployments and enhancements of Azure services to facilitate security considerations at every level of the Secure Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters.

Azure Production Support

The Azure Production Support team is responsible for build-out, deployment and management of Azure services. This team consists of the following:

- **Azure Live Site** - Monitors and supports the Azure platform; proactively addresses potential platform issues; and reacts to incidents and support requests
- **Azure Deployment Engineering** - Builds out new capacity for the Azure platform; and deploys platform and product releases through the release pipeline
- **Azure Customer Support** - Provides support to individual customers and multinational enterprises from basic break-fix support to rapid response support for mission critical applications

Azure Engineering Service Teams

The Azure Engineering Service teams manage the service lifecycle. Their responsibilities include development of new services, serving as an escalation point for support, providing operational support for existing services.

Global Ecosystem and Compliance Team

The Global Ecosystem and Compliance team is responsible for developing, maintaining and monitoring the Information Security (IS) program including the ongoing risk assessment process.

As part of managing compliance adherence, the team drives related features within the Azure product families. This team consists of personnel responsible for training, privacy, risk assessment, and internal and external audit coordination.

Networking

The Networking team is responsible for implementing, monitoring and maintaining the Microsoft network. This team consists of personnel responsible for network configuration, network problem management, and network capacity management.

Azure Environment

Azure is developed and managed by the Azure team, and provides a cloud platform based on machine virtualization where customers host their applications and data. Datacenters provide the underlying physical infrastructure on which the Azure platform runs and data is stored.

Azure Services

Azure services are grouped into categories discussed below. A complete list of Azure services available to customers is provided in the Azure Service Directory. Brief descriptions for each of the customer-facing services in scope for this report are provided below. Customers should consult extensive online documentation for additional information.

Compute

Batch: Batch makes it possible to run large-scale parallel and High-performance Computing (HPC) workloads in Azure. Customers can use Batch to scale out parallel workloads, manage the execution of tasks in a queue, and cloud-enable applications to offload compute jobs to the cloud.

Cloud Services: Cloud Services removes the need to manage server infrastructure. It lets customers build, deploy, and manage modern applications with web and worker roles.

Functions: Functions is an event driven, compute-on-demand experience. Customers can leverage Azure Functions to build HTTP endpoints accessible by mobile and IoT devices.

Service Fabric: Service Fabric is a micro-services platform used to build scalable managed applications for the cloud. Service Fabric addresses significant challenges in developing and managing cloud applications by allowing developers and administrators to shift focus from infrastructure maintenance to implementing mission-critical, demanding workloads.

Virtual Machines: Virtual Machines, which include Azure Reserved Virtual Machine Instances, lets customers deploy a Windows Server or Linux image in the cloud. Customers can select images from a marketplace or use their own customized images. A SQL Virtual Machine enables customers to create a SQL Server in the cloud that they control and manage. SQL VMs offer a robust infrastructure for SQL Server by using Azure as a hosting environment of enterprise database applications. SQL Server is a database for transactions, queries and analytics for big data solutions. SQL Server is not in scope of this SOC report.

Virtual Machine Scale Sets: Virtual Machine Scale Sets makes it possible to build highly scalable applications by allowing customers to deploy and manage identical VMs as a set. VM Scale sets are built on the Azure Resource Manager deployment model and are fully integrated with Azure load balancing and autoscale, as well as support Windows, Linux, custom images, and extensions.

Containers

Azure Container Registry: Azure Container Registry allows customers the ability to store images for all types of container deployments including DC / OS, Docker Swarm, Kubernetes, and Azure services such as App Service, Batch, Service Fabric, and others. DevOps teams can manage the configuration of apps isolated from the configuration of the hosting environment. The service reduces network latency and eliminates ingress / egress charges by keeping Docker registries in the same datacenters as customers' deployments. It provides local, network-close storage of container images within subscriptions, and full control over access and image names.

Azure Container Service: Azure Container Service is a container hosting environment optimized for Azure that lets customers deploy, scale, and orchestrate container-based applications using Docker Swarm and Apache Mesos.

Networking

Application Gateway: Application Gateway is an Azure-managed layer-7 solution providing HTTP load balancing, Secure Sockets Layer (SSL) termination service, and session-based cookie affinity to Internet-facing or internal web applications.

Azure DNS: Azure DNS lets customers host their Domain Name System (DNS) domains alongside their Azure apps and manage DNS records by using their existing Azure subscription.

Azure Network Watcher: Azure Network Watcher enables customers to monitor and diagnose conditions at a network scenario level. Network diagnostic and visualization tools available with Network Watcher allow customers to take packet captures on a VM, help them understand if an IP flow is allowed or denied on their Virtual Machine, find where their packet will be routed from a VM and gain insights to their network topology.

ExpressRoute: ExpressRoute lets customers create private connections between Azure datacenters and infrastructure that's on customers' premises or in a colocation environment.

Load Balancer: Load Balancer distributes Internet and private network traffic among healthy service instances in cloud services or virtual machines. It lets customers achieve greater reliability and seamlessly add more capacity to their applications.

Traffic Manager: Traffic Manager lets customers route incoming traffic across multiple hosted Azure services running in the same datacenter or in different datacenters across the world.

Virtual Network: Virtual Network lets customers create private networks in the cloud with full control over IP addresses, DNS servers, security rules, and traffic flows. Customers can securely connect a virtual network to on-premises networks by using a Virtual Private Network (VPN) tunnel, or connect privately by using the ExpressRoute service.

VPN Gateway: VPN Gateway lets customers establish secure, cross-premises connections between their virtual network within Azure and on-premises IT infrastructure.

Storage

Backup: Backup protects Windows client data and shared files and folders on customer's corporate laptops. Additionally, Backup protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in customer's datacenter, integrated with System Center Data Protection Manager (DPM). Backup enables customers to protect important data off-site with automated backup to Microsoft Azure. Customers can manage their cloud backups from the tools in Windows Server, Windows Server Essentials, or System Center Data Protection Manager. These tools allow the user to configure, monitor and recover backups to either a local disk or Azure Storage.

Data Lake Store: Data Lake Store provides a single repository where customers can capture data of any size type and speed without forcing changes to their application as the data scales. In the store, data can be shared for collaboration with enterprise-grade security. It is also designed for high-performance processing and analytics from Hadoop Distributed File System (HDFS) applications (e.g., Azure HDInsight, Data Lake Analytics, Hortonworks, Cloudera, MapR) and tools, including support for low latency workloads. For example, data can be ingested in real-time from sensors and devices for IoT solutions, or from online shopping websites into the store without the restriction of fixed limits on account or file size.

Site Recovery: Site Recovery contributes to a customer's Business Continuity and Disaster Recovery (BCDR) strategy by orchestrating replication of on-premises physical servers and Virtual Machine servers to Azure or to a secondary datacenter. When a disaster occurs in the customer's primary location, Site Recovery coordinates failover and recovery to the secondary location and ensures that applications / workloads continue to run in the secondary location. Customers can failback their workloads to the primary location when it resumes operations. Site Recovery supports protection and recovery of heterogeneous workloads (including System Center managed / unmanaged Hyper-V workloads, VMware workloads). With Site Recovery, customers can use a single dashboard to manage and monitor their deployment and also configure recovery plans with multiple machines to ensure that tiered application workloads failover together.

Storage: Storage provides distributed persistent storage and five different data storage types: Blob, Disk, File, Queue, and Table. The Storage access control model allows each subscription to create one or more Storage accounts. Each Storage account has a primary and secondary secret key that is used to control access to the data within the Storage account. Every Storage service account has redundant data copies for fault tolerance. Below are the five different Storage types supported by Azure:

- Blob: Blob contains large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data.

- Disk: Disk includes both managed and unmanaged disk that are attached to VMs to store application data, or other data that the customer needs to keep.

- File: File offers shared storage for applications using the Simple Messaging Protocol (SMP). Applications running in Azure VMs, Cloud Services or from on-premises clients can mount a file share in the cloud.

- Queue: Queue provides storage and delivery of messages between one or more applications and roles.

- Table: Table provides fast access to large amounts of structured data that do not require complex SQL queries. For example, Table Storage can be used to create a customer contact application that stores customer profile information and high volumes of user transaction.

Cool Storage: Cool Storage is a low cost Blob Storage for cool object data, where the data is not accessed often. Example use cases for Cool Storage include backups, media content, scientific data, compliance and archival data. Customers can use Cool Storage to retain data that is seldom accessed.

Premium Storage: Premium Storage delivers high-performance, low-latency disk support for I/O intensive workloads running on Azure VMs. Customers can attach several Premium Storage disks to a VM. With Premium Storage, applications can have up to 32 TB of storage per VM and achieve 64,000 IOPS (input / output operations per second) per VM with extremely low latencies for read operations. This enables customers to run demanding enterprise workloads including databases, big data and data warehousing on Azure.

Import / Export: Import / Export allows customers to securely transfer large amounts of data to Azure Blob Storage by shipping hard disk drives to an Azure datacenter. Customers can also use this service to transfer data from Azure Blob Storage to hard disk drives and ship to their on-premises site. This service is suitable in situations where customers want to transfer several TBs of data to or from Azure, but uploading or downloading over the network is not feasible due to limited bandwidth or high network costs.

StorSimple: StorSimple is a hybrid cloud storage solution for primary storage, archiving, and disaster recovery. StorSimple optimizes total storage costs and data protection. It includes an on-premises Storage Area Network (SAN) solution that is a bottomless file server using Azure Blob Storage. StorSimple automatically arranges data in logical tiers based on current usage, age, and relationship to other data. Data that is most active is stored locally, while less active and inactive data is automatically migrated to the cloud.

Web & Mobile

App Service: App Service enables customers to quickly build, deploy, and scale enterprise-grade web, mobile, and API apps that can run on a number of different platforms.

App Service: API Apps: API Apps enables customers to build and consume Cloud APIs. Customers can connect their preferred version control system to their API App, and automatically deploy commits, making code changes.

App Service: Mobile Apps: Mobile Apps allows customers to accelerate mobile application development by providing a turnkey way to structure storage, authenticate users, and send push notifications. Mobile Apps

allows customers to build connected applications for any platform and deliver a consistent experience across devices.

App Service: Web Apps: Web Apps offers secure and flexible development, deployment and scaling options for web applications of any size. Web Apps enables provisioning a production web application in minutes using a variety of methods including the Azure Portal, PowerShell scripts running on Windows, Command Line Interface (CLI) tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).

Azure Search: Azure Search is a search-as-a-service cloud solution that gives developers APIs and tools for adding a rich search experience over customers' data in web, mobile, and enterprise applications.

Media Services: Media Services offers cloud-based versions of many existing technologies from the Microsoft Media Platform and Microsoft media partners, including ingest, encoding, format conversion, content protection and both on-demand and live streaming capabilities. Whether enhancing existing solutions or creating new workflows, customers can combine and manage Media Services to create custom workflows that fit every need.

Databases

Azure Cosmos DB: Azure Cosmos DB, formerly known as Azure DocumentDB, was built from the ground up with global distribution and horizontal scale at its core. It offers turnkey global distribution across any number of Azure regions by transparently scaling and replicating customers' data wherever their users are. Customers can elastically scale throughput and storage worldwide, and pay only for the throughput and storage they need. Azure Cosmos DB guarantees single-digit-millisecond latencies at the 99th percentile anywhere in the world, offers multiple well-defined consistency models to fine-tune performance, and guarantees high availability with multi-homing capabilities all backed by industry-leading, comprehensive service level agreements (SLAs).

Redis Cache: Redis Cache gives customers access to a secure, dedicated cache for their Azure applications. Based on the open source Redis cache, the service allows quick access to frequently requested data. Redis Cache handles the management aspects of the cache instances, providing customers with replication of data, failover, and SSL support for connecting to the cache.

SQL Database: SQL Database is a relational database service that lets customers rapidly create, extend, and scale relational applications into the cloud. Azure SQL Database delivers mission-critical capabilities including predictable performance, scalability with no downtime, business continuity and data protection-all with near-zero administration. Customers can focus on rapid application development and accelerating time to market, rather than on managing VMs and infrastructure. Because the service is based on the SQL Server engine, Azure SQL Database provides a familiar programming model based on T-SQL and supports existing SQL Server tools, libraries and APIs, allowing customers to move and extend to the cloud.

Azure Database for MySQL: Azure Database for MySQL is a MySQL database service built on Microsoft's scalable cloud infrastructure for application developers. Built-in features maximize performance, availability, and security. Azure Database for MySQL empowers developers to focus on application innovation instead of database management tasks.

Azure Database for PostgreSQL: Azure Database for PostgreSQL is a PostgreSQL database service built on Microsoft's scalable cloud infrastructure for application developers. Built-in features maximize performance, availability, and security. Azure Database for PostgreSQL empowers developers to focus on application innovation instead of database management tasks.

SQL Data Warehouse: SQL Data Warehouse is an elastic data warehouse as a service with enterprise-grade features based on a massively parallel SQL Server processing architecture. It lets customers scale data, either on-premises or in cloud. SQL Data Warehouse lets customers use their existing T-SQL skills to integrate queries across structured and unstructured data. It integrates with Microsoft data platform tools, including Azure

HDInsight, Machine Learning Studio, Data Factory, and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud.

SQL Server Stretch Database: SQL Server Stretch Database dynamically stretches warm and cold transactional data from Microsoft SQL Server to Azure. Unlike typical cold data storage, data is always at hand within SQL Server Stretch Database. Additionally, Stretch Database lets customers provide longer data retention times than typical enterprise storage. Depending on how often customers access the data, they can choose the appropriate level of service, then scale up or down as needed. Using Stretch Database does not require any application changes. Customers can use Stretch Database with new Always Encrypted technology, which helps protect data at rest and in motion.

Data & Analytics

Azure Analysis Services: Azure Analysis Services, based on the proven analytics engine in SQL Server Analysis Services, is an enterprise grade OLAP engine and BI modeling platform, offered as a fully managed platform-as-a-service (PaaS). Azure Analysis Services enables developers and BI professionals to create BI Semantic Models that can power highly interactive and rich analytical experiences in BI tools and custom applications.

Data Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator (YARN) that dynamically scales so customers can focus on their business goals, not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, customers write queries to transform data and extract valuable insights. The analytics service can handle jobs of any scale instantly by simply setting the dial for how much power is needed. Customers only pay for their job when it is running, making the service cost-effective. The analytics service supports Azure Active Directory letting customers manage access and roles, integrated with on-premises identity system. It also includes U-SQL, a language that unifies the benefits of SQL with the expressive power of user code. U-SQL's scalable distributed runtime enables customers to efficiently analyze data in the store and across SQL Servers in Azure VMs, Azure SQL Database, and Azure SQL Data Warehouse.

HDInsight: HDInsight is a managed Apache Hadoop ecosystem offering in the cloud. It handles various amounts of data, scaling from terabytes to petabytes on demand, and can process unstructured or semi-structured data from web clickstreams, social media, server logs, devices and sensors, and more. HDInsight includes Apache HBase, a columnar NoSQL database that runs on top of the Hadoop Distributed File System (HDFS). This supports large transactional processing (Online Transaction Processing (OLTP)) of non-relational data, enabling use cases like interactive websites or having sensor data write to Azure Blob Storage. HDInsight also includes Apache Storm, an open-source stream analytics platform that can process real-time events at large-scale. This allows processing of millions of events as they are generated, enabling use cases like Internet of Things (IoT) and gaining insights from connected devices or web-triggered events. Furthermore, HDInsight includes Apache Spark, an open-source project in the Apache ecosystem that can run large-scale data analytics applications in memory. Lastly, HDInsight incorporates R Server for Hadoop, a scale-out implementation of one of the most popular programming languages for statistical computing and machine learning. HDInsight offers Linux or Windows clusters when deploying big data workloads into Azure.

Machine Learning Studio: Machine Learning Studio is a service that enables users to experiment with their data, develop and train a model using training data and operationalize the trained model as a web service that can be called for predictive analytics.

Stream Analytics: Stream Analytics is an event-processing engine that helps customers gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. Stream Analytics is integrated out of the box with Event Hubs, and the combined solution can ingest millions of events and do analytics to help customers better understand patterns, power a dashboard, detect anomalies, or kick off an action while data is being streamed in real time. Stream Analytics can apply time-sensitive computations on real-time streams of data, by providing a range of operators covering simple filters to complex correlations, and combining streams with historic records or reference data to derive business insights quickly.

Internet of Things

Event Hubs: Event Hubs enables elastic-scale telemetry and event ingestion with durable buffering and sub-second end-to-end latency for millions of devices and events. Event Hubs is a highly scalable publish-subscribe event ingestor that uses Advanced Message Queuing Protocol (AMQP) and HTTP as its primary interfaces. Event Hubs is a feature of Service Bus that provides a message stream handling capability through a partitioned consumer pattern in which each consumer only reads a specific subset, or partition, of the message stream. This pattern enables horizontal scale for event processing. A partition is an ordered sequence of events that is held in an Event Hub. As newer events arrive, they are added to the end of this sequence. An Event Hub contains multiple partitions. Each partition is independent and contains its own sequence of data.

IoT Hub: IoT Hub is used to connect, monitor, and control billions of IoT assets running on a broad set of operating systems and protocols. IoT Hub establishes reliable, bi-directional communication with assets, even if they're intermittently connected, and analyze and act on incoming telemetry data. Customers can enhance the security of their IoT solutions by using per-device authentication to communicate with devices that have the appropriate credentials. They can also revoke access rights to specific devices to maintain the integrity of their system.

Notification Hubs: Notification Hubs is a massively scalable mobile push notification engine for sending millions of notifications to iOS, Android, Windows, or Kindle devices, working with Apple Push Notification service (APNs), Google Cloud Messaging (GCM), Windows Push Notification Service (WNS), Microsoft Push Notification Service (MPNS), and more. It allows customers to tailor notifications to specific customers or entire audiences with just a few lines of code, and do it across any platform.

Enterprise Integration

API Management: API Management lets customers publish APIs to developers, partners, and employees securely and at scale. API publishers can use the service to quickly create consistent and modern API gateways for existing backend services hosted anywhere.

Data Catalog: Data Catalog is a fully managed service that serves as a system of registration and system of discovery for enterprise data sources. It lets users - from analysts to data scientists to developers - register, discover, understand, and consume data sources. Customers can use crowdsourced annotations and metadata to capture tribal knowledge within their organization, shine light on hidden data, and get more value from their enterprise data sources.

Logic Apps: Logic Apps automates the access and use of data across clouds without writing code. Customers can connect apps, data, and devices anywhere-on-premises or in the cloud-with Azure's large ecosystem of Software as a Service (SaaS) and cloud-based connectors that includes Salesforce, Office 365, Twitter, Dropbox, Google services, and more.

Service Bus: Service Bus is a messaging infrastructure that sits between applications allowing them to exchange messages for improved scale and resiliency. Service Bus allows applications to interact in three ways:

1. Letting applications send and receive messages through a simple queue
2. Using a queue with a publish-and-subscribe mechanism
3. Allowing a connection between applications when queues aren't required

Service Bus provides a hosted, secure, and widely available infrastructure for widespread communication, large-scale event distribution, naming, and service publishing.

Security & Identity

Azure Active Directory: Azure Active Directory provides identity management and access control for cloud applications. To simplify user access to cloud applications, customers can synchronize on-premises identities, and enable single sign-on. Azure Active Directory comes in 3 editions: Free, Basic, and Premium.

Azure Active Directory B2C: Azure Active Directory B2C extends Azure AD capabilities to manage consumer identities. Azure Active Directory B2C is a comprehensive identity management solution for consumer-facing applications that can be integrated into any platform, and accessible from any device.

Azure Active Directory Domain Services: Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory. Customers can consume these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Azure AD Domain Services integrates with the existing Azure AD tenant, thus making it possible for users to log in using their corporate credentials.

Azure Information Protection: Azure Information Protection controls and helps secure email, documents, and sensitive data that customers share outside their company walls. Azure Information Protection provides enhanced data protection capabilities to customers and assists them with classification of data using labels and permissions. Azure Information Protection includes **Azure Rights Management**, which used to be a standalone Azure service.

Key Vault: Key Vault safeguards keys and other secrets in the cloud by using Hardware Security Modules (HSMs). Protects cryptographic keys and small secrets like passwords with keys stored in HSMs. For added assurance, customers can import or generate keys in HSMs that are FIPS 140-2 Level 2 certified. Key Vault is designed so that Microsoft does not see or extract customer keys. Customers can create new keys for Dev-Test in minutes and migrate seamlessly to production keys managed by security operations. Key Vault scales to meet the demands of cloud applications without the need to provision, deploy, and manage HSMs and key management software.

Multi-Factor Authentication (MFA): MFA helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. MFA follows organizational security and compliance standards while also addressing user demand for convenient access. MFA delivers strong authentication via a range of options, including mobile apps, phone calls, and text messages, allowing users to choose the method that works best for them.

Security Center: Security Center helps customers 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. Key capabilities include monitoring the security state of customer's Azure resources, policy-driven security maintenance, analysis of security data while applying advanced analytics, machine learning and behavioral analysis, prioritized security alerts as well as insights into the source of the attack and impacted resources.

Developer Tools

Application Insights: Application Insights is an all-in-one telemetry solution that can help customers detect issues, triage impact and solve problems in web apps and services. It provides deep diagnostics and real-time insights while being a seamless part of the Application Lifecycle Management (ALM) processes through Visual Studio, Visual Studio Team Services, and Azure Diagnostics integrations. It supports ASP.NET, J2EE and most of the popular web technologies for web apps on Azure or on customer's own servers.

Azure DevTest Labs: Azure DevTest Labs is a service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. Customers can test the latest version of your application by quickly provisioning Windows and Linux environments using reusable templates and artifacts.

Monitoring & Management

Automation: Automation lets customers create, deploy, monitor, and maintain resources in their Azure environment automatically by using a highly scalable and reliable workflow execution engine. Automation enables customers to create their PowerShell content (Runbooks) or choose from many available in the Runbook Gallery, and trigger job execution (scheduled or on-demand). Customers can also upload their own PowerShell modules and make use of them in their Runbooks. The distributed service takes care of executing the jobs per customer-specified schedule in a reliable manner, providing tenant context, tracking, and debugging as well as authoring experience.

Azure Advisor: Azure Advisor is a personalized recommendation engine that helps customers follow Azure best practices. It analyzes Azure resource configuration and usage telemetry, then provides recommendations that can reduce costs and improve the performance, security, and reliability of applications.

Azure Monitor: Azure Monitor is a centralized dashboard which provides detailed up-to-date performance and utilization data, access to the activity log that tracks every API call, and diagnostic logs that help customers debug issues in their Azure resources.

Azure Resource Manager: Azure Resource Manager enables customers to repeatedly deploy their app and have confidence that their resources are deployed in a consistent state. Customers can define the infrastructure and dependencies for their app in a single declarative template. This template is flexible enough to use for all customer environments such as test, staging, or production. If customers create a solution from the Azure Marketplace, the solution will automatically include a template that customers can use for their app. With Azure Resource Manager (ARM), customers can put resources with a common lifecycle into a resource group that can be deployed or deleted in a single action. Customers can see which resources are linked by any dependencies. Moreover, customers can control who in their organization can perform actions on the resources. Customers manage permissions by defining roles and adding users or groups to the roles. For critical resources, customers can apply an explicit lock that prevents users from deleting or modifying the resource. ARM logs all user actions so customers can audit those actions. For each action, the audit log contains information about the user, time, events, and status.

Log Analytics: Log Analytics lets customers collect, correlate and visualize all their machine data, such as event logs, network logs, performance data, and much more, from both on-premises and cloud assets. It enables transformation of machine data into near real-time operational intelligence for better decision making. Customers can search, correlate, or combine outputs of search from multiple data sources regardless of volume, format, or location. They can also visualize their data, separating signals from noise, with powerful log-management capabilities.

Microsoft Azure Portal: Microsoft Azure Portal builds, manages, and monitors all Azure resources in a single, unified console. Azure is designed to abstract much of the infrastructure and complexity that typically underlies applications (i.e., servers, operating systems, and network) so that developers can focus on building and deploying applications. Customers manage these Azure applications through the Azure Portal and Service Management API (SMAPI). Users who have access to Azure customer applications are authenticated based on their **Microsoft Accounts (MSA)** and / or **Organizational Accounts**. Azure customer billing is handled by **Microsoft Online Services Customer Portal (MOCP)**. MOCP and MSA / Organizational Accounts and their associated authentication mechanisms are not in scope for this SOC report.

Scheduler: Scheduler lets customers invoke actions that call HTTP/S endpoints or post messages to a Storage queue, Service Bus queue, or Service Bus topic on any schedule. Scheduler creates jobs that reliably call services either inside or outside of Azure and run those jobs right away, on a regular or irregular schedule, or at a future date.

Azure Supporting Infrastructure Services

Azure Supporting Infrastructure Services is a collection of internal services that are not directly available to third-party customers. They are included in SOC examination scope for Azure and Azure Government because they are critical to platform operations or support dependencies by first-party services, e.g., Office 365 and Dynamics 365.

Access Control Service (ACS): ACS is a feature of Azure Active Directory that provides a process of authenticating and authorizing users to gain access to web applications and services while allowing the features of authentication and authorization to be factored out of the code.

Azure Active Directory Application Proxy: Azure Active Directory Application Proxy provides Single Sign-on (SSO) and secure remote access for web applications hosted on-premises. This can include SharePoint sites, Outlook Web Access, or any other Line of Business (LOB) web applications customers have. These on-premises web applications are integrated with Azure Active Directory (AD), the same identity and control platform that is used by Office 365. End users can then access their on-premises applications the same way they access Office 365 and other SaaS applications integrated with Azure AD. Customers are not required to change the network infrastructure or require VPN to provide this solution for their users.

Azure Active Directory Connect Health[13]: Azure Active Directory Connect Health helps customers monitor and gain insight into their on-premises identity infrastructure and synchronization services by monitoring the health of identity servers and sending notification alerts, providing usage analytics and performance data trends, and reporting on-going activity on the servers.

Azure Active Directory Gateway (ADGateway): ADGateway is an Azure service that acts as a stateless front door / reverse proxy for all requests to other services in Azure AD. ADGateway does not implement any identity / authorization functionality and hence, does not have any customer specific state that is stored. It proxies the requests to the services behind it, routing them appropriately based on the URL and returns the responses from the services to the calling client.

Azure Active Directory Ibiza UX - Management UX[14]: Azure Active Directory Ibiza UX - Management UX is a stateless, UI-only extension to the Azure Management Portal that allows directory users in various administrative roles to manage all aspects of a lifecycle of objects in an Azure Active Directory (such as users, groups, applications, domains, policies etc.), in terms of creation, deletion, viewing and editing. It also enables access to various AAD features depending on the licensing level of the customer.

Azure Active Directory Portal Extension for Azure Portal (ADIUX): ADIUX is a stateless user interface service built on top of Ibiza SDK to be used in the Azure Portal to allow Role Based Access Control (RBAC) scenarios, such as enumerating roles, assigning and removing users and groups from roles and vice versa, inviting MSA users into directory in order to assign them to roles etc.

Azure Active Directory Privileged Identity Management[14]: Azure Active Directory Privileged Identity Management lets customers manage, control and monitor their privileged identities and their access to resources in Azure AD, and in other Microsoft online services such as Office 365 or Microsoft Intune. Azure AD Privileged Identity Management allows customers to see which users are Azure AD administrators; enables on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune; provides reports about administrator access history and changes in administrator assignments; provides alerting about access

[13] Controls for this service were tested from Q3 2017 through Q4 2017 (July 1, 2017 to December 31, 2017).

[14] Controls for this service were tested from Q2 2017 through Q4 2017 (April 1, 2017 to December 31, 2017).

to a privileged role. It can manage the built-in Azure AD organizational roles, such as Global Administrator, Billing Administrator, Service Administrator, User Administrator and Password Administrator.

IAM – Data Insights and Reporting Service (previously named "Azure Active Directory Reporting (AXM)")[13]: IAM – Data Insights and Reporting Service provides security and activity reports for Azure Active Directory available to customers.

IAM – Shared Backend Services (previously named "Azure Active Directory User Experience (ADUXP)"): IAM – Shared Backend Services acts as the core data layer that serves the Azure Portal Administrator UX, as well as portions of the Information Worker UX. This data layer connects with various components, including the core directory (MSODS) and OrgID / eSTS in order to provide these experiences.

Azure Device Registration Service (ADRS): ADRS enables customers' employees' devices to be provisioned with an identity. Once the customer sets a policy that allows only compliant devices to access the list of customer defined applications (including Office 365 applications), Azure AD authenticates the device and checks whether the device is compliant before allowing access to the customer defined applications such as Exchange and SharePoint.

Azure Front Door (AFD): AFD is a content delivery network service that acts as an Internet gateway for major Microsoft services, such as Bing, Office, MSN, and Skype. It is essentially a network layer between consumers (end users) and the Microsoft services they interface with, for routing user traffic to improve availability, performance, and consistency of user experiences for these services. AFD has multiple gateways distributed around the world through Microsoft datacenters including edge sites, which provides close network proximity to all clients. Once the customer (end user) traffic enters the AFD service, AFD will pick the best Microsoft service endpoint to route the traffic to via intelligent load balancing.

Azure Notification Services[13]: Azure Notification Services enables customers to receive notification for different Azure level outages, maintenance, and audit events.

Azure Monitor - IDC[13]: Azure Monitor - IDC provides mapping from Arm Id of a resource to Internal Id of that resource (and vice versa).

Azure Watson: Azure Watson is an internal tool for service troubleshooting and crash dump analysis.

Backend Health Management: Backend Health Management is available to first-party customers (e.g., Office 365, Dynamics 365) for the management of hyper-scale services used in high-availability scenarios. Customers are guaranteed a defined level of service health, health monitoring, reporting and alerting, secure communications between servers, secure Remote Desktop Protocol (RDP) capability, and full logical and physical machine lifecycle management.

Cloud App Discovery[13]: Cloud App Discovery is a premium feature of Azure Active Directory (AAD) that enables customers to discover cloud applications that are used by the employees in their organization.

Cloud Data Ingestion (CDI)[14]: CDI is a set of worker roles that reads sign-in and audit events from multiple sources like Evolved Security Token Service (eSTS), MSODS, IAM – Self Service Credentials Management Service etc. and ingest them into the data processing pipeline for products like Identity Protection Center (IPC) and audit reports in the Ibiza portal. CDI also has a web role that manages Event Hubs and storage for all the services in the data processing pipeline.

Custom Speech Service[13]: Custom Speech Service is a cloud based speech to text service that enables customers to customize and deploy acoustic and language models.

Common Data Service (CDS): CDS is a fully extensible data management application platform. CDS provides customers with the ability to bring their data together from across Microsoft Online Services (including Dynamics

365). Customers can then derive insights from this data with Power BI, build or extend applications with PowerApps and the CDS SDK, or automate business processes with Microsoft Flow.

Domain Name System - DNS (AzDNS, iDNS/Recursive Revolvers)

- **AzDNS**: AzDNS is a Domain Name System (DNS) service that hosts critical domains belonging to the Azure platform, as opposed to the customers' domains. For example, each new Storage account or Cloud Service gets a DNS name that is hosted in AzDNS. It is deployed to multiple datacenters globally and uses Anycast to route DNS queries to the closest site.
- **iDNS**: iDNS offers hostname to Dedicated Internet Protocol (DIP) resolution within the customers' Virtual Network (VNet). This allows different VMs / roles in the VNet to refer to each other by a friendly name rather than an IP. This service is Fabric deployed, i.e., 100% VM based, with three tenants and a Storage account in each region for resilience. Each region is independent of other regions in that the records are not stored in other regions and resolvers in other regions are not needed during either provisioning or resolution.
- **Recursive Resolvers (RR)**: Recursive Resolvers provide DNS resolution capabilities to Azure VMs and infrastructure. These servers do not host DNS zones, they perform the task of recursive resolution, which involves the traversal of public DNS records to resolve the name requested by the client. These servers access the Internet but do not provide any services to (and are not accessible from) parties outside of Azure. In each region, there is a cluster of resolvers and each VM / Host is configured with at least two clusters for resilience.

Datacenter Secrets Management Service (dSMS): dSMS is an Azure service that automates secrets generation, their delivery to the consumer services, and periodic rollover at runtime.

Datacenter Security Token Service (dSTS): dSTS provides a highly available and scalable security token service for authenticating and authorizing clients (users and services) of Azure foundation and essential services. Fabric Controller and Load Balancer are examples of Azure foundation services; Service Bus and Red Dog Front End (RDFE) are examples of Azure essential services.

Dynamics 365 Portal: Dynamics 365 Portal is where users can log-in and view an aggregated list of their business apps across various partner services including PowerApps.

Evolved Security Token Service (eSTS): eSTS provides a stateless service that accesses multiple principal and key stores. eSTS absorbs the roles of multiple STSs, so that users see one Azure AD STS. eSTS relies on MSODS to hold information required to complete the authentication. eSTS supports a number of protocols including OAuth 2.0, Open ID Connect, WS-Fed, and Security Assertion Markup Language (SAML) protocol.

Fabric / Compute Manager: Fabric / Compute Manager is a core Azure service that manages Fabric Controllers.

Hybrid Identity Service[13]: Hybrid Identity Service (HIS) is the backend service for tunneling requests from the cloud to resources on-premises. Current products include Pass-through Authentication (PTA), which allows Evolved Security Token Service (EvoSTS) to authenticate users against Active Directory on-premises.

Identity and Access Management Cloud Password Single Sign On (IAM - Password SSO): IAM - Password SSO provides customers the ability to use a single set of credentials to access both on-premises and online resources. This single set of credentials is managed in the customer's AD, and requires Active Directory Federation Services.

IAM – Management UX (previously named "Identity and Access Management Self Service Group Management (IAM – SSGM)"): IAM - Management UX supports group object Create, Read, Update, and Delete (CRUD) operations through Azure AD Graph API. The Graph API provides programmatic access to Azure AD through REST API endpoints. Applications can use the Graph API to perform CRUD operations on directory data and objects.

IAM – Self Service Credentials Management Service (previously named "Identity and Access Management Self Service Password Reset (IAM – SSPR)"): IAM - Self Service Credentials Management Service is a feature of Azure AD that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support.

Identity and Access Management Sync Fabric (IAM - SF): IAM - SF enables the automatic creation, management and removal of user identities in SaaS applications by connecting to provisioning endpoints provided by application vendors. The SF service ensures that the identities in SaaS applications remain current based on changes in Azure AD. Automated provisioning also extends to user groups.

IAM – Information Worker UX (previously named "Identity and Access Management User Experience (IAMUX)"): IAM – Information Worker UX is a simple Azure service that hosts various pages that information workers interact with to perform daily tasks like managing their profile, changing their passwords, and the like.

Jumpboxes: Jumpboxes are used by Azure service teams to operate Azure services. Jumpbox servers allow access to and from datacenters. They function as utility servers for runners, deployments, and debugging; building out new clusters; managing certificates; and, collecting diagnostics information from production systems. There are multiple Jumpboxes per datacenter. They may be shared inside each region, but typically, a Jumpbox located in one datacenter is used to operate just that datacenter. Jumpboxes are in their own Organizational Unit (OU) and Group Policy Object (GPO). Two-Factor Authentication (2FA) is required for access to all Jumpboxes.

Kusto: Kusto is a near real-time log analytics platform for interactive data exploration that enables Microsoft cloud service teams to understand what is happening across their services and to detect, diagnose, and repair problems. Kusto ingests over 1 trillion events and more than a petabyte of log data per day across hundreds of Microsoft cloud services. It has also been released to customers as Application Insights Analytics.

Managed Service Identity[14]: Managed Service Identity is an Azure service which enables Azure resources to gain secure identities. This, in turn, enables Azure resources to access high value assets using well-established protocols and using the Azure Active Directory as the identity provider. The service manages the issuing of credentials for a given identity, registering them with the directory, rotating them as necessary, and enables provisioning these credentials securely onto the resource host - all without user intervention or exposure to secrets.

MSODS: MSODS is Microsoft Online Directory Services, a feature of Azure Active Directory that also includes Azure Active Directory B2B.

OneDDoS: OneDDOS is a fully automated solution aimed primarily at protecting the underlying infrastructure from Distributed Denial of Service (DDoS) attacks. The OneDDoS mitigation system helps to prevent service interruptions by eliminating harmful volumetric traffic flows. Protecting the infrastructure ensures that attack traffic intended for one customer does not result in collateral damage or diminished network quality of service for other customers. The OneDDoS mitigation system is highly scalable and protects inbound, outbound, and region to region traffic.

OneDeploy Express v2: OneDeploy Express v2 offers a safe and secure method to rollout services to multiple regions across Azure. OneDeploy Express v2 rolls out ARM based templates for IaaS and PaaS services and allows users to 1) manage their rollout orchestration, 2) use system health checks for controlling how the rollouts are orchestrated in a safe manner, and 3) manage their keys and secrets necessary for deployments in Key Vault or dSMS.

OrgID: OrgID is an identity provider for Azure Active Directory. It provides authentication services for identities owned by enterprise customers of Microsoft's Cloud Services, including Azure and Office 365. It is an identity provider for "org-owned" identities that are hosted within cloud as well as a federation provider for identities that a customer prefers to host in their on-premises AD environment. OrgID is accessed via ADGateway. The

ADGateway service performs proxy and routing services between OrgID and other services, such as Evolved Security Token Service (eSTS).

PowerApps Authoring: PowerApps Authoring is a component service that supports the PowerApps service for authoring cross platform applications without the need to write code. It provides the service to visually compose the app using a browser, to connect to data using different connections and APIs, and to generate a packaged application that is published to the PowerApps Service. The packaged application can be previewed using the service while authoring or it can be shared and played on iOS, Android and Windows Phone.

PowerApps Portal: PowerApps Portal is the management website for PowerApps, where users can sign up for the product and perform management operations on PowerApps and related resources. It communicates directly with the PowerApps RP for most operations and provides entry points for users to launch into other PowerApps services as necessary.

PowerApps Resource Provider (RP): PowerApps RP is the back-end RESTful service for PowerApps that handles the management operations for PowerApps and related entities such as connections and APIs. Architecturally, the RP is an Azure Resource Manager (ARM) resource provider, meaning that incoming requests are authenticated by the ARM front door and proxied through to the RP.

Physical Network (PhyNet): PhyNet is used to provide all datacenter connectivity for Azure. PhyNet is completely transparent to Azure customers who cannot interact directly with any physical network device. The PhyNet service provides APIs to manage network devices in Azure datacenters. PhyNet is responsible for performing write operations to the network devices, including any operation that can change the code or configuration on the devices. The API exposed by PhyNet is used to perform certain operations, e.g., enable / disable a port for an unresponsive blade. PhyNet hosts all code and data necessary to manage network devices and does not have any dependency on services that are deployed after the build out.

Policy Administration Service (PAS): PAS is responsible for providing Role Based Access Control (RBAC) capability to an application. Applications can use this capability to create access policy.

Protection Center[14]: Protection Center is a cloud security service that uses state of the art machine learning to analyze terabytes of behavioral and contextual data every day to detect and prevent attempts to attack organizations' Azure AD accounts. This service helps prevent the use of compromised accounts using industry leading machine learning (ML) based real time detection and automated mitigation, helping protect all of the cloud and on-premise applications customers use with Azure AD. Azure AD Identity Protection also notifies the identity admins or security analysts when new compromised users, risky sign-ins, or configuration vulnerabilities are detected in their environment. If Conditional Access policies are enabled, administrators and security analysts can prevent and/or remediate these risks before they are exploited.

RDFE: RDFE is a communication path from the user to the Fabric used to manage Azure services. RDFE represents the publicly exposed classic APIs, which is the front end to the Azure Portal and the Service Management API (SMAPI). All requests from the user go through the RDFE or the new Azure Resource Manager (ARM).

Red Dog Operating System (RDOS): RDOS provides all Guest and Host Operating Systems for the virtual environment and the services hosted on Azure.

Resource Providers: Resource Providers enables seamless, automated deployment of Compute, Storage, and Networking resources as needed and on demand using the Azure Resource Manager (ARM) templates.

- **Compute Resource Provider (CRP)**: CRP, also referred to as **Compute Platform (CP)** offers the regional Control Plane for all IaaS-related services. It is always paired with the Network Resource Provider (NRP), Storage Resource Provider (SRP) and the Azure Resource Manager (ARM) as a complete offering.
- **Network Resource Provider (NRP)**: NRP, is a regional, highly-available, scalable frontend service for Azure Networking that exposes consistent APIs through the Azure Resource Manager. By being compatible

with the Azure Resource Manager, role-based access control, integration with the Azure portal, and template-based deployments are all supported. NRP works with CRP to provide the network support for creating and managing VMs and VM Scale Sets.

- **Storage Resource Provider (SRP)**: SRP, enables customers to manage storage accounts and their keys programmatically.

Service Fabric - Resource Provider (RP) Clusters: Service Fabric - RP Clusters provide the runtime and VM hosting capabilities for the core Azure resource providers which include Compute Platform and Network Resource Provider.

WANetMon: WANetMon is a network monitoring tool used primarily by the Operations team to monitor and troubleshoot issues within the Azure network. WANetMon collects different types of data (e.g., Simple Network Management Protocol (SNMP) counters, syslogs, traps) from network devices, processes and corresponding alerts. The Operations team can view this data while troubleshooting networking issues. WANetMon also collects and monitors availability data at datacenter and cluster levels and provides alerts when there is a drop in availability.

Workflow: Workflow provides a highly scalable environment where workflows authored by customers in the Office 365 platform can execute. SharePoint Online allows workflows to be attached to SharePoint sites or lists. This feature enables customers to automate numerous human and document management processes. For every customer who signs up with SharePoint Online, a corresponding tenant is created in the Workflow service (called a scope). Customers who have signed up for Office 365 need not sign up for the Workflow service; setup and configuration of Workflow happens automatically. When the customer authors a SharePoint Workflow and deploys it, SharePoint Online calls into the Workflow service to execute the workflow. Office 365 services including SharePoint Online are not in scope of this SOC report.

Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS): MCAS is a comprehensive service that provides customers the ability to extend their on-premise controls to their cloud applications and provide deeper visibility, comprehensive controls, and improved protection for these apps. MCAS provides Shadow IT discovery, information protection to cloud applications, threat detection and in-session controls.

Microsoft Flow

Microsoft Flow: Microsoft Flow is a product to help customers set up automated workflows between their favorite apps and services to synchronize files, get notifications, collect data, and more.

Microsoft Graph

Microsoft Graph: Microsoft Graph exposes multiple APIs from Office 365 and other Microsoft cloud services through a single endpoint: https://graph.microsoft.com. Microsoft Graph and Microsoft Graph Webhooks simplifies queries that would otherwise be more complex. Customers can use Microsoft Graph and Microsoft Graph Webhooks to:

- Access data from multiple Microsoft cloud services, including Azure Active Directory, Exchange Online as part of Office 365, SharePoint, OneDrive, OneNote, and Planner.
- Navigate between entities and relationships.
- Access intelligence and insights from the Microsoft cloud (for commercial users).

Microsoft Intune

Microsoft Intune: Microsoft Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud. Using Intune, organizations can provide their employees with access to corporate applications, data, and resources from virtually anywhere on almost any device, while helping to keep corporate information secure.

Microsoft Power BI

Power BI: Power BI and Power BI Embedded are a suite of business analytics tools to analyze data and share insights. Power BI dashboards provide a 360-degree view for business users with their most important metrics in one place, updated in real time, and available on all of their devices. With one click, users can explore the data behind their dashboard using intuitive tools that make finding answers easy. Power BI facilitates creation of dashboards with over 50 connections to popular business applications, and comes with pre-built dashboards crafted by experts that help customers get up and running quickly. And customers can access their data and reports from anywhere with the Power BI Mobile apps, which update automatically with any changes to customers data.

Microsoft PowerApps

PowerApps: PowerApps enables customers to connect to their existing systems and create new data, build apps without writing code, and publish and use the apps on the web and mobile devices.

Microsoft Stream

Microsoft Stream: Microsoft Stream provides a common destination for video management, with built-in intelligence features, and the IT management and security capabilities that businesses of all sizes require. It's a fully managed SaaS service for enterprise customers in which users can upload, share and view videos within a small team, or across an entire organization, all inside a securely managed environment. Microsoft Stream leverages cognitive services that enable in-video face detection and speech-to-text transcription that enhances learning and productivity. Microsoft Stream also includes IT admin capabilities for managing video content and increases engagement within an organization by integrating video into the applications used every day. Microsoft Stream utilizes built-in, industry-leading encryption and authenticated access to ensure videos are shared securely.

Data

Customers upload data for storage or processing within the services or applications that are hosted on the cloud services platform. In addition, certain types of data are provided by the customers or generated on the customer's behalf to enable the usage of the cloud services. Microsoft only uses customer data in order to support the provisioning of the services subscribed to by the customers in accordance with the Service Level Agreements (SLAs). **System Metadata** is configuration, usage and event data, that does not have customer data or any other category of data described above.

Data Ownership

Microsoft does not inspect, approve, or monitor applications that customers deploy to Azure. Moreover, Microsoft does not know what kind of data customers choose to store in Azure. Microsoft does not claim data ownership over the customer information entered into Azure. Azure's Agreement states, "Customers are solely responsible for the content of all Customer Data. Customers will secure and maintain all rights in Customer Data necessary for Azure to provide the Online Services to them without violating the rights of any third party or otherwise obligating Microsoft to them or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to their use of the Product other than as expressly set forth in the Agreement or as required by applicable law."