Microsoft

Microsoft Corporation - Azure Including Dynamics 365

(Azure & Azure Government)

SOC 3 Report

April 1, 2019 - March 31, 2020

Table of contents

Section I:
Independent Service Auditors’ Report

Deloitte & Touche LLP
925 Fourth Avenue
Suite 3300
Seattle, WA 98104-1126
USA

Tel: 206-716-7000
Fax: 206-965-7000
www.deloitte.com

Section I: Independent Service Auditors' Report

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

Scope

We have examined Microsoft Corporation's (the "Service Organization" or "Microsoft") accompanying assertion titled "Management's Assertion" ("assertion") that the controls within Microsoft's in-scope services and offerings for its Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters for Azure and Azure Government cloud environments ("system") were effective throughout the period April 1, 2019 to March 31, 2020[1], to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria")[2] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved. Microsoft has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Microsoft is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Our examination included:

- Obtaining an understanding of the system and Microsoft's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Service Organization's system were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte & Touche LLP

April 30, 2020

Section II:
Management Assertion

Section II: Management's Assertion

Microsoft Azure's Management Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Microsoft Corporation (the "Service Organization" or "Microsoft") related to in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters for Azure and Azure Government cloud environments throughout the period April 1, 2019 to March 31, 2020[3], to provide reasonable assurance that Microsoft's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality ("applicable trust services criteria")[4] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Microsoft's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2019 to March 31, 2020, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria.

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

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

Section III:
Description of the Boundaries of the Microsoft Azure System

Section III: Description of the Boundaries of the Microsoft Azure System

Overview of Operations

Business Description

Azure

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, Microsoft Dynamics 365, and 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 offerings and Online Services that are in scope for this report.

Dynamics 365

Dynamics 365 is an online business application suite that integrates the Customer Relationship Management (CRM) capabilities and its extensions with the Enterprise Resource Planning (ERP) capabilities. These end-to-end business applications help customers turn relationships into revenue, earn customers, and accelerate business growth.

"Azure", when referenced in this report, comprises of "Microsoft Azure", "Microsoft Dynamics 365", "Online Services", and the supporting datacenters listed in this report.

Azure and Azure Government Report Scope Boundary

Azure is 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 and offerings are in scope for this report:

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
		Microsoft Datacenters					
Microsoft Datacenter and Operations Service		✓	✓	✓	✓	✓	✓
		Azure					
Compute	App Service	✓	✓	✓	✓	✓	✓
	Azure Functions	✓	✓	✓	✓	✓	✓
	Azure Service Fabric	✓	✓	✓	✓	✓	✓
	Batch	✓	✓	✓	✓	✓	✓
	Cloud Services[6]	✓	✓	✓	✓	✓	✓
	Virtual Machines	✓	✓	✓	✓	✓	✓
	Virtual Machine Scale Sets	✓	✓	✓	✓	✓	✓
Containers	Azure Container Service[7]	✓	✓	✓	✓	✓	✓
	Azure Kubernetes Service (AKS)[7]	✓	✓	✓	✓	✓	✓
	Azure Red Hat OpenShift (ARO)	✓	-	-	-	✓	✓
	Container Instances[7]	✓	✓	✓	✓	✓	✓
	Container Registry	✓	✓	✓	✓	✓	✓
Networking	Application Gateway	✓	✓	✓	✓	✓	✓
	Azure Bastion	✓	✓	-	-	✓	✓
	Azure DDoS Protection[7]	✓	✓	✓	✓	✓	✓
	Azure DNS	✓	✓	✓	✓	✓	✓

[5] Examination period scope Q4 FY19 extends from April 1, 2019 to June 30, 2019.
Examination period scope Q1 FY20 extends from July 1, 2019 to September 30, 2019.
Examination period scope Q2 FY20 extends from October 1, 2019 to December 31, 2019.
Examination period scope Q3 FY20 extends from January 1, 2020 to March 31, 2020.

[6] Offerings for which AICPA Processing Integrity trust service criteria were examined: Cloud Services, Azure Resource Manager (ARM), Microsoft Azure Portal and Azure Service Manager (RDFE).

[7] Examination period for this offering / service for Azure was from April 1, 2019 to March 31, 2020, while the examination period for Azure Government was from October 1, 2019 to March 31, 2020.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Azure ExpressRoute	✓	✓	✓	✓	✓	✓
	Azure Firewall	✓	✓	✓	✓	✓	✓
	Azure Firewall Manager	✓	-	-	-	-	✓
	Azure Front Door[7]	✓	✓	✓	✓	✓	✓
	Azure Internet Analyzer	✓	-	-	-	✓	✓
	Azure Private Link	✓	✓	-	-	✓	✓
	Azure Web Application Firewall	✓	✓	-	-	✓	✓
	Content Delivery Network	✓	-	✓	✓	✓	✓
	Load Balancer	✓	✓	✓	✓	✓	✓
	Network Watcher	✓	✓	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓	✓	✓
	Virtual Network	✓	✓	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓	✓	✓
	Virtual WAN	✓	✓	-	-	✓	✓
Storage	Azure Archive Storage[7]	✓	✓	✓	✓	✓	✓
	Azure Backup	✓	✓	✓	✓	✓	✓
	Azure Data Box	✓	✓	-	-	✓	✓
	Azure Data Lake Storage Gen1	✓	-	✓	✓	✓	✓
	Azure File Sync[7]	✓	✓	✓	✓	✓	✓
	Azure HPC Cache	✓	-	-	-	✓	✓
	Azure Import/Export	✓	✓	✓	✓	✓	✓
	Azure Site Recovery	✓	✓	✓	✓	✓	✓
	Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables) including Cool and Premium	✓	✓	✓	✓	✓	✓
	Azure Ultra Disk	✓	-	-	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	StorSimple	✓	✓	✓	✓	✓	✓
Databases	Azure API for FHIR	✓	-	✓	✓	✓	✓
	Azure Cache for Redis	✓	✓	✓	✓	✓	✓
	Azure Cosmos DB	✓	✓	✓	✓	✓	✓
	Azure Database for MariaDB[7]	✓	✓	✓	✓	✓	✓
	Azure Database for MySQL[7]	✓	✓	✓	✓	✓	✓
	Azure Database for PostgreSQL[7]	✓	✓	✓	✓	✓	✓
	Azure Database Migration Service	✓	-	✓	✓	✓	✓
	Azure SQL Database	✓	✓	✓	✓	✓	✓
	Azure Synapse Analytics	✓	✓	✓	✓	✓	✓
	SQL Server on Virtual Machines	✓	✓	✓	✓	✓	✓
Developer Tools	Azure DevTest Labs	✓	✓	✓	✓	✓	✓
	Azure Lab Services	✓	✓	✓	✓	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓	✓	✓	✓
	Azure Data Explorer	✓	✓	✓	✓	✓	✓
	Azure Data Share	✓	-	-	-	✓	✓
	Azure Stream Analytics[7]	✓	✓	✓	✓	✓	✓
	Data Catalog	✓	-	✓	✓	✓	✓
	Data Factory	✓	✓	✓	✓	✓	✓
	Data Lake Analytics	✓	-	✓	✓	✓	✓
	HDInsight	✓	✓	✓	✓	✓	✓
	Power BI Embedded	✓	✓	✓	✓	✓	✓
AI + Machine Learning	AI Builder	✓	-	-	-	✓	✓
	Azure Bot Service	✓	✓	✓	✓	✓	✓
	Azure Open Datasets	✓	-	-	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Azure Machine Learning	✓	-	✓	✓	✓	✓
	Cognitive Services	✓	✓	✓	✓	✓	✓
	Cognitive Services: Anomaly Detector	✓	-	-	-	✓	✓
	Cognitive Services: Computer Vision	✓	✓	✓	✓	✓	✓
	Cognitive Services: Content Moderator	✓	✓	✓	✓	✓	✓
	Cognitive Services: Custom Vision	✓	-	✓	✓	✓	✓
	Cognitive Services: Face	✓	✓	✓	✓	✓	✓
	Cognitive Services: Form Recognizer	✓	-	-	-	✓	✓
	Cognitive Services: Language Understanding	✓	✓	✓	✓	✓	✓
	Cognitive Services: Translator	✓	✓	✓	✓	✓	✓
	Cognitive Services: Personalizer	✓	-	-	-	✓	✓
	Cognitive Services: QnA Maker	✓	-	✓	✓	✓	✓
	Cognitive Services: Speech Services[7]	✓	✓	✓	✓	✓	✓
	Cognitive Services: Text Analytics	✓	✓	✓	✓	✓	✓
	Cognitive Services: Video Indexer	✓	-	✓	✓	✓	✓
	Machine Learning Studio (Classic)	✓	-	✓	✓	✓	✓
	Microsoft Genomics	✓	-	✓	✓	✓	✓
	Microsoft Healthcare Bot	✓	-	✓	✓	✓	✓
Internet of Things	Azure IoT Central	✓	-	✓	✓	✓	✓
	Azure IoT Hub	✓	✓	✓	✓	✓	✓
	Event Grid	✓	✓	✓	✓	✓	✓
	Event Hubs	✓	✓	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
	Notification Hubs	✓	✓	✓	✓	✓	✓
	Time Series Insights	✓	-	-	✓	✓	✓
	Windows 10 IoT Core Services	✓	-	-	-	✓	✓
Integration	API Management	✓	✓	✓	✓	✓	✓
	Logic Apps	✓	✓	✓	✓	✓	✓
	Service Bus	✓	✓	✓	✓	✓	✓
Identity	Azure Active Directory	✓	✓	✓	✓	✓	✓
	Azure Active Directory B2C	✓	-	✓	✓	✓	✓
	Azure Active Directory Domain Services	✓	-	✓	✓	✓	✓
	Azure Information Protection	✓	✓	✓	✓	✓	✓
Management and Governance	Automation	✓	✓	✓	✓	✓	✓
	Azure Advisor	✓	✓	✓	✓	✓	✓
	Azure Blueprints	✓	-	-	✓	✓	✓
	Azure Lighthouse	✓	✓	-	-	✓	✓
	Azure Managed Applications[8]	✓	✓	-	✓	✓	✓
	Azure Migrate	✓	✓	✓	✓	✓	✓
	Azure Monitor	✓	✓	✓	✓	✓	✓
	Azure Policy	✓	✓	✓	✓	✓	✓
	Azure Resource Graph	✓	✓	-	-	✓	✓
	Azure Resource Manager (ARM)[6]	✓	✓	✓	✓	✓	✓
	Cloud Shell[7]	✓	✓	✓	✓	✓	✓
	Microsoft Azure Portal[6]	✓	✓	✓	✓	✓	✓
	Scheduler	✓	✓	✓	✓	✓	✓

[8] Examination period for this offering / service for Azure was from July 1, 2019 to March 31, 2020, while the examination period for Azure Government was from October 1, 2019 to March 31, 2020.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[5]			
		Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Security	Azure Advanced Threat Protection[7]	✓	✓	✓	✓	✓	✓
	Azure Dedicated HSM[7]	✓	✓	✓	✓	✓	✓
	Azure Security Center	✓	✓	✓	✓	✓	✓
	Azure Sentinel	✓	-	-	✓	✓	✓
	Customer Lockbox for Microsoft Azure	✓	-	-	-	✓	✓
	Key Vault	✓	✓	✓	✓	✓	✓
	Multi-Factor Authentication	✓	✓	✓	✓	✓	✓
Media	Azure Media Services	✓	✓	✓	✓	✓	✓
Web	Azure Cognitive Search[7]	✓	✓	✓	✓	✓	✓
	Azure SignalR Service	✓	-	✓	✓	✓	✓
Internal Supporting Services[6,9]		✓	✓	✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Online Services						
Intune[7]	✓	✓	✓	✓	✓	✓
Microsoft Cloud App Security[7]	✓	✓	✓	✓	✓	✓
Microsoft Defender Advanced Threat Protection[7]	✓	✓	✓	✓	✓	✓
Microsoft Graph[7]	✓	✓	✓	✓	✓	✓
Microsoft Managed Desktop	✓	-	✓	✓	✓	✓

[9] Azure Government scope boundary for internal services: AsimovEventForwarder, Azure Networking, Azure RBAC Ibiza UX (Hosted extension), Azure Security Monitoring (ASM SLAM), Azure Stack Bridge, Azure Stack Edge Service, Azure Watson, CEDIS-Active Directory Domain Services, CEDIS-Active Directory Federation Services, CEDIS-Azure Active Directory, Cloud Data Ingestion, Compute Manager, dSCM, dSMS, dSTS, Geneva Actions, Geneva Warm Path, IAM - Management Admin UX, OneDS Collector, PilotFish, Protection Center, WANetMon, Windows Azure Jumpbox, Workflow. The coverage period for internal services for both Azure and Azure Government is Q4 FY19 through Q3 FY20 except for those specified with shorter coverage periods in the *Internal Supporting Services* subsection herein.

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Stream	✓	-	✓	✓	✓	✓
Microsoft Threat Experts	✓	-	-	-	✓	✓
Microsoft Threat Protection[7]	✓	✓	✓	✓	✓	✓
Power Apps	✓	✓	✓	✓	✓	✓
Power Automate	✓	✓	✓	✓	✓	✓
Power BI	✓	✓	✓	✓	✓	✓
Power Virtual Agents	✓	-	-	-	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[5]			
	Azure	Azure Government	Q4 FY19	Q1 FY20	Q2 FY20	Q3 FY20
Microsoft Dynamics 365						
Dynamics 365 AI Customer Insights	✓	-	✓	✓	✓	✓
Dynamics 365 Business Central	✓	-	✓	✓	✓	✓
Dynamics 365 Commerce	✓	-	✓	✓	✓	✓
Dynamics 365 Customer Engagement	✓	✓	✓	✓	✓	✓
Dynamics 365 Customer Service	✓	✓	✓	✓	✓	✓
Dynamics 365 Field Service	✓	✓	✓	✓	✓	✓
Dynamics 365 Finance	✓	-	✓	✓	✓	✓
Dynamics 365 Fraud Protection	✓	-	-	✓	✓	✓
Dynamics 365 Human Resources	✓	-	✓	✓	✓	✓
Dynamics 365 Marketing	✓	-	-	✓	✓	✓
Dynamics 365 Portals	✓	✓	✓	✓	✓	✓
Dynamics 365 Project Service Automation	✓	-	✓	✓	✓	✓
Dynamics 365 Sales	✓	✓	✓	✓	✓	✓
Dynamics 365 Supply Chain Management	✓	-	-	-	✓	✓

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:

Domestic Datacenters

West US
- Santa Clara, CA (BY1/2/3/4/5[10]/21/22/24[10]/30[11])
- San Jose, CA (SJC31)

West US 2
- Quincy, WA (CO1/2, MWH01/02[10]/03[10])

West Central US
- Cheyenne, WY (CYS01/04/05[10])

Central US
- Des Moines, IA (DM1/2/3, DSM05/06[10]/08[10])

USGOV Iowa
- Des Moines, IA (DM2)

North Central US
- Chicago, IL (CH1/3/4[10], CHI20/21[10])

USGOV Arizona
- Phoenix, AZ (PHX20/21[10])

South Central US
- San Antonio, TX (SN1/2/3/4/6, SAT09[11])

USGOV Texas
- San Antonio, TX (SN5)

East US
- Bristow, VA (BLU)
- Reston, VA (BL4/31[11])
- Sterling, VA (BL20)
- Ashburn, VA (BL2/3/5/6/7/21[10]/22[10]/23[10]/30)
- Manassas, VA (MNZ20[10])

East US 2
- Boydton, VA (BN1/3/4/6/7[10]/8[10]/14[10])

USGOV Virginia
- Boydton, VA (BN1)

USDoD East
- Boydton, VA (BN3)

[10] Examination period for this datacenter was from October 1, 2019 to March 31, 2020.

[11] Examination period for this datacenter was from July 1, 2019 to March 31, 2020.

International Datacenters

Canada East

- Quebec, Canada (YQB20)

Canada Central

- Toronto, Canada (YTO20/21[10])

Brazil South

- Campinas, Brazil (CPQ01/02/20)
- Sao Paulo, Brazil (GRU)

Brazil Southeast

- Rio de Janeiro, Brazil (RIO01)

Brazil Northeast

- Fortaleza, Brazil (FOR01)

Chile Central

- Santiago, Chile (SCL01)

West Europe

- Amsterdam, Netherlands (AM1/2/3, AMS04/05/06/07[10]/20/21[11]/23[10])
- Luxembourg A: SecureIT (LUA[10])

East Europe

- Vienna, Austria (VIE)

North Europe

- Dublin, Ireland (DB3/4/5, DUB06/07/08/11[10]/20/21[10]/24/31[10])

North Europe 2

- Vantaa, Finland (HEL01)

UK North

- Durham, United Kingdom (MME20)

UK South

- London, United Kingdom (LON21/22[11]/23[11]/24[11])

UK South 2

- London, United Kingdom (LON20)

UK West

- Cardiff, United Kingdom (CWL20)

East Asia

- Hong Kong (HK1/2, HKG20/21[10])

West India

- Mumbai, India (BOM01)

Central India

- Dighi, India (PNQ01)

South India

- Ambattur, India (MAA01)

Japan West

- Osaka, Japan (OSA01/02/20/21[10]/22[10])

Japan East

- Tokyo, Japan (KAW, TYO01/20/21/22/31[10])

Southeast Asia

- Singapore (SG1/2/3, SIN20)

Southeast Asia 2

- Cyberjaya, Malaysia (KUL01)

Korea South

- Busan, South Korea (PUS01/20)

Korea Central

- Seoul, South Korea (SEL20/21[11])

UAE Central

- Abu Dhabi (AUH20)

UAE North

- Dubai (DXP20)

Australia East

- Macquarie Park, Australia (SYD03)
- Sydney, Australia (SYD21/22/23[10]/25[10])

Australia Southeast

- Melbourne, Australia (MEL01/20[10]/21[10])

Australia Central

- Canberra, Australia (CBR20/21)

International Datacenters

France Central

- Paris, France (PAR20/21/22/23[10])

France South

- Marseille, France (MRS20)

Germany North

- Berlin, Germany (BER20[12])

Germany West Central

- Frankfurt, Germany (FRA21[12])

Switzerland West

- Geneva, Switzerland (GVA20[11])

Switzerland North

- Zurich, Switzerland (ZRH20[11])

South Africa North

- Johannesburg, South Africa (JNB20/21/22)

South Africa West

- Cape Town, South Africa (CPT20)

Norway East

- Oslo, Norway (OSL20[10])

Norway West

- Stavanger, Norway (SVG20[10])

[12] Examination period for this datacenter was from May 1, 2019 to March 31, 2020.

Edge Sites

- Ashburn, VA (ASH)
- Athens, Greece (ATH01)
- Atlanta, GA (ATA)
- Auckland, New Zealand (AKL01)
- Bangkok, Thailand (BKK30)
- Barcelona, Spain (BCN30)
- Berlin, Germany (BER30)
- Boston, MA (BOS01/31[13])
- Brisbane, Australia (BNE01)
- Brussels, Belgium (BRU30)
- Bucharest, Romania (BUH01)
- Budapest, Hungary (BUD01)
- Busan, South Korea (PUS03)
- Cape Town, South Africa (CPT02)
- Chicago, IL (CHG)
- Copenhagen, Denmark (CPH30)
- Dallas, TX (DAL)
- Denver, CO (DEN02)
- Dubai, United Arab Emirates (DXB30)
- Frankfurt, Germany (FRA)
- Geneva, Switzerland (GVA30[13])
- Helsinki, Finland (HEL03)
- Hong Kong (HKB)
- Honolulu, HI (HNL01)
- Houston, TX (HOU01)
- Hyderabad, India (HYD30[14])
- Jakarta, Indonesia (JKT30[13])
- Johannesburg, South Africa (JNB02)
- Kuala Lumpur, Malaysia (KUL30)
- Las Vegas, NV (LAS01)
- Lisbon, Portugal (LIS01)
- Los Angeles, CA (LAX)
- Lagos, Nigeria (LOS30[13])
- Madrid, Spain (MAD30)
- Manchester, United Kingdom (MAN30)
- Manila, Philippines (MNL30)
- Marseille, France (MRS01)
- Munich, Germany (MUC30[13])
- Nairobi, Kenya (NBO30[13])
- Queretaro, Mexico (MEX30)
- Miami, FL (MIA)
- Milan, Italy (MIL30)
- Montreal, Canada (YMQ01)
- Mumbai, India (BOM02)
- New Delhi, India (DEL01)
- Newark, NJ (EWR30)
- Osaka, Japan (OSA31[13])
- Oslo, Norway (OSL30[13])
- New York City, NY (NYC)
- Paris, France (PAR02/PRA)
- Perth, Australia (PER01/30[13])
- Phoenix, AZ (PHX01)
- Portland, OR (PDX31[14])
- Prague, Czech Republic (PRG01)
- Sao Paulo, Brazil (SAO03[13])
- San Jose, CA (SJC)
- Santiago, Chile (SCL30)
- Seattle, WA (WST)
- Seoul, South Korea (SLA)
- Sofia, Bulgaria (SOF01)
- Stockholm, Sweden (STO)
- Taipei, Taiwan (TPE30)
- Tokyo, Japan (TYA/TYB)
- Toronto, Canada (YTO01)
- Vancouver, Canada (YVR01)
- Warsaw, Poland (WAW01)
- Zagreb, Croatia (ZAG30)
- Zurich, Switzerland (ZRH)

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.

People

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

[13] Examination period for this edge site was from October 1, 2019 to March 31, 2020.

[14] Examination period for this edge site was from July 1, 2019 to March 31, 2020.

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 + AI Security

The Cloud + AI Security team works to make Azure a secure and compliant cloud platform by building common security technologies, tools, processes, and best practices. The Cloud + AI 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 and Offerings

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

Compute

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 Apps, 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 Functions: Azure Functions is a serverless compute service that lets customers run event-triggered code without having to explicitly provision or manage infrastructure. Azure Functions is an event driven, compute-on-demand experience. Customers can leverage Azure Functions to build HTTP endpoints accessible by mobile and Internet of Things (IoT) devices.

Azure Service Fabric: Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. It is a micro-services platform used to build scalable managed applications for the cloud. Azure Service Fabric addresses significant challenges in developing and managing cloud applications by allowing developers and administrators to shift focus from infrastructure maintenance to implementation of mission-critical, demanding workloads.

Batch: Batch runs large-scale parallel applications and High-performance Computing (HPC) workloads efficiently in the cloud. It allows customers to schedule compute-intensive tasks and dynamically adjust resources for their solution without managing the infrastructure. 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 is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. Cloud Services is hosted on virtual machines. However, customers have more control over the VMs. Customers can install their own software on VMs that use Cloud Services and access them remotely. It removes the need to manage server infrastructure and lets customers build, deploy, and manage modern applications with web and worker roles.

Virtual Machines: Virtual Machines is one of the several types of on-demand, scalable computing resources that Azure offers. Virtual Machines, which includes Azure Reserved Virtual Machine Instances, lets customers deploy a Windows Server or a Linux image in the cloud. Customers can select images from a marketplace or use their own customized images. It gives customers the flexibility of virtualization without having to buy and maintain the physical hardware that runs it.

Virtual Machine Scale Sets: Virtual Machine Scale Sets service lets customers create and manage a group of identical, load balanced, and autoscaling VMs. It 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, are fully integrated with Azure load balancing and autoscaling, and support Windows and / or Linux custom images, and extensions.

Containers

Azure Kubernetes Service (AKS): Azure Kubernetes Service is an enterprise ready managed service that allows customers to run Open source Kubernetes on Azure without having to manage it on their own. It also includes the functionality of Azure Container service (ACS), which was retired in calendar year Q1 2020. ACS was a container hosting environment which provided users the choice of container orchestration platforms such as Mesosphere DC/OS and Docker Swarm. AKS makes deploying and managing containerized applications easy. It offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance. AKS unites the customer development and operations teams on a single platform to rapidly build, deliver, and scale applications with confidence.

Azure Red Hat OpenShift (ARO): Azure Red Hat OpenShift offering provides flexible, self-service deployment of fully managed OpenShift clusters. It helps customers maintain regulatory compliance and focus on their application development, while the master, infrastructure, and application nodes are patched, updated, and monitored by both Microsoft and Red Hat.

Container Instances: Container Instances enables the creation of containers as first-class objects in Azure, without requiring VM management and without enforcing any prescriptive application model. Container Instances is a solution for any scenario that can operate in isolated containers, without orchestration. Customer can run event-driven applications, quickly deploy from their container development pipelines, and run data processing and build jobs.

Container Registry: 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, Azure Service Fabric, and others. Developers can manage the configuration of apps isolated from the configuration of the hosting environment. Container Registry 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.

Networking

Application Gateway: Application Gateway is a web traffic load balancer that enables customers to manage traffic to their web applications. It is an Azure-managed layer-7 solution providing HTTP load balancing, Web Application Firewall (WAF), Transport Layer Security (TLS) termination service, and session-based cookie affinity to Internet-facing or internal web applications.

Azure Bastion: Azure Bastion is a managed PaaS service that provides secure and seamless RDP and SSH access to customer's virtual machines directly through the Azure Portal. Azure Bastion is provisioned directly in the customer Virtual Network (VNet) and supports all VMs in their VNet using SSL without any exposure through public IP addresses.

Azure DDoS Protection: Azure DDoS Protection is a fully automated solution aimed primarily at protecting resources against Distributed Denial of Service (DDoS) attacks. Azure DDoS Protection helps prevent service interruptions by eliminating harmful volumetric traffic flows.

Azure DNS: Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. Azure DNS lets customers host their Domain Name System (DNS) domains alongside their Azure apps and manage DNS records by using the same credentials, APIs, tools, and billing as their other Azure services.

Azure ExpressRoute: Azure ExpressRoute lets customers create private connections between Azure datacenters and customer's infrastructure located on-premises or in a colocation environment. ExpressRoute connections do not go over the public Internet, and offer more reliability, faster speeds, and lower latencies than typical Internet connections.

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. Customers can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for virtual network resources allowing outside firewalls to identify traffic originating from a virtual network. This service is fully integrated with Azure Monitor Essentials for logging and analytics purposes.

Azure Firewall Manager: Azure Firewall Manager is a security management service that provides central security policy and route management for cloud-based security perimeters. Azure Firewall Manager simplifies central configuration and management of rules for multiple Azure Firewall instances, across Azure regions and subscriptions. This allows customers to automate Azure Firewall deployment to multiple secured virtual hubs and integrates with trusted security partner solutions for advanced services.

Azure Front Door: Azure Front Door (AFD) is Microsoft's highly available and scalable Web Application Acceleration Platform, Global HTTP Load Balancer, Application Protection and Content Delivery Network. AFD enables customers to build, operate and scale out their dynamic web application and static content. AFD provides customers' application with end-user performance, unified regional / stamp maintenance automation, Business Continuity and Disaster Recovery (BCDR) automation, unified client / user information, caching and service insights.

Azure Internet Analyzer: Azure Internet Analyzer is a client-side measurement platform that tests how changes to customer's networking infrastructure impact their client's / end-user's performance. Internet Analyzer uses a small JavaScript client embedded in the customer's web application to measure the latency from their end-users to customer selected set of network destinations (endpoints). Internet Analyzer allows customers to set up multiple side-by-side tests, allowing to evaluate a variety of scenarios as their infrastructure and needs evolve. It provides custom and preconfigured endpoints, providing a customer both the convenience and flexibility to make trusted performance decisions for their end-users.

Azure Private Link: Azure Private Link provides private connectivity from a virtual network to Azure PaaS, customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public Internet.

Azure Web Application Firewall: Azure Web Application Firewall (WAF) helps protect customer's web apps from malicious attacks and top 10 Open Web Application Security Project (OWASP) security vulnerabilities, such as SQL injection and cross-site scripting. Cloud-native Azure Web Application Firewall service deploys in minutes and offers customized rules that meet the customer's web app security requirements.

Content Delivery Network: Content Delivery Network (CDN) sends audio, video, applications, images, and other files faster and more reliably to customers by using the servers that are closest to each user. This dramatically increases speed and availability. Due to its distributed global scale, CDN can handle sudden traffic spikes and heavy loads without new infrastructure costs or capacity worries. CDN is built on a highly scalable, reverse-proxy architecture with sophisticated DDoS identification and mitigation technologies. Customers can choose to use Azure CDN from Verizon or Akamai partners. Verizon and Akamai are not covered in this SOC report.

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.

Network Watcher: 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.

Traffic Manager: Traffic Manager is a DNS-based traffic load balancer that enables customers to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Traffic

Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.

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 Azure ExpressRoute service.

VPN Gateway: VPN Gateway lets customers establish secure, cross-premises connections between their virtual network within Azure and on-premises IT infrastructure. VPN gateway sends encrypted traffic between Azure virtual networks over the Microsoft network. The connectivity offered by VPN Gateway is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

Virtual WAN: Virtual WAN is a networking service that brings many networking, security and routing functionalities together to provide a single operational interface. This service enables customers to automate large-scale branch connectivity which unifies network and policy management by optimizing routing using Microsoft global network.

Storage

Azure Archive Storage: Azure Archive Storage offers low-cost, durable, and highly available secure cloud storage optimized to store rarely accessed data that is stored for at least 180 days with flexible latency requirements (of the order of hours).

Azure Backup: Azure Backup protects Windows client data and shared files and folders on customer's corporate devices. Additionally, it protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications in the customer's datacenter(s) integrated with System Center Data Protection Manager (DPM). Azure 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.

Azure Data Box: Azure Data Box offers offline data transfer devices which are shipped between the customer's datacenter(s) and Azure, with little to no impact to the network. Azure Data Boxes use standard network-attached storage (NAS) protocols (SMB/CIFs and NFS), AES encryption to protect data, and perform a post-upload sanitization process to ensure that all data is wiped clean from the device. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

Azure Data Lake Storage Gen1: Azure Data Lake Storage (Gen1) 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.

Azure File Sync: Azure File Sync is used to centralize file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of any Azure file share.

Azure HPC Cache: Azure HPC Cache is a file cache that speeds access to data for HPC tasks by caching files in Azure. It brings the scalability of cloud computing to existing workflows while allowing large datasets to remain in existing NAS or in Azure Blob storage.

Azure Import / Export: Azure 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.

Azure Site Recovery: Azure Site Recovery contributes to a customer's BCDR strategy by orchestrating replication of their servers running on-premises or on Azure. The on-premises physical servers and virtual machine servers can be replicated to Azure or to a secondary datacenter. The virtual machine servers running in any Azure region can also be replicated to a different Azure region. When a disaster occurs in the customer's primary location, customers can coordinate failover and recovery to the secondary location using Azure Site Recovery and ensure that applications / workloads continue to run in the secondary location. Customers can failback their workloads to the primary location when it resumes operations. It supports protection and recovery of heterogeneous workloads (including System Center managed / unmanaged Hyper-V workloads, VMware workloads). With Azure 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 machines hosting tiered applications failover in the appropriate sequence.

Azure Storage: Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. 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. Listed below are the different storage types supported by Azure Storage:

- Blobs (including Data Lake Storage Gen2): Blobs is Microsoft's object storage solution for the cloud. Blobs can be used to store large amounts of binary data. For example, Blob Storage can be used for an application to store video, or to backup data. Azure Data Lake Storage Gen2 (a feature of Blobs) provides a hierarchical namespace, per object ACLs, and Hadoop Distributed File System (HDFS) APIs.

- Data Lake Storage Gen2: Data Lake Storage Gen2 is a highly scalable and cost-effective data lake solution for Big Data analytics. It combines the power of a high-performance file system with massive scale and economy to help accelerate time to insight. Data Lake Storage Gen2 extends Azure Blob Storage capabilities and is optimized for analytics workloads and compliant file system interfaces with no programming changes or data copying.

- Disks: A managed or an unmanaged disk is a Virtual Hard Disk (VHD) that is attached to a VM to store application and system data. This allows for a highly durable and available solution while still being simple and scalable.

- Files: Files offer shared storage for applications using the Server Message Block (SMB) protocol or REST protocol. Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Applications running in Azure VMs, Cloud Services or from on-premises clients can access Files using SMB or REST.

- Queues: Queues is a service for storing large number of messages. Queues provide storage and delivery of messages between one or more applications and roles.

- Tables: Tables provide fast access to large amounts of structured data that do not require complex SQL queries. For example, Tables 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 storage tier for cooler 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 and low-latency storage support for virtual machines with input / output (IO) intensive workloads. Premium Storage is designed for mission-critical production applications.

Azure Ultra Disk: Azure Ultra Disk offers high throughput, high Input / Output Operations Per Second (IOPS), and consistent low latency disk storage for Azure IaaS virtual machines. It allows the ability to dynamically change the performance of the SSD along with a customer's workloads without the need to restart VMs. Azure Ultra Disks are suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.

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. A StorSimple appliance is managed via the Azure Portal.

Databases

Azure API for FHIR: Azure API for FHIR is an API for clinical health data that enables customers to create new systems of engagement for analytics, machine learning, and actionable intelligence with health data. Azure API for FHIR improves health technologies' interoperability and makes it easier to manage data.

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

Azure Cosmos DB: Azure Cosmos DB 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).

Azure Database for MariaDB: Azure Database for MariaDB is a relational database based on the open-source MariaDB Server engine. It is a fully managed database as a service offering that can handle mission-critical workloads with predictable performance and dynamic scalability.

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

Azure Database Migration Service: Azure Database Migration Service helps customers assess and migrate their databases and solve their compatibility and migration issues. The service is designed as a seamless, end-to-end solution for moving on-premises databases to the cloud.

Azure SQL Database: Azure 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.

Azure Synapse Analytics: Azure Synapse Analytics, formerly known as SQL Data Warehouse, is a limitless analytics service that brings together enterprise data warehousing and Big Data analytics. It lets customers scale data, either on-premises or in the cloud. Azure Synapse Analytics lets customers use their existing T-SQL knowledge 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 on Virtual Machines: SQL Server on Virtual Machines enables customers to create a SQL Server in the cloud that they can control and manage. SQL Server on Virtual Machines offers a robust infrastructure for SQL Server by using Azure as a hosting environment for 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.

Developer Tools

Azure DevTest Labs: Azure DevTest Labs helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost. Azure DevTest Labs creates labs consisting of pre-configured bases or Azure Resource Manager templates allowing customers to test the latest version of their application.

Azure Lab Services: Azure Lab Services streamlines and simplifies setting up and managing resources and environments in the cloud. Azure Lab Services can quickly provision Windows and Linux virtual machines, Azure PaaS services, or complex environments in labs through reusable custom templates.

Analytics

Azure Analysis Services: Azure Analysis Services, based on the proven analytics engine in SQL Server Analysis Services, is an enterprise grade Online analytical processing (OLAP) engine and BI modeling platform, offered as a fully managed PaaS service. 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.

Azure Data Explorer: Azure Data Explorer is a fast and highly scalable, fully managed data analytics service for real-time analysis on large volumes of data streaming from applications, websites, IoT devices and more. Azure Data Explorer makes it simple to ingest this data and enables customers to quickly perform complex ad hoc queries on the data.

Azure Data Share: Azure Data Share is a simple and safe service for sharing data, in any format and any size, from multiple sources with other organizations. Customers can control what they share, who receives the data, and the terms of use via a user-friendly interface.

Azure Stream Analytics: Azure Stream Analytics is an event-processing engine that helps customers gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. Azure 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. It 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.

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.

Data Factory: Data Factory is a fully managed, serverless data integration service that refines raw data at cloud scale into actionable business insights. Customers can construct Extract, Transform, Load (ETL / ELT) processes code free in an intuitive visual environment, and easily operationalize and manage the data pipelines at scale.

Data Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator (YARN) that scales dynamically so customers can focus on their business goals and not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, customers can 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 on Azure VMs, Azure SQL Database, and Azure Synapse Analytics.

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, 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 written 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 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 clusters when deploying Big Data workloads into Azure.

Power BI Embedded: Power BI Embedded is a service which simplifies how customers use Power BI capabilities with embedded analytics. Power BI Embedded simplifies Power BI capabilities by helping customers quickly add visuals, reports, and dashboards to their apps, similar to the way apps built on Microsoft Azure use services like Machine Learning and IoT. Customers can make quick, informed decisions in context through easy-to-navigate data exploration in their apps.

AI + Machine Learning

AI Builder: AI Builder is integrated with Power Platform and Power Automate capabilities that help customers improve business performance by automating processes and predicting outcomes. AI Builder is a turnkey solution that brings the power of AI through a point-and-click experience. With AI Builder, customers can add intelligence to their applications with little to no coding or data science experience.

Azure Bot Service: Azure Bot Service helps developers build bots / intelligent agents and connect them to the communication channels their users are in. Azure Bot Service solution provides a live service (connectivity switch), along with SDK documentation, solution templates, samples, and a directory of bots created by developers.

Azure Open Datasets: Azure Open Datasets service offers customers curated public datasets that can be used to add scenario-specific features to machine learning solutions for more accurate models. Azure Open Datasets are integrated into Azure Machine Learning and readily available to Azure Databricks and Machine Learning Studio (classic). Customers can also access the datasets through APIs and use them in other products, such as Power BI and Azure Data Factory. It includes public-domain data for weather, census, holidays, public safety, and location that helps customers train machine learning models and enrich predictive solutions.

Azure Machine Learning: Azure Machine Learning (ML) is a cloud service that allows data scientists and developers to prepare data, train, and deploy machine learning models. It improves productivity and lowers costs through capabilities such as automated ML, autoscaling compute, hosted notebooks & ML Ops. It is open-source friendly and works with any Python framework, such as PyTorch, TensorFlow, or scikit-learn.

Cognitive Services: Cognitive Services is the platform on which an evolving portfolio of REST APIs and SDKs enables developers to easily add intelligent services into their solutions to leverage the power of Microsoft's natural data understanding.

Cognitive Services: Anomaly Detector: Cognitive Services: Anomaly Detector enables customers to monitor and detect abnormalities in time series data with machine learning. It utilizes an API which adapts by automatically identifying and applying the best-fitting models to data, regardless of industry, scenario, or data volume. Using time series data, the API determines boundaries for anomaly detection, expected values, and which data points are anomalies.

Cognitive Services: Computer Vision: Cognitive Services: Computer Vision provides services to accurately identify and analyze content within images and videos. It also provides customers the ability to extract rich information from images to categorize and process visual data – and protect users from unwanted content.

Cognitive Services: Content Moderator: Cognitive Services: Content Moderator is a suite of intelligent screening tools that enhance the safety of customer's platform. Image, text, and video moderation can be configured to support policy requirements by alerting customers to potential issues such as pornography, racism, profanity, violence, and more.

Cognitive Services: Custom Vision: Cognitive Services: Custom Vision is a cognitive service that can train and deploy image classifiers and object detectors. The custom models trained by the AI service infer the contents of images based on visual characteristics.

Cognitive Services: Face: Cognitive Services: Face is a service that has two main functions - face detection with attributes and face recognition. It provides customers the ability to detect human faces and compare similar ones, organize people into groups according to visual similarity, and identify previously tagged people in images.

Cognitive Services: Form Recognizer: Cognitive Services: Form Recognizer is a cognitive service that uses machine learning technology to identify and extract text, key / value pairs and table data from form documents. It ingests text from forms and outputs structured data that includes the relationships in the original file. Customers receive accurate results that are tailored to specific content without heavy manual intervention or extensive data science expertise. Form Recognizer is comprised of custom models, the prebuilt receipt model, and the layout API. Customers can call Form Recognizer models by using a REST API to reduce complexity and integrate it into a workflow or an application.

Cognitive Services: Language Understanding: Cognitive Services: Language Understanding is a cloud-based API service that enables developers to build their custom language models (i.e., intent classifier and entity extractor). It enables its customers to integrate those custom machine-learning models into any conversational application, or unstructured text to predict, and pull out relevant, detailed information presented in a structured format i.e., JSON.

Cognitive Services: Translator: Cognitive Services: Translator is a cloud-based machine translation service, translating natural language text between more than 60 languages, via a REST-based web service API. Besides translation, the API provides functions for dictionary lookup, language detection and sentence breaking.

Cognitive Services: Personalizer: Cognitive Services: Personalizer offers customers automatic model optimization based on reinforcement learning through a cloud-based API service that helps client applications choose the best, single content item to show each user. Personalizer collects and uses real-time information customers provide about content and context in order to select the most relevant content. Personalizer uses system monitoring of customer and user behavior to report a reward score in order to improve its ability to select the best content based on the context information it receives. Content collected consists of any unit of information such as text, images, URLs, emails, and more.

Cognitive Services: QnA Maker: Cognitive Services: QnA Maker is a cognitive service offering deployed on Azure. The endpoint is used by third party developers to create knowledge base endpoints. It allows users to distill information into an easy-to-navigate FAQ.

Cognitive Services: Speech Services: Cognitive Services: Speech Services is an Azure service that offers speech to text, text to speech and speech translation using base (out of the box) and custom models.

Cognitive Services: Text Analytics: Cognitive Services: Text Analytics is a cloud-based service that provides advanced natural language processing over raw text, and includes five main functions: sentiment analysis, key phrase extraction, named entities recognition, linked entities, and language detection.

Cognitive Services: Video Indexer: Cognitive Services: Video Indexer is a cloud application built as a cognitive video indexing platform that processes the videos that users upload and creates a cognitive index of the content within the video. It enables customers to extract the insights from videos using Video Indexer models.

Machine Learning Studio (Classic): Machine Learning Studio (Classic) 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.

Microsoft Genomics: Microsoft Genomics offers a cloud implementation of the Burrows-Wheeler Aligner (BWA) and the Genome Analysis Toolkit (GATK) for secondary analysis which are then used for genome alignment and variant calling.

Microsoft Healthcare Bot: Microsoft Healthcare Bot is an intelligent, highly personalized virtual health assistant that aims to improve the conversation between healthcare providers, payers and patients, via conversational navigation. It allows healthcare providers and payers to empower their users to get information related to their health, such as checking their symptoms, asking about their health plans, and receiving personalized, meaningful, credible answers, in an easy, self-serve and conversational way.

Internet of Things

Azure IoT Central: Azure IoT Central is a managed IoT SaaS solution that makes it easy to connect, monitor, and manage IoT assets at scale.

Azure IoT Hub: Azure IoT Hub is used to connect, monitor, and control billions of IoT assets running on a broad set of operating systems and protocols. Azure IoT Hub establishes reliable, bi-directional communication with assets, even if they’re intermittently connected, and analyzes and acts 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. Customers can also revoke access rights to specific devices to maintain the integrity of their system.

Event Grid: Event Grid is a high scale Pub / Sub service which enables event-driven programming. It integrates with webhooks for delivering events.

Event Hubs: Event Hubs is a Big Data streaming platform and event ingestion service capable of receiving and processing millions of events per second. Event Hubs can process, and store events, data, or telemetry produced by distributed software and devices. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching / storage adapters. Event Hubs for Apache Kafka enables native Kafka clients, tools, and applications such as Mirror Maker, Apache Flink, and Akka Streams to work seamlessly with Event Hubs with only configuration changes. Event Hubs uses Advanced Message Queuing Protocol (AMQP), HTTP, and Kafka as its primary protocols.

Notification Hubs: Notification Hubs is a massively scalable mobile push notification engine for sending notifications to Android, iOS, and Windows devices. It aggregates sending notifications through the Apple Push Notification service (APNs), Firebase Cloud Messaging (FCM) service, 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.

Time Series Insights: Time Series Insights is used to collect, process, store, analyze, and query highly contextualized, time-series-optimized IoT-scale data. Time Series Insights is ideal for ad hoc data exploration and operational analysis. It is a uniquely extensible and customized service offering that meets the broad needs of industrial IoT deployments.

Windows 10 IoT Core Services: Windows 10 IoT Core Services is a cloud subscription-based service that provides essential aids needed to commercialize a device on Windows 10 IoT Core. Through this subscription, OEMs have access to support channel, along with services to publish device updates and assess device health. Windows 10 IoT Core services offers monthly security and reliability updates, keeping devices stable and secure and utilizes Device Update Center to control device updates using the same content distribution network that is used by millions of customers to manage Windows updates.

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.

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 SaaS and cloud-based connectors that includes Salesforce, Office 365, Twitter, Dropbox, Google services, and more.

Service Bus: Service Bus is a multi-tenant cloud messaging service that can be used to send information between applications and services. The asynchronous operations enable flexible, brokered messaging, along with structured first-in, first-out (FIFO) messaging, and publish / subscribe capabilities. Service Bus uses Advanced Message Queuing Protocol (AMQP), Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols.

Identity

Azure Active Directory (AAD): 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. AAD comes in 3 editions: Free, Basic, and Premium. Self-service credentials management is a feature of AAD that allows Azure AD tenant administrators to register for and subsequently reset their passwords without needing to contact Microsoft support. Microsoft Online Directory Services (MSODS) is also a feature of AAD that provides the backend to support authentication and provisioning for AAD.

Azure Active Directory B2C: Azure Active Directory B2C extends Azure Active Directory 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 accessed from any device.

Azure Active Directory Domain Services: Azure Active Directory 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 Active Directory Domain Services integrates with the existing Azure Active Directory 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.

Management and Governance

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, and then provides recommendations that can reduce costs and improve the performance, security, and reliability of applications.

Azure Blueprints: Azure Blueprints provides governed subscriptions to enterprise customers, simplifying largescale Azure deployments by packaging key environment artifacts, role-based access controls, and policies in a single blueprint definition.

Azure Lighthouse: Azure Lighthouse offers service providers a single control plane to view and manage Azure across all their customers with higher automation, scale, and enhanced governance. With Azure Lighthouse, service providers can deliver managed services using comprehensive and robust management tooling built into the Azure platform. This offering can also benefit enterprise IT organizations by managing resources across multiple tenants.

Azure Managed Applications: Azure Managed Applications enables customers to offer cloud solutions that are easy for consumers to deploy and operate. It can help customers implement the infrastructure and provide ongoing support. A managed application can be made available to all customers or only to users in the customer's organization by publishing it in the Azure marketplace or to an internal catalog, respectively.

Azure Migrate: Azure Migrate enables customers to migrate to Azure, also serving as a single point to track migrations to Azure. Customers can choose from Microsoft first-party and Independent Software Vendor (ISV) partner solutions for their assessment and migration activities. Customers can plan and carry out migration of their servers using the Server Assessment and Server Migration tools; these are Microsoft solutions available on Azure Migrate. Server Assessment helps to discover on-premise applications and servers (Hyper-V and VMware VMs), and provides a migration assessment: a mapping from discovered servers to recommended Azure VMs, migration readiness analysis and cost estimates to run the VMs in Azure. It allows for dependency visualization to view dependencies of a single VM or a group of VMs. Server Migration allows customers to migrate the on-premises servers (non-virtualized physical or virtualized using Hyper-V and VMware) to Azure. Microsoft solutions to assess and migrate database workloads - Database Assessment and Database Migration - are also discoverable on Azure Migrate. In addition to these tools, ISV partner tools for assessment and migration are also discoverable on Azure Migrate. The machines discovered using these tools and the assessment and migration activities conducted using these tools can be tracked on Azure Migrate; this helps customers to track all their migration activities at one place.

Azure Monitor: Azure Monitor provides full observability into a customer's applications, infrastructure and networks and collects, analyzes and acts on telemetry data from Azure and on-premises environments. It helps customers maximize performance and availability of applications and proactively identifies problems in real time. It includes, but is not limited to, the following four services: Azure Monitor Essentials, Application Insights, Application Insights Profiler, and Log Analytics.

- Azure Monitor Essentials: Azure Monitor Essentials 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.

- Application Insights: Application Insights is used to monitor any connected App; It is on by default to be able to monitor multiple types of Azure resources, particularly Web Applications. It includes analytics tools to help diagnose issues and understand what users do with the App. It can monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center.

- Application Insights Profiler: Application Insights Profiler is used to help understand and troubleshoot performance issues in production. It helps teams collect performance data in a low-impact way to minimize overhead to the system.

- Log Analytics: Log Analytics enables customers to collect, correlate and visualize all their machine data, such as event logs, network logs, performance data, and 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, separate signals from noise, with powerful log-management capabilities.

Azure Policy: Azure Policy provides real-time enforcement and compliance assessment on Azure resources to apply standards and guardrails.

Azure Resource Graph: Azure Resource Graph is a service designed to extend Azure Resource Management by providing efficient and performant resource exploration with the ability to query at scale across a given set of subscriptions so that customers can effectively govern their environment. Azure Resource Graph offers the ability to query resources with complex filtering, grouping and sorting by resource properties and the ability to iteratively explore resources based on governance requirements. Resource Graph also offers the ability to assess the impact of applying policies in a vast cloud environment.

Azure Resource Manager: Azure Resource Manager (ARM) 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 for use across 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, 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, they 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, they 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.

Cloud Shell: Cloud Shell provides a web-based command line experience from Ibiza portal, Azure mobile, docs.microsoft.com, shell.azure.com, and Visual Studio Code. Both Bash and PowerShell experiences are available for customers to choose from.

Microsoft Azure Portal: Microsoft Azure Portal provides a framework SDK, telemetry pipeline and infrastructure for Microsoft Azure services to be hosted inside the Azure Portal shell, and manages and monitors the required components to allow Azure services to run 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. Microsoft Azure portal simplifies the development work for Azure service owners and developers by providing a comprehensive SDK with tools and controls for easily building and packaging the service applications. Customers manage these Azure applications through the Microsoft 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 an Azure Storage queue, Service Bus queue, or Service Bus topic on any schedule. It 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. Scheduler was retired in calendar year Q4 2019 with all of the service functionality moved to Logic Apps. However, this service continues to support existing customers until it is fully decommissioned.

Security

Azure Advanced Threat Protection: Azure Advanced Threat Protection (ATP) is a cloud-based security solution that leverages on-premises Active Directory (AD) signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at the organization.

Azure Dedicated HSM: Azure Dedicated HSM provides cryptographic key storage in Azure where the customer has full administrative control over the HSM. It offers a solution for customers who require the most stringent security requirements.

Azure Security Center: Azure 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.

Azure Sentinel: Azure Sentinel is a cloud-native Security Information and Event Management (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise. Azure Sentinel aggregates data from all sources, including users, applications, servers, and devices running on-premises or in any cloud, letting customers reason over millions of records in a few seconds. It includes built-in connectors for easy onboarding of security solutions.

Customer Lockbox for Microsoft Azure: Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject customer data access requests. It is used in cases where a Microsoft engineer needs to access customer data during a support request.

Key Vault: Key Vault safeguards keys and other secrets in the cloud by using Hardware Security Modules (HSMs). It 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: Multi-Factor Authentication (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.

Media

Azure Media Services: Azure 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.

Web

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

Azure SignalR Service: Azure SignalR service is a managed service to help customers easily build real-time applications with SignalR technology. This real-time functionality allows the service to push content updates to connected clients, such as a single page web or a mobile application. As a result, clients are updated without the need to poll the server or submit new HTTP requests for updates.

Internal Supporting Services

Internal Supporting Services is a collection of 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.

Asimov Event Forwarder: Asimov Event Forwarder reads full event stream from OneDS Collector and breaks it apart into separate event streams based upon a set of subscription matching criteria. These event streams are then forwarded to the downstream services which subscribe to that stream.

Azure Networking: Azure Networking is used to provide all datacenter connectivity for Azure. Azure Networking is completely transparent to Azure customers who cannot interact directly with any physical network device. The Azure Networking service provides APIs to manage network devices in Azure datacenters. It 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 Azure Networking is used to perform certain operations, e.g., enable / disable a port for an unresponsive blade. It 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.

Azure Privileged Identity Management: Azure 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 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 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.

Azure RBAC Ibiza UX (Hosted extension): Azure RBAC Ibiza UX (Hosted extension) covers the Access Control (IAM) experience for Azure resources in the Ibiza portal. It supports operations like listing, granting, and revoking access to Azure resources, managing Azure RBAC custom roles, checking what access a principal has on an Azure resource, and more.

Azure Security Monitoring (ASM SLAM): ASM SLAM contains the features and services related to Security Monitoring in Azure. This includes Azure Security Pack which is deployed by services to configure their security monitoring.

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

Azure Stack Bridge: Azure Stack Bridge is an integration service which provides hybrid capabilities between on-premise Azure Stack deployments and the online Azure cloud.

Azure Stack Edge Service[15]: Azure Stack Edge Service, formerly known as Data Box Edge Service, manages appliances on customer premises that ingest data to customer storage account over network.

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

CEDIS - Active Directory Domain Services: CEDIS - Active Directory Domain Services provides Active Directory Domain Services (AD DS) for internal Microsoft customers like Azure, Online Services, and Microsoft Retail in the Public and Government cloud environments.

CEDIS - Active Directory Federation Services: CEDIS - ADFS manages an instance of ADFS for internal users of Microsoft in Public Azure and the National clouds.

CEDIS - Azure Active Directory: CEDIS - AAD manages an instance of AAD Connect for internal users of Microsoft in Public Azure and the National clouds. The services are limited to authorized access to low levels of the cloud environment only.

Cloud Data Ingestion: Cloud Data Ingestion (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.

Cognitive Services: Container Platform: Cognitive Services: Container Platform is the backend platform that hosts multiple Cognitive Services offerings.

Compute Manager: Compute Manager is an Azure core service responsible for the allocation of Azure tenants and their associated containers (VMs) to the hardware resources in the datacenter, and for the management of

[15] Examination period for this service was from July 1, 2019 to March 31, 2020.

their lifecycle. Subcomponents include the Service Manager (SM / Aztec), Tenant Manager (TM), Container Manager (CM) and Allocator.

Dynamics 365 Integrator App: Dynamics 365 Integrator App is responsible for the sync of data between all Dynamics 365 platforms.

DataGrid: DataGrid system is comprised of a metadata repository system to store data contract for all Common Schema events and data ingested from SQL, Azure SQL, Azure Tables, Azure Queues, CSV and TSV files.

DesktopAnalytics: DesktopAnalytics provides enterprise customers with device telemetry data to obtain and maintain accurate customer details across Office and Windows.

Datacenter Service Configuration Manager (dSCM): dSCM enables service teams to onboard to Azure Security internal services by providing specific configuration settings. The goal of dSCM is to reduce the onboarding and configuration management time for services onboarding to Azure Security services.

Datacenter Secrets Management Service (dSMS): dSMS is an Azure service that handles, stores, and manages the lifecycle for Azure Foundational Services.

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.

Enterprise Data Platform[15]: Enterprise Data Platform is a data pipeline service that collects, analyzes and shares back value add telemetry to Microsoft Enterprise customers.

Enterprise Knowledge Graph[16]: Enterprise Knowledge Graph enables customers to build scalable knowledge solutions based on a flexible ontology and advanced conflation capability. This service was decommissioned in calendar year Q4 2019.

Falcon: Falcon is a pseudo-serverless ecosystem that enables teams across Microsoft to build highly scalable microservices powering various features that span across Bing, Skype and Office.

Geneva Actions: Geneva Actions is an extensible platform enabling compliant management of production services and resources running on the Azure Cloud. It allows users to plug in their own live site operations to the Geneva Actions authorization and auditing system to ensure safe and secure control of the Azure platform.

Geneva Warm Path: Geneva Warm Path is a monitoring / diagnostic service used by teams across Microsoft to monitor the health of their service deployments.

Hybrid Identity Service: 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.

IAM - Management Admin UX: IAM - Management Admin 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.

[16] Examination period for this service was from July 1, 2019 to September 30, 2019.

MEE Privacy Service: MEE Privacy Service, also known as Next Generation Privacy Common Infrastructure, is a set of services that provides Data Subject Rights (DSR) distribution and auditing for internal Microsoft GDPR compliance. The service acts as the entry point for all view, export, delete and account close DSR signals that are then fanned out to various agents throughout the company to process in their data sets. Each of those agents then send back completion / acknowledgement signals that are subsequently used to produce several audit reports used to report Microsoft's GDPR compliance to executive management.

OneDS Collector: OneDS Collector is the ingestion front end for the telemetry pipelines used by Microsoft Windows, Microsoft Office and other Microsoft products. Microsoft products are instrumented with telemetry clients for logging and sending telemetry in the form of events. OneDS Collector validates and scrubs the events, then forwards them to the Asimov Event Forwarder service.

Pilotfish: Pilotfish 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.

Protection Center: Protection Center is a cloud security service that uses state of the art machine learning to analyze 10 terabytes of behavioral and contextual data every day to detect and prevent attempts to attack organizations' Azure AD accounts.

TuringAtAzure: TuringAtAzure is an API service that allows Microsoft product teams to access Turing language models in their production scenario.

WANetMon: WaNetMon monitors the health and availability of the Azure network and its services across all regions and all cloud environments. The platform provides monitoring, alerting and diagnostics capabilities for the Azure networking DRIs to quickly detect and diagnose issues. WaNetMon is also responsible for democratization of all network telemetry data, getting the data to a common data store and making it accessible for everyone.

Windows Azure Jumpbox: Windows Azure 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.

Workflow: Workflow lets users upload their workflows to Azure and have them executed in a highly scalable manner. This service is currently consumed only by O365 SharePoint Online service.

Microsoft Online Services

Intune: 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 Cloud App Security (MCAS): Microsoft Cloud App Security 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 Defender Advanced Threat Protection: Microsoft Defender Advanced Threat Protection is a complete endpoint security solution for preventative protection, post-breach detection, automated investigation, and response.

Microsoft Graph: Microsoft Graph exposes multiple APIs from Office 365 and other Microsoft cloud services through a single endpoint. Microsoft Graph 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 Managed Desktop (MMD): Microsoft Managed Desktop (MMD) combines Microsoft 365 Enterprise with an IT-as-a-Service (ITaaS) backed by Microsoft, for providing the best user experience, the latest technology as well as Desktop security and IT services, with an end-to-end cloud-based solution that is managed, supported, and monitored by Microsoft.

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 is 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.

Microsoft Threat Experts: Microsoft Threat Experts is a managed threat hunting service that provides Security Operation Centers (SOCs) with expert level monitoring and analysis to help them ensure that critical threats in their unique environments do not get missed.

Microsoft Threat Protection: Microsoft Threat Protection (MTP) is an integrated experience with AI and automation built in, that is built on best-in-class Microsoft 365 threat protection services and pools their collective knowledge and capabilities to accrue to something even better. It leverages and integrates these services' industry-leading prevention, detection, investigation, and response techniques to help secure attack vectors across users, endpoints, cloud apps, and data.

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. Services under PowerApps include, but are not limited to, the following:

- **PowerApps Authoring Service:** PowerApps Authoring Service 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 MakerX Portal**: PowerApps MakerX 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 Service RP for most operations and provides entry points for users to launch into other PowerApps services as necessary.
- **PowerApps Service RP:** PowerApps Service 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 ARM resource provider, meaning that incoming requests are authenticated by the ARM on the front end and proxied through to the RP.

Power Automate: Power Automate helps customers set up automated workflows between their favorite apps and services to synchronize files, get notifications, collect data, and more.

Power BI: Power BI is 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. Customers can access their data and reports from anywhere with the Power BI Mobile apps, which update automatically with any changes to customers data.

Power Virtual Agents: Power Virtual Agents is an offering that enables anyone to create powerful chatbots using a guided, no-code graphical interface, without the need for data scientists or developers. It eliminates the gap between subject matter experts and the development teams building the chatbots, and the long latency between subject matter experts recognizing an issue and updating a chatbot to address it. It removes the complexity of exposing teams to the nuances of conversational AI and the need to write complex code. It also minimizes the IT effort required to deploy and maintain a custom conversational solution by empowering subject matter experts and departments to build and maintain their own conversational solutions.

Microsoft Dynamics 365

Dynamics 365 AI Customer Insights: Dynamics 365 AI Customer Insights is a cloud-based SaaS service that enables organizations of all sizes to bring together data from multiple sources and generate knowledge and insights to build a holistic 360 degree view of their customers.

Dynamics 365 Business Central: Dynamics 365 Business Central, formerly known as Dynamics NAV, is Microsoft’s Small and Medium Business (SMB) service built on and for the Azure cloud. It provides organizations with a service that supports their unique requirements and rapidly adjusts to constantly changing business environments, without the additional overhead of managing infrastructure.

Dynamics 365 Commerce, Dynamics 365 Finance, and Dynamics 365 Supply Chain Management: These offerings are supported by the same set of underlying services. These offerings provide customers with a complete set of adaptable ERP functionality that includes financials, demand planning, procurement / supply chain, manufacturing, distribution, services industries, public sector and retail capabilities that are combined with BI, infrastructure, compute and database services.

Dynamics 365 Customer Engagement: Dynamics 365 Customer Engagement is a cloud-based customer relationship management (CRM) business solution that can help customers drive sales productivity and improve the value of marketing efforts through social insights, business intelligence, and campaign management. It includes a variety of applications such as Dynamics 365 for Sales, Dynamics 365 for Customer Service, Dynamics 365 for Project Service Automation, and Dynamics 365 for Field Service.

Dynamics 365 Customer Service: Dynamics 365 Customer Service provides tools / apps that help build great customer relationships by focusing on optimum customer satisfaction. It provides many features and tools that organizations can use to manage the services they provide to customers.

Dynamics 365 Field Service: Dynamics 365 Field Service business application helps organizations deliver onsite service to customer locations. It combines workflow automation, algorithm scheduling, and mobility to help mobile workers fix issues when they are onsite at the customer location.

Dynamics 365 Fraud Protection: Dynamics 365 Fraud Protection provides customers with a payment fraud solution helping e-commerce merchants drive down fraud loss, increase bank acceptance rates to yield higher revenue, and improve the online shopping experience for its customers.

Dynamics 365 Human Resources: Dynamics 365 Human Resources provides a Microsoft-hosted HR solution that delivers core HR functionality to HR professionals, managers and employees across the organization.

Dynamics 365 Marketing: Dynamics 365 Marketing is a marketing-automation application that helps customers turn prospects into business relationships. Dynamics 365 Marketing has built-in intelligence to allow customers create emails and online content to support marketing initiatives, organize and publicize events, and share information.

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

Dynamics 365 Project Service Automation: Dynamics 365 Project Service Automation (PSA) application helps organizations efficiently track, manage, and deliver project-based services, from the initial sale all the way to invoicing.

Dynamics 365 Sales: Dynamics 365 Sales enables sales professionals to build strong relationships with their customers, take actions based on insights, and close sales faster. It can be used to keep track of customer accounts and contacts, nurture sales from lead to order, and create sales collateral.

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). The customer provided data are broadly classified into the following data types:

1. **Access Control Data** is data used to manage access to administrative roles or sensitive functions.
2. **Customer Content** is the data, information and code that Microsoft internal employees, and non-Microsoft personnel (if present) provide to, transfer in, store in or process in a Microsoft Online Service or product.
3. **End User Identifiable Information (EUII)** is data that directly identifies or could be used to identify the authenticated user of a Microsoft service. EUII does not extend to other personal information found in Customer Content.
4. **Support Data** is data provided to Microsoft and generated by Microsoft as part of support activities.
5. **Account Data** is information about payment instruments. This type of data is not stored in the Azure platform.
6. **Public Personal Data** is publicly available personal information that Microsoft obtains from external sources.
7. **End User Pseudonymous Identifiers (EUPI)** are identifiers created by Microsoft, tied to the user of a Microsoft service.
8. **Organization Identifiable Information (OII)** is data that can be used to identify a particular tenant / Azure subscription / deployment / organization (generally configuration or usage data) and is not linkable to a user.
9. **System Metadata** is data generated in the course of running the service, not linkable to a user or tenant. It does not contain Access Control Data, Customer Content, EUII, Support Data, Account Data, Public Personal Data, EUPI, or OII.
10. **Public Non-Personal Data** is publicly available information that Microsoft obtains from external sources. It does not contain Public Personal Data.

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."

Section IV: Principal Service Commitments and System Requirements

Section IV: Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers and has established system requirements as part of the Azure service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Microsoft is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Microsoft's service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in the Microsoft Online Subscription Agreement, Microsoft Enterprise Enrollment Agreement (Volume Licensing - Online Services Terms), Microsoft Azure Privacy Statement, and Microsoft Trust Center, as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: Microsoft has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.

- Availability: Microsoft has made commitments related to percentage uptime and connectivity for Azure as well as commitments related to service credits for instances of downtime.

- Processing Integrity: Microsoft has made commitments related to processing customer actions completely, accurately and timely. These customer actions include, for example, specifying geographic regions for the storage and processing of customer data.

- Confidentiality: Microsoft has made commitments related to maintaining the confidentiality of customers' data through data classification policies, data encryption and other relevant security controls.

Microsoft has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Azure's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various Azure services and offerings.