Microsoft Corporation - Azure Including Dynamics 365

(Azure & Azure Government)

SOC 3 Report

October 1, 2023 to September 30, 2024

Table of contents

Section 1: Independent Service Auditor's Report

Deloitte & Touche LLP
1015 Second Avenue
Suite 500
Seattle, WA 98104
USA

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

Section 1: Independent Service Auditor's Report

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Scope

We have examined the management of Microsoft Corporation's (the "Service Organization" or "Microsoft") accompanying assertion titled "Management of Microsoft's Assertion" (the "assertion") that the controls within Microsoft's Azure[1] system ("system") were effective throughout the period October 1, 2023 to September 30, 2024[2], 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")[3] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.

Service Organization's Responsibilities

Management of 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. Management of Microsoft has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, management of 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 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 (AICPA) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board (IAASB). Those standards require that we

---

[1] Azure comprises of in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters in the Azure and Azure Government cloud environments.

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

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

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.

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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants. We have complied with those requirements. We applied the Statements on Quality Control Standards established by the AICPA and the International Standards on Quality Management issued by the IAASB and, accordingly, maintain a comprehensive system of quality control.

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.

Emphasis of a Matter - Cyber Incident

Microsoft has publicly acknowledged cyberattacks by a state-sponsored entity known as Midnight Blizzard. According to Microsoft, threat actors initially gained access to a Microsoft non-production corporate tenant. Passwords and other secrets were exfiltrated, allowing access to certain source code repositories, additional secrets, databases, and applications.

As of October 15, 2024, Microsoft acknowledged that certain passwords, secrets, and code repositories relevant to this report were accessed or exfiltrated. Microsoft represented that passwords and secrets were rotated or remediated upon identification. Microsoft also stated that code repository access by the threat actor did not include production change capability. We inspected certain listings provided by Microsoft of applications, resources, and code repositories impacted by these incidents, including those aligned to passwords and secrets that were accessed. We did not identify evidence that contradicts Microsoft's explanations and representations. Microsoft has determined that the incident was closed on 10/15/2024.

Opinion

In our opinion, management's assertion that the controls within the Microsoft's Azure system were effective throughout the period October 1, 2023 to September 30, 2024, 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

November 8, 2024

Section 2:
Management of Microsoft's Assertion

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

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

Microsoft

Section 2: Management of Microsoft's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Microsoft Corporation's (the "Service Organization's" or "Microsoft's") Azure[4] system throughout the period October 1, 2023 to September 30, 2024[5], 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")[6] set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in section 3 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 October 1, 2023 to September 30, 2024, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable 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 4.

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 October 1, 2023 to September 30, 2024, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria.

.

[4] Azure comprises of in-scope services and offerings for Microsoft Azure, Microsoft Dynamics 365, and Microsoft datacenters in the Azure and Azure Government cloud environments.

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

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

Section 3: Management of Microsoft's Description of its Azure System

Section 3: Management of Microsoft's Description of its 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 and 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 and Boundary

Azure is global multi-tenant cloud platform that provides a public cloud deployment model. Azure Government is a US Government Community Cloud 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[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
Microsoft Datacenters					
Microsoft Datacenter and Operations Service		✓	✓	✓	✓
Azure					
Compute	Azure App Service	✓	✓	✓	✓
	Azure Arc	✓	✓	✓	✓
	Azure Cloud Services[8]	✓	✓	✓	✓
	Azure Cloud Services (Extended Support)	✓	✓	✓	✓
	Azure Functions	✓	✓	✓	✓
	Azure Large Instances	✓	-	✓	✓
	Azure Machine Configuration	✓	✓	✓	✓
	Azure Service Fabric	✓	✓	✓	✓
	Azure Virtual Desktop	✓	✓	✓	✓
	Azure Virtual Machines	✓	✓	✓	✓
	Azure Virtual Machine Scale Sets	✓	✓	✓	✓
	Azure VM Image Builder	✓	-	✓	✓
	Azure VMware Solution	✓	✓	✓	✓
	Batch	✓	✓	✓	✓
	Planned Maintenance	✓	✓	✓	✓
Containers	Azure Arc Enabled Kubernetes	✓	✓	✓	✓
	Azure Container Apps	✓	-	✓	✓
	Azure Container	✓	✓	✓	✓

[7] Examination period scope H2 FY24 extends from October 1, 2023 to March 31, 2024.
Examination period scope H1 FY25 extends from April 1, 2024 to September 30, 2024.

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

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Instances				
	Azure Container Registry	✓	✓	✓	✓
	Azure Kubernetes Configuration Management	✓	✓	✓	✓
	Azure Kubernetes Service (AKS)	✓	✓	✓	✓
	Azure Red Hat OpenShift	✓	✓	✓	✓
	Microsoft Artifact Registry	✓	-	✓	✓
Networking	Application Gateway	✓	✓	✓	✓
	Azure Bastion	✓	✓	✓	✓
	Azure Communications Gateway	✓	-	✓	✓
	Azure Content Delivery Network	✓	✓	✓	✓
	Azure DDoS Protection	✓	✓	✓	✓
	Azure DNS	✓	✓	✓	✓
	Azure ExpressRoute	✓	✓	✓	✓
	Azure Firewall	✓	✓	✓	✓
	Azure Firewall Manager	✓	✓	✓	✓
	Azure Front Door	✓	✓	✓	✓
	Azure Internet Analyzer	✓	-	✓	-
	Azure Load Balancer	✓	✓	✓	✓
	Azure NAT Gateway	✓	✓	✓	✓
	Azure Orbital Ground Station	✓	-	✓	✓
	Azure Peering Service	✓	✓	✓	✓
	Azure Private Link	✓	✓	✓	✓
	Azure Private MEC	✓	-	✓	✓
	Azure Route Server	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Azure Traffic Collector	✓	-	-	✓
	Azure Virtual Network	✓	✓	✓	✓
	Azure Virtual Network IP Services	✓	✓	✓	✓
	Azure Virtual Network Manager	✓	-	✓	✓
	Azure Web Application Firewall	✓	✓	✓	✓
	Network Watcher	✓	✓	✓	✓
	Traffic Manager	✓	✓	✓	✓
	Virtual WAN	✓	✓	✓	✓
	VPN Gateway	✓	✓	✓	✓
Storage	Azure Archive Storage	✓	✓	✓	✓
	Azure Backup	✓	✓	✓	✓
	Azure Data Box	✓	✓	✓	✓
	Azure Data Lake Storage Gen1	✓	-	✓	-
	Azure File Sync	✓	✓	✓	✓
	Azure HPC Cache	✓	✓	✓	✓
	Azure Managed Lustre	✓	✓	✓	✓
	Azure NetApp Files	✓	✓	✓	✓
	Azure Site Recovery	✓	✓	✓	✓
	Azure Storage (Blobs (including Azure Data Lake Storage Gen2), Disks, Files, Queues, Tables, Azure Disk Storage) including Cool and Premium	✓	✓	✓	✓
	Azure Storage Mover	✓	-	-	✓
Databases	Azure Cache for Redis	✓	✓	✓	✓
	Azure Cosmos DB	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Azure Database for MariaDB	✓	✓	✓	✓
	Azure Database for MySQL	✓	✓	✓	✓
	Azure Database for PostgreSQL	✓	✓	✓	✓
	Azure Database Migration Service	✓	✓	✓	✓
	Azure Health Data Services	✓	✓	✓	✓
	Azure SQL	✓	✓	✓	✓
	Azure SQL Managed Instance	✓	✓	✓	✓
	Azure Synapse Analytics	✓	✓	✓	✓
	Microsoft Azure Managed Instance for Apache Cassandra	✓	-	✓	✓
	SQL Managed Instance enabled by Azure Arc	✓	-	✓	✓
	SQL Server enabled by Azure Arc	✓	-	✓	✓
	SQL Server on Azure Virtual Machines	✓	✓	✓	✓
	SQL Server Stretch Database	✓	✓	✓	✓
Developer Tools	Azure App Configuration	✓	✓	✓	✓
	Azure Deployment Environments	✓	-	✓	✓
	Azure DevTest Labs	✓	✓	✓	✓
	Azure for Education	✓	-	✓	✓
	Azure Lab Services	✓	-	✓	✓
	Azure Load Testing	✓	-	✓	✓
	Azure Managed Grafana	✓	-	✓	✓
	GitHub AE	✓	✓	✓	-
	Microsoft Dev Box	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Service Connector	✓	-	✓	✓
Analytics	Azure Analysis Services	✓	✓	✓	✓
	Azure Chaos Studio	✓	-	✓	✓
	Azure Data Explorer	✓	✓	✓	✓
	Azure Data Factory	✓	✓	✓	✓
	Azure Data Share	✓	✓	✓	✓
	Azure HDInsight	✓	✓	✓	✓
	Azure Operator Insights	✓	-	✓	✓
	Azure Stream Analytics	✓	✓	✓	✓
	Data Catalog	✓	-	✓	✓
	Data Lake Analytics	✓	-	✓	✓
	Microsoft Fabric	✓	-	✓	✓
	Power BI Embedded	✓	✓	✓	✓
AI + Machine Learning	AI Builder	✓	✓	✓	✓
	Azure AI Services	✓	✓	✓	✓
	Azure AI Services: AI Anomaly Detector	✓	-	✓	✓
	Azure AI Services: Azure AI Containers	✓	✓	✓	✓
	Azure AI Services: Azure AI Content Safety	✓	✓	✓	✓
	Azure AI Services: Azure AI Custom Vision	✓	✓	✓	✓
	Azure AI Services: Azure AI Document Intelligence	✓	✓	✓	✓
	Azure AI Services: Azure AI Face Service	✓	✓	✓	✓
	Azure AI Services: Azure AI Immersive Reader	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Azure AI Services: Azure AI Language	✓	-	✓	✓
	Azure AI Services: Azure AI Metrics Advisor	✓	-	✓	✓
	Azure AI Services: Azure AI Personalizer	✓	✓	✓	✓
	Azure AI Services: Azure AI Search	✓	✓	✓	✓
	Azure AI Services: Azure AI Speech	✓	✓	✓	✓
	Azure AI Services: Azure AI Translator	✓	✓	✓	✓
	Azure AI Services: Azure AI Video Indexer	✓	✓	✓	✓
	Azure AI Services: Azure AI Vision	✓	✓	✓	✓
	Azure AI Services: Conversational Language Understanding	✓	✓	✓	✓
	Azure AI Services: Question Answering	✓	✓	✓	✓
	Azure AI Bot Service	✓	✓	✓	✓
	Azure Health Bot	✓	-	✓	✓
	Azure Open Datasets	✓	✓	✓	✓
	Azure OpenAI Service[9]	✓	✓	✓	✓
	Azure Machine Learning	✓	✓	✓	✓
	Machine Learning Studio (Classic)	✓	-	✓	✓
	Microsoft 365 Copilot for Sales	✓	-	✓	✓
	Microsoft Genomics	✓	-	✓	✓

[9] Examination period for this offering / service for Azure was from October 1, 2023 to September 30, 2024, while the examination period for Azure Government was from April 1, 2024 to September 30, 2024.

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Seeing AI	✓	-	✓	✓
Internet of Things	Azure Digital Twins	✓	-	✓	✓
	Azure Event Grid	✓	✓	✓	✓
	Azure IoT Central	✓	-	✓	✓
	Azure IoT Hub	✓	✓	✓	✓
	Azure Sphere	✓	-	✓	✓
	Azure Time Series Insights	✓	-	✓	✓
	Device Update for IoT Hub	✓	-	-	✓
	Event Hubs	✓	✓	✓	✓
	Microsoft Cloud for Sustainability	✓	-	✓	✓
	Microsoft Defender for IoT	✓	✓	✓	✓
	Notification Hubs	✓	✓	✓	✓
Integration	API Management	✓	✓	✓	✓
	Azure Data Manager for Energy	✓	-	-	✓
	Azure Logic Apps	✓	✓	✓	✓
	Azure Service Bus	✓	✓	✓	✓
	Universal Print	✓	✓	✓	✓
Identity	Azure Active Directory B2C	✓	-	✓	✓
	Microsoft Entra Domain Services	✓	✓	✓	✓
	Microsoft Entra ID	✓	✓	✓	✓
	Microsoft Entra Permissions Management	✓	-	-	✓
	Microsoft Global Secure Access	✓	-	-	✓
	Microsoft Purview Information Protection	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
Management and Governance	Application Change Analysis	✓	-	✓	✓
	Automation	✓	✓	✓	✓
	Azure Advisor	✓	✓	✓	✓
	Azure Blueprints	✓	✓	✓	✓
	Azure Lighthouse	✓	✓	✓	✓
	Azure Managed Applications	✓	✓	✓	✓
	Azure Migrate	✓	✓	✓	✓
	Azure Monitor	✓	✓	✓	✓
	Azure Policy	✓	✓	✓	✓
	Azure Quotas	✓	✓	✓	✓
	Azure Resource Graph	✓	✓	✓	✓
	Azure Resource Manager (ARM)[8]	✓	✓	✓	✓
	Azure Resource Mover	✓	✓	✓	✓
	Azure Signup Portal	✓	✓	✓	✓
	Azure Update Manager	✓	✓	-	✓
	Cloud Shell	✓	✓	✓	✓
	Cost Management	✓	✓	✓	✓
	Microsoft Azure Portal[8]	✓	✓	✓	✓
	Microsoft Purview (Governance)[9]	✓	✓	✓	✓
Security	Azure Confidential Computing	✓	-	✓	✓
	Azure Confidential Ledger	✓	-	-	✓
	Azure Dedicated HSM	✓	✓	✓	✓
	Azure Payment HSM	✓	-	✓	✓
	Customer Lockbox for Microsoft Azure	✓	✓	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Key Vault	✓	✓	✓	✓
	Microsoft Azure Attestation	✓	-	✓	✓
	Microsoft Copilot for Security	✓	-	-	✓
	Microsoft Defender Experts for Hunting	✓	-	-	✓
	Microsoft Defender Experts for XDR	✓	-	-	✓
	Microsoft Defender for Cloud	✓	✓	✓	✓
	Microsoft Defender Threat Intelligence	✓	-	✓	✓
	Microsoft Sentinel	✓	✓	✓	✓
	Multi-Factor Authentication	✓	✓	✓	✓
	Windows Autopatch	✓	-	✓	✓
Media	Azure Media Services	✓	✓	✓	✓
Web	Azure Fluid Relay	✓	✓	✓	✓
	Azure Maps	✓	✓	✓	✓
	Azure SignalR Service	✓	✓	✓	✓
	Azure Spring Apps	✓	-	✓	✓
	Azure Web PubSub	✓	✓	✓	✓
Mixed Reality	Remote Rendering	✓	-	✓	✓
	Spatial Anchors	✓	-	✓	✓
Hybrid + MultiCloud	Azure Arc enabled System Center Virtual Machine Manager	✓	-	✓	✓
	Azure Arc enabled VMware vSphere	✓	-	✓	✓
	Azure Center for SAP Solutions	✓	-	✓	✓
	Azure Kubernetes Service on AzureStack HCI	✓	-	✓	✓

Product Category	Offering / Service	Cloud Environment Scope		Examination Period Scope[7]	
		Azure	Azure Government	H2 FY24	H1 FY25
	Azure Operator Nexus	✓	-	-	✓
	Azure Operator Service Manager	✓	-	-	✓
	Azure Monitor for SAP Solutions	✓	-	✓	✓
Internal Supporting Services[7,10]		✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H2 FY24	H1 FY25
Microsoft Online Services				
Appsource	✓	-	✓	✓
Dynamics 365 Customer Voice	✓	-	✓	✓
Endpoint Attack Notifications	✓	-	✓	✓
Intelligent Recommendations	✓	-	✓	✓
Microsoft Copilot Studio	✓	✓	✓	✓
Microsoft Defender for Cloud Apps	✓	✓	✓	✓
Microsoft Defender for Endpoint	✓	✓	✓	✓
Microsoft Defender for Identity	✓	✓	✓	✓
Microsoft Graph	✓	✓	✓	✓

[10] Azure Government scope boundary for internal services: Access Monitoring, Asimov Event Forwarder, Atlas, Autopilot Security, AzCP Platform, Azure Diagnostic Services, Azure Notebooks Component, Azure Security Monitoring (ASM SLAM), Azure Service Health, Azure Stack Bridge, Azure Stack Diagnostics and Analytics Service, Azure Stack Edge Service, Azure Support Center, Azure System Lockdown, Azure Throttling Solutions, Azure Watson, CoreWAN, dSCM, dSMS, dSTS, Dynamics 365 Integrator App, Fabric Controller Fundamental Services, Fabric Network Devices, Gateway Manager, Geneva Actions, Geneva Analytics Orchestration, Geneva Warm Path, Interflow, JIT, M365D Automated IR, M365D Investigation and Exploration, M365D Management Service, MDM, MEE Privacy Service, Microsoft Bot Framework, Microsoft Email Orchestrator, MSaaS File Management (DTM V2), MSFT.RR DNS, Network Billing, OneBranch Release, OneDeploy Deployment Infrastructure (DE), OneDS Collector, PF-FC, Pilotfish, PMI Foundation, Resource Provider Service as a Service, Unified Remote Scanning (URSA), Vulnerability Scanning & Analytics, WaNetMon, Windows Azure Jumpbox, and Workflow. The coverage period for internal services for both Azure and Azure Government is October 1, 2023 through September 30, 2024 except for those specified with shorter coverage periods in the *Internal Supporting Services* subsection herein.

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H2 FY24	H1 FY25
Microsoft Intune	✓	✓	✓	✓
Microsoft Managed Desktop	✓	-	✓	✓
Microsoft Stream	✓	✓	✓	✓
Nomination Portal	✓	-	✓	✓
Power Apps	✓	✓	✓	✓
Power Automate	✓	✓	✓	✓
Power BI	✓	✓	✓	✓
Windows Update for Business reports	✓	-	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H2 FY24	H1 FY25
Microsoft Dynamics 365				
Chat for Dynamics 365	✓	✓	✓	✓
Dataverse	✓	✓	✓	✓
Dynamics 365 AI Customer Insights	✓	✓	✓	✓
Dynamics 365 Athena - CDS to Azure Data Lake	✓	✓	✓	✓
Dynamics 365 Business Central	✓	-	✓	✓
Dynamics 365 Commerce	✓	-	✓	✓
Dynamics 365 Contact Center	✓	-	-	✓
Dynamics 365 Customer Insights - Data	✓	-	✓	✓
Dynamics 365 Customer Insights - Journeys	✓	-	✓	✓
Dynamics 365 Customer Service	✓	✓	✓	✓
Dynamics 365 Field Service	✓	✓	✓	✓
Dynamics 365 Finance	✓	✓	✓	✓
Dynamics 365 Fraud Protection	✓	-	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H2 FY24	H1 FY25
Dynamics 365 Guides	✓	-	✓	✓
Dynamics 365 Human Resources	✓	-	✓	✓
Dynamics 365 Intelligent Order Management	✓	-	✓	✓
Dynamics 365 Project Operations	✓	-	✓	✓
Dynamics 365 Remote Assist	✓	-	✓	✓
Dynamics 365 Resource Scheduling Optimization	✓	✓	-	✓
Dynamics 365 Sales	✓	✓	✓	✓
Dynamics 365 Sales Insights	✓	-	✓	✓
Dynamics 365 Supply Chain Management	✓	-	✓	✓
Microsoft Power Platform on Azure	✓	✓	✓	✓
Nuance Conversational IVR	✓	-	-	✓
Power Pages	✓	✓	✓	✓

Offering	Cloud Environment Scope		Examination Period Scope[7]	
	Azure	Azure Government	H2 FY24	H1 FY25
Microsoft Cloud for Financial Services				
Unified Customer Profile	✓	-	✓	✓
Collaboration Manager	✓	-	✓	✓
Customer Onboarding	✓	-	✓	✓

Regions Covered by this Report

Azure production infrastructure is located in globally distributed datacenters. These datacenters across multiple regions 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:

Azure Regions

Americas

- West US
- West US 2
- West US 3
- West Central US
- Central US
- USGOV Iowa
- North Central US
- USGOV Arizona
- South Central US
- USGOV Texas
- East US
- East US 2
- USGOV Virginia
- USGOV Wyoming
- Canada East
- Canada Central
- Mexico Central[11]
- Brazil South
- Brazil Southeast

APAC

- Australia East
- Australia Southeast
- Australia Central
- Australia Central 2
- West India
- Central India
- Jio India West
- Jio India Central
- South India
- East Asia
- Japan West
- Japan East
- Southeast Asia
- Korea South
- Korea Central
- Malaysia South
- Taiwan North[11]
- Taiwan Northwest[11]

EMEA

- West Europe
- North Europe
- UK South
- UK West
- France Central
- France South
- Germany North
- Germany West Central
- Spain Central[11]
- Switzerland West
- Switzerland North
- Norway East
- Norway West
- Qatar Central
- Sweden Central
- Sweden South
- Poland Central
- Italy North
- South Africa North
- South Africa West
- UAE Central
- UAE North
- Israel Central

In addition to the datacenters included in the Azure regions listed above, there are datacenters outside of those regions which are included in the scope of the examination and are supporting Microsoft 365 services. Note that the Microsoft 365 services are not included in the scope of the examination.

[11] Examination period for the Azure region was from April 1, 2024 to September 30, 2024.

Edge Sites

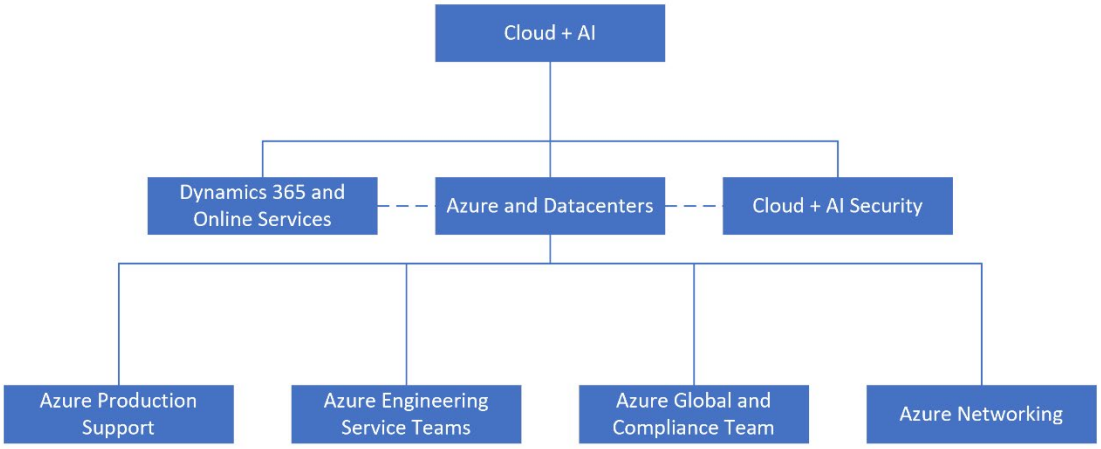
- Athens, Greece (ATH01)
- Atlanta, GA (ATA)
- Auckland, New Zealand (AKL30)
- Bangkok, Thailand (BKK30)
- Barcelona, Spain (BCN30)
- Barueri, Brazil (GRU30)
- Berlin, Germany (BER30)
- Bogota, Colombia (BOG30)
- Brisbane, Australia (BNE01)
- Brussels, Belgium (BRU30)
- Bucharest, Romania (BUH01)
- Budapest, Hungary (BUD01)
- Buenos Aires, Argentina (BUE30)
- Busan, South Korea (PUS03)
- Cairo, Egypt (CAI30)
- Cape Town, South Africa (CPT02/30)
- Chicago, IL (CHG, CHI30)
- Cincinnati, OH (CVG30)
- Copenhagen, Denmark (CPH30)
- Dallas, TX (DFW30)
- Detroit, MI (DTT30)
- Doha, Qatar (DOH30[12]/31)
- Dubai, United Arab Emirates (DXB30)
- Dusseldorf, Germany (DUS30)
- Frankfurt, Germany (FRA/31)
- Geneva, Switzerland (GVA30)
- Helsinki, Finland (HEL02)
- Ho Chi Minh City, Vietnam (SGN30)
- Hong Kong (HKB, HKG30)
- Honolulu, HI (HNL01)
- Houston, TX (HOU01)
- Hyderabad, India (HYD30)
- Istanbul, Turkey (IST30)
- Jakarta, Indonesia (JKT30)
- Jacksonville, FL (JAX30)
- Johannesburg, South Africa (JNB02)
- Kuala Lumpur, Malaysia (KUL30)
- Luanda, Angola (LAD30)
- Lisbon, Portugal (LIS01)
- London, United Kingdom (LON04, LTS)
- Los Angeles, CA (LAX)
- Lagos, Nigeria (LOS30)
- Madrid, Spain (MAD30)
- Manchester, United Kingdom (MAN30/31)
- Manila, Philippines (MNL30)
- Memphis, TN (MEM30)
- Miami, FL (MIA)
- Milan, Italy (MIL30)
- Minneapolis, MN (MSP30)
- Montreal, Canada (YMQ01)
- Mumbai, India (BOM02)
- Munich, Germany (MUC30)
- Nairobi, Kenya (NBO30)
- Nashville, TN (BNA30)
- New Delhi, India (DEL01)
- New York City, NY (NYC)
- Newark, NJ (EWR30)
- Osaka, Japan (OSA30/31)
- Oslo, Norway (OSL30)
- Palo Alto, CA (PAO)
- Paris, France (PRA)
- Philadelphia, PA (PHL30)
- Phoenix, AZ (PHX31)
- Portland, OR (PDX31)
- Prague, Czech Republic (PRG01)
- Pune, India (PNQ30)
- Queretaro, Mexico (MEX30/31)
- Rabat, Morocco (RBA30)
- Rio de Janeiro (RIO02/03)
- Rome, Italy (ROM30)
- Sao Paulo, Brazil (SAO31)
- Salt Lake City, UT (SLC31)
- Seattle, WA (WST, STB)
- Seoul, South Korea (SLA)
- Singapore (SGE, SIN30, SG1)
- Sofia, Bulgaria (SOF01)
- Stockholm, Sweden (STO)
- Taipei, Taiwan (TPE30/31)
- Tel Aviv, Israel (TLV30)
- Teterboro, NJ (TEB31)
- Tokyo, Japan (TYA/TYB)
- Toronto, Canada (YTO01/30)
- Warsaw, Poland (WAW01/30)
- 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.

[12] Examination period for the edge site was from April 1, 2024 to September 30, 2024.

People

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



Online, Infrastructure, and Platform Services

Online services are software hosted in Azure Engineering Service teams managed production subscriptions for the purpose of making an Azure offering available or delivering features and capabilities to the Azure product. Infrastructure services manage the data center hardware that is essential for Azure services to run. Platform services manage the availability and features of a platform on which an Azure online service is hosted. Altogether, Online, Infrastructure, and Platform services manage the service lifecycle of the finished PaaS, SaaS, and IaaS Azure offerings.

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 Security Development Lifecycle (SDL). They also perform security reviews and provide security guidance for the datacenters. This team consists of personnel responsible for:

- Security Development Lifecycle
- Security incident response
- Driving security functionality within service development work

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

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

- Azure 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.
- Azure App Service: App Center: App Center 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.
- Azure 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 tools running on any OS, source code control driven deployments, as well as from within the Visual Studio Integrated Development Environment (IDE).

- Azure App Service Static Web Apps: Static Web Apps offers streamlined full-stack development from source code to global high availability. It allows customers accelerated app development with a static front end and dynamic back end powered by serverless APIs. Customers experience high productivity with a tailored local development experience, GitHub native workflows to build and deploy apps, and unified hosting and management in the cloud.

Azure Arc: Azure Arc allows customers to manage, monitor and govern machines running on-premises or in other clouds, from Azure.

Azure Cloud Services: Azure Cloud Services is a PaaS service designed to support applications that are scalable, reliable, and inexpensive to operate. Azure 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 Azure 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.

Azure Cloud Services (Extended Support): Azure Cloud Services (extended support) is a new Azure Resource Manager (ARM) based deployment model for Azure Cloud Services product. It has the primary benefit of providing regional resiliency along with feature parity with Azure Cloud Services deployed using Azure Service Manager. It also offers some ARM capabilities such as role-based access and control (RBAC), tags, policy, and supports deployment of ARM templates.

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 Hypertext Transfer Protocol (HTTP) endpoints accessible by mobile and Internet of Things (IoT) devices.

Azure Large Instances: Azure Large Instances is intended for critical workloads that require special architecture, certified hardware, or extraordinarily large servers. Azure Large Instances implementations are dedicated only to the customer, and customers have full access (root access) to the operating system (OS). Customers can manage OS and application installation according to their needs. For security, the instances are provisioned within the customer Azure Virtual Network (VNet) with no Internet connectivity.

Azure Machine Configuration: Azure Machine Configuration provides management and configuration capabilities to Azure compute resources in Azure and Arc VMs. Azure Machine Configuration uses the Azure policy to audit the internal configuration of a VM's OS, deployed applications, and the environment configuration. Azure Machine Configuration is a digital security and risk engineering DevOps Kit baseline control and helps audit VM configurations.

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.

Azure Virtual Desktop: Azure Virtual Desktop is a virtualization management service running on Azure that provisions and manages connections to virtual desktops and apps on Windows 7, Windows 10, Windows Server 2012 R2+ in single or multi-session environments. It allows users to set up a scalable and flexible environment as well as connect, deploy to, and manage virtual desktops.

Azure Virtual Machines: Azure 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.

Azure Virtual Machine Scale Sets: Azure 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.

Azure VM Image Builder: Azure VM Image Builder is an Azure Resource Provider service that allows customers to create custom virtual machine images.

Azure VMware Solution: Azure VMware Solution delivers a comprehensive VMware environment in Azure allowing customers to run native VMware workloads on Azure. Azure VMware Solution allows customers to seamlessly run, manage and secure applications across VMware environments and Microsoft Azure with a common operating framework.

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.

Planned Maintenance: Planned Maintenance is responsible for the roll out of planned maintenance activities to the nodes and VMs in Azure.

Containers

Azure Arc Enabled Kubernetes: Azure Arc Enabled Kubernetes allows customers (cluster operators) to use Azure as their single control plane for connecting, configuring and governing their Kubernetes clusters spread out across other public clouds and on-premise environments.

Azure Container Apps: Azure Container Apps is a fully managed environment that enables customers to run microservices and containerized applications on a serverless platform. Common uses of Azure Container Apps include deploying API endpoints, hosting background processing applications, handling event-driven processing, and running microservices.

Azure Container Instances: Azure Container Instances enables the creation of containers as first-class objects in Azure, without requiring VM management and without enforcing any prescriptive application model. Azure 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.

Azure Container Registry: Azure Container Registry allows customers the ability to store images for all types of container deployments including DC / OS, Docker Swarm, Kubernetes, and Azure services such as Azure App Service, Batch, Azure Service Fabric, and others. Developers can manage the configuration of apps isolated from the configuration of the hosting environment. Azure 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.

Azure Kubernetes Configuration Management: Azure Kubernetes Configuration Management allows customers (cluster operators) to use GitOps to manage configuration on various Kubernetes clusters - Azure Arc connected clusters, AKS clusters, and eventually other cluster types like Azure Red Hat OpenShift (ARO).

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: 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.

Microsoft Artifact Registry: Microsoft Artifact Registry is a registry of Docker and Open Container Initiative (OCI) images, with support for all OCI artifacts. It allows users to build, store, secure, scan, replicate, and manage container images and artifacts with a fully managed, geo-replicated instance of OCI distribution.

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 Remote Desktop Protocol (RDP) and Secure Shell (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 Communications Gateway: Azure Communications Gateway is a managed, cloud-based voice gateway that simplifies connecting operator fixed and mobile voice networks to Teams Phone. It combines a high-availability, Teams-certified and mobile-standards-compliant Session Border Controller (SBC) with API mediation function, removing the need for disruptive voice network changes and substantial IT system integration projects.

Azure Content Delivery Network: Azure 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.

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 Domain Name System (DNS) domains that provides name resolution by using Microsoft Azure infrastructure. Azure DNS lets customers host their 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 Azure 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 Load Balancer: Azure 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.

Azure NAT Gateway: Azure NAT (network address translation) Gateway simplifies outbound-only Internet connectivity for virtual networks. When configured on a subnet, all outbound connectivity uses specified static public IP addresses. Outbound connectivity is possible without a load balancer or public IP addresses directly attached to virtual machines.

Azure Orbital Ground Station: Azure Orbital Ground Station is a fully managed end-to-end service that enables customers to communicate, downlink, and process data from their satellites' spacecrafts on a pay-as-you-go basis without needing them to build their own satellite ground stations.

Azure Peering Service: Azure Peering Service is a networking service that enhances customer connectivity to Microsoft cloud services such as Microsoft 365, Dynamics 365, SaaS services, Azure, or any Microsoft services

accessible via the public Internet. Microsoft has partnered with Internet Service Providers (ISPs), Internet Exchange Partners, and Software-Defined Cloud Interconnect (SDCI) providers worldwide to provide reliable and high-performing public connectivity with optimal routing from the customer to the Microsoft network.

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 Private MEC: Azure Private MEC is a solution that delivers ultra-low-latency networking, applications, and services at the enterprise edge. It enables customers to accelerate time to market, reduce integration complexity, and improve security of end-to-end solutions.

Azure Route Server: Azure Route Server enables the customer's network appliances to exchange route information with Azure virtual networks dynamically. It allows customers to exchange routing information directly through Border Gateway Protocol (BGP) routing protocol between any Network Virtual Appliances (NVA) that supports the BGP routing protocol and the Azure Software Defined Network (SDN) in the Azure Virtual Network (VNET) without the need to manually configure or maintain route tables.

Azure Traffic Collector: Azure Traffic Collector enables sampling of network flows sent over the customer's ExpressRoute circuits. Flow logs get sent to a Log Analytics workspace where customers can create their own log queries for further analysis.

Azure Virtual Network: Azure 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.

Azure Virtual Network IP Services: Azure Virtual Network IP Services allows Internet resources to communicate inbound to Azure resources, as well as providing a predictable method for communicating outbound to the Internet and other public-facing Azure services. Customers can associate IP Services addresses to virtual machine network interfaces, public load balancers, VPN gateways, and other resources.

Azure Virtual Network Manager: Azure Virtual Network Manager is a management service that enables customers to group, configure, deploy, and manage virtual networks globally across subscriptions. With Virtual Network Manager, customers can define network groups to identify and logically segment their virtual networks. Customers can determine the connectivity and security configurations they want and apply them across all the selected virtual networks in network groups at once.

Azure Web Application Firewall: Azure Web Application Firewall 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.

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 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.

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).

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. 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 (Server Message Block (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 Managed Lustre: Azure Managed Lustre is a managed, pay-as-you-go file system for high-performance computing (HPC) and AI workloads that provides the open-source Lustre file system as a service. The Lustre file system is used in AI and HPC [High Performance Computing] scenarios for high-throughput applications.

Azure NetApp Files: Azure NetApp Files enables enterprise line-of-business and storage professionals to migrate and run complex, file-based applications with no code change. It is widely used as the underlying shared file-

storage service in various scenarios. These include migration (lift and shift) of POSIX-compliant Linux and Windows applications, SAP HANA, databases, HPC infrastructure and apps, and enterprise web applications.

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 Access Control List (ACLs), and 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 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 Representational State Transfer (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.
- Azure Disk Storage: Azure Disk Storage offers high throughput, high Input / Output Operations Per Second, 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 Disk Storage is suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.

- 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 Storage Mover: Azure Storage Mover is a fully managed, hybrid migration service that enables customers to migrate on-premises file shares to Azure.

Databases

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 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 Health Data Services: Azure Health Data Services 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 Health Data Services improves health technologies' interoperability and makes it easier to manage data.

Azure SQL: Azure SQL is a relational database service that lets customers rapidly create, extend, and scale relational applications into the cloud. Azure SQL 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 provides a familiar programming model based on T-SQL and supports existing SQL Server tools, libraries and APIs.

Azure SQL Managed Instance: Azure SQL Managed Instance is a PaaS service that has near 100% compatibility with the latest Enterprise Edition SQL Server database engine, providing a native virtual network (VNet) implementation that addresses common security concerns, and a business model favorable to existing SQL Server customers. SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes.

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

Microsoft Azure Managed Instance for Apache Cassandra: Microsoft Azure Managed Instance for Apache Cassandra provides automated deployment and scaling operations for managed open-source Apache Cassandra datacenters, accelerating hybrid scenarios and reducing ongoing maintenance.

SQL Managed Instance enabled by Azure Arc: SQL Managed Instance enabled by Azure Arc is designed to provide the existing SQL server applications an option to migrate to the latest version of the SQL Server engine and gain the PaaS style built in management capabilities without moving outside of the existing infrastructure, allowing customers to maintain the data sovereignty and meet other compliance criteria. This is achieved by leveraging the Kubernetes platform with Azure data services, which can be deployed on any infrastructure.

SQL Server enabled by Azure Arc: SQL Server enabled by Azure Arc extends Azure services to SQL Server instances hosted outside of Azure, in the customer's data center, in edge site locations like retail stores, or any public cloud or hosting provider. Azure Arc enables customers to manage all of their SQL Servers from a single point of control. As customers connect their SQL Servers to Azure, they get a single place to view the detailed inventory of their SQL Servers and databases.

SQL Server on Azure Virtual Machines: SQL Server on Azure Virtual Machines is a cloud database that allows users to migrate their SQL Server workloads to the cloud without having to manage any on-premise hardware. It can get the performance, security, and analytics of SQL Server backed by the flexibility and hybrid connectivity of Azure.

SQL Server Stretch Database: SQL Server Stretch Database helps customers migrate warm and cold transactional data transparently and securely to Azure while still providing inexpensive long data retention times.

Developer Tools

Azure App Configuration: Azure App Configuration allows customers to manage configuration within the cloud. Customers can create App Configuration stores to store key-value settings and consume stored settings from within applications, deployment pipelines, release processes, microservices, and other Azure resources. App Configuration allows customers to store and manage configurations effectively and reliably, in real time, without affecting customers by avoiding time-consuming redeployments.

Azure Deployment Environments: Azure Deployment Environments empowers development teams to quickly and easily spin up app infrastructure with project-based templates that establish consistency and best practices while maximizing security. This on-demand access to secure environments accelerates the stages of the software development lifecycle in a compliant and cost-efficient way.

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 for Education: Azure for Education provides resources for students to learn about programming, cloud technologies, and world-class developer tools.

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.

Azure Load Testing: Azure Load Testing is a fully managed load-testing service that enables customers to generate high-scale load. The service simulates traffic for applications, regardless of where they are hosted. Developers, testers, and quality assurance (QA) engineers can use it to optimize application performance, scalability, or capacity.

Azure Managed Grafana: Azure Managed Grafana is a fully managed service for analytics and monitoring solutions. It is supported by Grafana Enterprise, which provides extensible data visualizations. Grafana dashboards are deployed with built-in high availability and control access with Azure security.

GitHub AE: GitHub AE is a security-enhanced and compliant way to use GitHub in the cloud. GitHub AE enables customers to move DevOps workload to the cloud while meeting stringent security and compliance requirements. GitHub AE is fully managed, reliable, and scalable, allowing the customer to accelerate delivery without sacrificing risk management. GitHub AE offers one developer platform from idea to production. Customers can increase development velocity, while maintaining industry and regulatory compliance with unique security and access controls, workflow automation, and policy enforcement.

Microsoft Dev Box: Microsoft Dev Box is an Azure service that gives developers self-service access to preconfigured, project-specific developer boxes. It provides developers the ability to connect on demand and work across multiple dev boxes to avoid configuration conflicts. Users can manage dev boxes with physical devices in Microsoft Intune to maximize security, compliance, and cost efficiency.

Service Connector: Service Connector is an Azure-managed service that helps developers easily connect compute services to target backing services. Service Connector configures the network settings and connection information between compute services and target backing services in the management plane.

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 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 Chaos Studio: Azure Chaos Studio helps customers to measure, understand, and build application and service resilience to real-world incidents, such as a region going down or an application failure causing 100% CPU usage on a VM. With Chaos Studio, customers can run chaos engineering experiments that inject faults against their service and then monitor how the service responds to disruptions.

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 Factory: Azure 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 processes code free in an intuitive visual environment, and easily operationalize and manage the data pipelines at scale.

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 HDInsight: Azure 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. Azure HDInsight includes Apache Hbase, a columnar NoSQL database that runs on top of the HDFS. This supports large transactional processing (Online Transaction Processing) of non-relational data, enabling use cases like interactive websites or having sensor data written to Azure Blob Storage. Azure 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, Azure HDInsight includes Apache Spark, an open-source project in the Apache ecosystem that can run large-scale data analytics applications in memory. Lastly, Azure HDInsight incorporates R Server for Hadoop, a scale-out implementation of one of the most popular programming languages for statistical computing and machine learning. Azure HDInsight offers Linux clusters when deploying Big Data workloads into Azure.

Azure Operator Insights: Azure Operator Insights is a fully managed service that enables users with the collection and analysis of massive quantities of network data gathered from complex multi-part or multi-vendor network functions. It delivers statistical, machine learning, and AI-based insights for operator-specific workloads to help operators understand the health of their networks and the quality of their subscribers' experiences in near real-time.

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 Lake Analytics: Data Lake Analytics is a distributed analytics service built on Apache Yet Another Resource Negotiator 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 Microsoft Entra ID 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, and Azure Synapse Analytics.

Microsoft Fabric: Microsoft Fabric is an all-in-one analytics solution for enterprises that covers everything from data movement to data science, real-time analytics, and business intelligence. Microsoft Fabric brings together new and existing components from Power BI, Azure Synapse, and Azure Data Factory into a single integrated environment. These components are then presented in various customized user experiences.

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 AI Services: Azure AI 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.

Azure AI Services: AI Anomaly Detector: Azure AI Services: AI 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.

Azure AI Services: Azure AI Containers: Azure AI services: Azure AI Containers provide several Docker containers that let customers use the same APIs that are available in Azure, on-premises. Using these containers gives customers the flexibility to bring Azure AI services closer to their data for compliance, security or other operational reasons.

Azure AI Services: Azure AI Content Safety: Azure AI Services: Azure AI Content Safety 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.

Azure AI Services: Azure AI Custom Vision: Azure AI Services: Azure AI Custom Vision is an Azure AI 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.

Azure AI Services: Azure AI Document Intelligence: Azure AI Services: Azure AI Document Intelligence is an Azure AI 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. Azure AI Document Intelligence is comprised of custom models, the prebuilt receipt model, and the layout API. Customers can call Azure AI Document Intelligence models by using a REST API to reduce complexity and integrate it into a workflow or an application.

Azure AI Services: Azure AI Face Service: Azure AI Services: Azure AI Face Service 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.

Azure AI Services: Azure AI Immersive Reader: Azure AI Services: Azure AI Immersive Reader is a service that lets customers embed text reading and comprehension capabilities into applications. Azure AI Immersive Reader helps users of any age and reading ability with features like reading aloud, translating languages, and focusing attention through highlighting and other design elements.

Azure AI Services: Azure AI Language: Azure AI Services: Azure AI Language is a cloud-based service that provides Natural Language Processing (NLP) features for understanding and analyzing text. This service is used to help build intelligent applications using the web-based Language Studio, REST APIs, and client libraries. Azure AI Language includes language customization capabilities such as custom Named Entity Recognition (NER), custom text classification, and conversational language understanding.

Azure AI Services: Azure AI Metrics Advisor: Azure AI Services: Azure AI Metrics Advisor uses AI to perform data monitoring and anomaly detection in time series data. The service automates the process of applying models to the customer's data, and provides a set of APIs and a web-based workspace for data ingestion, anomaly detection, and diagnostics, without needing to know machine learning.

Azure AI Services: Azure AI Personalizer: Azure AI Services: Azure AI 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. Azure AI Personalizer collects and uses real-time information customers provide about content and context in order to select the most relevant content. Azure AI 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.

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

Azure AI Services: Azure AI Translator: Azure AI Services: Azure AI 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.

Azure AI Services: Azure AI Video Indexer: Azure AI Services: Azure AI 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.

Azure AI Services: Azure AI Vision: Azure AI Services: Azure AI 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.

Azure AI Services: Conversational Language Understanding: Azure AI Services: Conversational 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.

Azure AI Services: Question Answering: Azure AI Services: Question Answering is an Azure AI 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.

Azure AI Bot Service: Azure AI Bot Service helps developers build bots / intelligent agents and connect them to the communication channels their users are in. Azure AI 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 Health Bot: Azure Health 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.

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 OpenAI Service: Azure OpenAI Service provides REST API access to OpenAI's language models including the GPT-3, Codex and Embeddings model series. These models can be adapted to the customer's specific task including content generation, summarization, semantic search, and natural language to code translation. Customers can access the service through REST APIs, Python SDK, or our web-based interface in the Azure OpenAI Studio.

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 and ML Ops. It is open-source friendly and works with any Python framework, such as PyTorch, TensorFlow, or scikit-learn.

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 365 Copilot for Sales: Microsoft 365 Copilot for Sales is a tool designed to increase productivity through CRM task automation, auto-generated email or meeting summaries, and more. Microsoft Copilot for Sales also generates AI-assisted content and recommendations, in addition to real-time customer opportunity insights.

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

Seeing AI: Seeing AI is a free consumer mobile app that narrates the world by using AI and describes nearby people, text, and objects for the blind and low vision community.

Internet of Things

Azure Digital Twins: Azure Digital Twins is an IoT platform that enables the customer's business to create a digital representation of real-world things, places, business processes, and people.

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

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 are 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.

Azure Sphere: Azure Sphere is a secured, high-level application platform with built-in communication and security features for Internet-connected devices. It comprises a secured, connected, crossover microcontroller unit, a custom high-level Linux-based OS, and a cloud-based security service that provides continuous, renewable security.

Azure Time Series Insights: Azure 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.

Device Update for IoT Hub: Device Update for IoT Hub enables customers to deploy over-the-air updates for IoT devices. It is an end-to-end platform that customers can use to publish, distribute, and manage over the air updates for all devices from tiny sensors to gateway level devices.

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.

Microsoft Cloud for Sustainability: Microsoft Cloud for Sustainability enables customers to reach their environmental sustainability goals and advance their conservation efforts with secure, globally scalable, and innovative IoT solutions. Customers can reduce their energy usage in their factory or building, monitor the quality of their water output and decrease material waste spillage, and also to help prevent wildlife poaching and keep watch on endangered habitats.

Microsoft Defender for IoT: Microsoft Defender for IoT provides customers with security protection by delivering unified visibility and control, adaptive threat prevention, and intelligent threat detection and response across IoT devices, IoT edges and IoT hubs running on-premises and in Azure cloud. It provides unified security management that enables end-to-end threat detection and analysis across hybrid cloud workloads and on customer's Azure IoT solution.

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, Firebase Cloud Messaging service, Windows Push Notification Service, Microsoft Push Notification Service, 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.

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.

Azure Data Manager for Energy: Azure Data Manager for Energy helps energy companies gain actionable insights, improve operational efficiency, and accelerate time to market on the enterprise-grade, cloud-based OSDU (Open Subsurface Data Universe) data platform service. It supports innovation with a flexible, open energy platform that customers can customize according to their needs.

Azure Logic Apps: Azure 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, Microsoft 365, Twitter, Dropbox, Google services, and more.

Azure Service Bus: Azure 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 messaging, and publish / subscribe capabilities. Service Bus uses AMQP, Service Bus Messaging Protocol (SBMP), and HTTP as its primary protocols. Additionally, Azure Relay is a multi-tenant service offering that enables connectivity across network boundaries without normally required networking infrastructure.

Universal Print: Universal Print is a modern print solution that organizations can use to manage their print infrastructure through cloud services from Microsoft. This cloud-based print solution provides secure printing, and eliminates the need for an on-premises infrastructure.

Identity

Azure Active Directory B2C: Azure Active Directory B2C extends Microsoft Entra ID 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.

Microsoft Entra Domain Services: Microsoft Entra 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 (AD). Customers can consume these domain services without the need to deploy, manage, and patch domain controllers in the cloud. Microsoft Entra Domain Services integrates with the existing Microsoft Entra ID tenant, thus making it possible for users to log in using their corporate credentials.

Microsoft Entra ID: Microsoft Entra ID (formerly 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. Microsoft Entra ID comes in three editions: Free, Basic, and Premium. Self-service credentials management is a feature of Microsoft Entra ID that allows Microsoft Entra ID 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 Microsoft Entra ID that provides the backend to support authentication and provisioning for Microsoft Entra ID.

Microsoft Entra Permissions Management: Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) service that provides comprehensive visibility and control over permissions for all identities and resources in customer's Microsoft Azure, Amazon Web Services (AWS) and Google Cloud Platform (GCP) accounts. It detects, automatically right-sizes, and continuously monitors for unused and excessive permissions.

Microsoft Global Secure Access: Microsoft Global Secure Access is designed to provide secure and seamless access to applications and resources, regardless of location. Built upon the core principles of Zero Trust, it ensures least privilege, explicit verification, and assumes breach to maintain security.

Microsoft Purview Information Protection: Microsoft Purview Information Protection controls and helps secure email, documents, and sensitive data that customers share outside their company walls. Microsoft Purview Information Protection provides enhanced data protection capabilities to customers and assists them with

classification of data using labels and permissions. Microsoft Purview Information Protection includes Azure Rights Management, which used to be a standalone Azure service.

Management and Governance

Application Change Analysis: Application Change Analysis is a subscription-level Azure resource provider. It checks for resource changes in the subscription, and provides data for various diagnostic tools to help users understand what changes might have caused issues.

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 Quotas: Azure Quotas enables Azure end customers to view and manage quotas for Azure Services by subscription. It provides the capability to request Quota increase inline for adjustable quotas and eliminate latency between the fulfillment and what customer can see in their portal.

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 (ARM): 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.

Azure Resource Mover: Azure Resource Mover helps customers smoothly orchestrate moves for various Azure resources between regions. Customers can move resources to different Azure regions to align to a region launch, align for services / features, respond to business developments, align for proximity, meet data requirements, respond to deployment requirements or respond to decommissioning. Azure Resource Mover provides a single

hub for moving resources across regions, allowing for reduced move time and complexity, simple and consistent experience, easy identification of dependencies, automatic cleanup of resources, and testing.

Azure Signup Portal: Azure Signup Portal enables customers to sign up for Azure subscriptions. The service handles pre-requisites for signup such as Commerce account creation, Payment Instrument attachment, agreement acceptance, etc., and then finally funnels the user down to provisioning of a new subscription.

Azure Update Manager: Azure Update Manager service helps manage updates for all customers machines, including those running on Windows and Linux, across Azure, on-premises, and on other cloud platforms. It helps customers with monitoring update compliance from a single dashboard, make system updates in real-time, schedule updates within a maintenance window, or automatically update during off-peak hours.

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.

Cost Management: Cost management is an external offering for cloud cost management capabilities included with Azure subscriptions for financial governance for the customer's organization. It provides the ability to explore cost and usage data via multidimensional analysis, where creating customized filters and expressions allow the customer to answer consumption-related questions for their Azure resources.

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 MOCP. MOCP and MSA / Organizational Accounts and their associated authentication mechanisms are not in scope for this SOC report.

Microsoft Purview (Governance): Microsoft Purview (Governance) is a unified data governance service that helps customers manage and govern on-premises, multi-cloud, and SaaS data. Customers can easily create a holistic, up-to-date map of their data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage. Note: Only the Microsoft Purview Governance sub-offering is certified by this report.

Security

Azure Confidential Computing: Azure Confidential Computing offers customers with solutions to enable isolation of sensitive data while it is being processed in the cloud. Azure Confidential Computing lets processing of data from multiple sources without exposing the input data to other parties. This type of secure computation enables many scenarios like anti-money laundering, fraud-detection, and secure analysis of healthcare data.

Azure Confidential Ledger: Azure Confidential Ledger provides customers a managed and decentralized ledger for data entries backed by Blockchain. Customers can maintain data integrity by preventing unauthorized or accidental modification with tamperproof storage. The service helps protect customer's data at rest, in transit, and in use with hardware-backed secure enclaves used in Azure Confidential Computing.

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

Azure Payment HSM: Azure Payment HSM is a bare metal Infrastructure as a Service (IaaS) that provides cryptographic key operations for real-time payment transactions in Azure. It is delivered using Thales payShield 10K payment HSMs and meets the most stringent payment card industry (PCI) requirements for security, compliance, low latency, and high performance.

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 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.

Microsoft Azure Attestation: Microsoft Azure Attestation enables customers to verify the identity and security posture of a platform before the user interacts with it. Azure Attestation receives evidence from the platform, validates it with security standards, evaluates it against configurable policies, and produces an attestation token for claims-based applications. The service supports attestation of trusted platform modules (TPMs) and trusted execution environments (TEEs) and virtualization-based security (VBS) enclaves.

Microsoft Copilot for Security: Microsoft Copilot for Security empowers security and IT teams to protect organizations at the speed and scale of AI. It is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale. It helps support security professionals in end-to-end scenarios such as incident response, threat hunting, intelligence gathering, and posture management.

Microsoft Defender Experts for Hunting: Microsoft Defender Experts for Hunting is a proactive threat hunting service that goes beyond the endpoint to hunt across endpoints, Microsoft 365, cloud applications, and identity. Microsoft Defender Experts will investigate any findings and hand off the associated contextual alert information, along with remediation instructions, to customers so they can quickly respond.

Microsoft Defender Experts for XDR: Microsoft Defender Experts for XDR is a managed extended detection and response service that helps Security Operations Centers (SOCs) focus on and accurately respond to incidents that matter. It provides extended detection and response for customers who use the following Microsoft Defender XDR services: Microsoft Defender for Endpoint, Microsoft Defender for Microsoft 365, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, and Microsoft Entra ID.

Microsoft Defender for Cloud: Microsoft Defender for Cloud 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.

Microsoft Defender Threat Intelligence: Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence. Defender TI enables security professionals to focus on what actually helps their organization defend themselves, deriving insights about the actors through analysis and correlation instead of spending time on the data discovery, collection, and parsing of data.

Microsoft Sentinel: Microsoft 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. Microsoft 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.

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.

Windows Autopatch: Windows Autopatch is a cloud service that automates Windows, Microsoft 365 Apps for Enterprise, Microsoft Edge, and Microsoft Teams updates to improve security and productivity across a customer's organization.

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 Fluid Relay: Azure Fluid Relay is a managed offering for the Fluid Framework that helps developers build real-time collaborative experiences and replicate state across connected JavaScript clients in real-time. The Fluid Framework is a collection of client libraries for distributing and synchronizing shared state.

Azure Maps: Azure Maps is a collection of geospatial services and SDKs that use fresh mapping data to provide geographic context to web and mobile applications. Azure Maps enables features such as map drawing, routing, search, time zones and traffic. The APIs can be subscribed to by customers in the Azure Portal or ARM.

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.

Azure Spring Apps: Azure Spring Apps service makes it easy to deploy Spring Boot-based microservice applications to Azure with zero code changes. It manages the infrastructure of Spring Cloud applications, so developers can focus on their code. It provides lifecycle management using comprehensive monitoring and diagnostics, configuration management, service discovery, CI/CD integration, blue-green deployments, and more.

Azure Web PubSub: The Azure Web PubSub service helps customers build real-time messaging web applications using WebSockets and the publish-subscribe pattern easily. This real-time functionality allows publishing content updates between server and connected clients (for example a single page web application or mobile application).

Mixed Reality

Remote Rendering: Remote Rendering enables customers to render high quality interactive 3D content in the cloud and stream it in real-time to devices running on the edge.

Spatial Anchors: Spatial Anchors helps customers create spatially aware mixed reality experiences across iOS, Android, and HoloLens devices. Customers can use this cross-platform service to unlock mixed reality capabilities like wayfinding, and enhance collaboration in facilities management, training, gaming, and other scenarios.

Hybrid + Multicloud

Azure Arc enabled System Center Virtual Machine Manager: Azure Arc enabled System Center Virtual Machine Manager allows on-premises System Center Virtual Machine Manager (SCVMM) customers to connect their SCVMM environment to Azure and perform VM self-service operations from the Azure portal. Additionally, customers can manage, monitor, and govern machines running on-premises from Azure through Arc.

Azure Arc enabled VMware vSphere: Azure Arc enabled VMware vSphere performs full lifecycle management on VMware VMs and uses Azure RBAC to provision and manage VMs on demand in the Azure portal. It performs access governance, monitoring, update management, and security at scale for VMware VMs from customer datacenters or by using Azure VMware Solution, Kubernetes clusters, and VMware Tanzu Application Service.

Azure Center for SAP Solutions: Azure Center for SAP solutions is an Azure offering that makes SAP a top-level workload on Azure. Azure Center for SAP solutions is an end-to-end solution that enables customers to create and run SAP systems as a unified workload on Azure and provides a more seamless foundation for innovation. Customers can take advantage of the management capabilities for both new and existing Azure-based SAP systems.

Azure Kubernetes Service on Azure Stack HCI: Azure Kubernetes on Azure Stack HCI (hyperconverged infrastructure) uses Azure Arc to create new Kubernetes clusters on Azure Stack HCI directly from Azure. It enables customers to use familiar tools like Azure portal, Azure CLI (Command Line Interface), and Azure Resource Manager templates to create and manage their Kubernetes clusters running on Azure Stack HCI. Since clusters are automatically connected to Arc when they are created, customers can use their Microsoft Entra ID for connecting to their clusters from anywhere. This ensures developers and application operators to provision and configure Kubernetes clusters in accordance with company policies.

Azure Operator Nexus: Azure Operator Nexus is a carrier-grade hybrid cloud platform built for mission-critical mobile network applications. It helps customers simplify provisioning of new network services, optimize deployment of network functions and applications on-premises, and run network-intensive workloads and mission-critical applications with resiliency, security, observability, and high performance.

Azure Operator Service Manager: Azure Operator Service Manager is a cloud orchestration service designed to simplify management of complex edge network services hosted on the Azure Operator Nexus platform. It provides customers with persona-based capabilities to onboard, compose, deploy and update multi-vendor applications across one-to-many Azure sites and regions.

Azure Monitor for SAP Solutions: Azure Monitor for SAP solutions is an Azure-native monitoring product that enables customers to monitor availability, performance, and operation of SAP systems running on Azure.

Internal Supporting Services[10]

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., Microsoft 365 and Dynamics 365.

Access Monitoring: Access Monitoring (AM) evaluates permissions throughout the infrastructure to report on effective access across Cloud + AI. AM drives reporting in the quarterly User Access Review and several KPIs inside the division.

AIP Masters: AIP Masters is a data processing pipeline that produces two business intelligence data sets (Azure Usage and Customer Catalog) used by other Azure services. The Azure Usage data set includes consumption data of Azure services by Azure customers at the subscription and meter level and the Customer Catalog dataset contains non-PII customer metadata and identifiers associated with Azure subscriptions.

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.

Atlas: Atlas (formerly OneIdentity) is used for managing user accounts and security groups in different domains.

Autopilot Security: Autopilot Security manages major parts of the security of the Azure core control plane, such as Certificate management and rollover, as well as the management of encryption and decryption keys. These services are related to Autopilot and Pilotfish systems that the rest of the Azure stack depends on.

AzCP Platform: AzCP Platform is a set of Service Fabric (SF) applications that install a SF cluster with a declarative deployment model paired with a collection of microservices to fill in gaps in the out-of-the-box support for common application needs within the Azure Control Plane.

Azure Marketplace Portal: Azure Marketplace Portal is the new marketplace for Azure applications. It is an online store for thousands of certified, open source, and community software applications, developer services, and data pre-configured for Azure.

Azure Code Scanning: Azure Code Scanning offers anti-malware scanning service for Azure service teams and services to protect against malware. Azure Code Scanning uses multiple anti-malware scanning engines to detect malware and Potentially Unwanted Programs (PUP).

Azure Diagnostic Services: Azure Diagnostic Services helps Azure customers and Support engineers to troubleshoot customer issues and identify root cause and recovery actions.

Azure Notebooks Component: Azure Notebooks Component is an internal service that allows Microsoft teams to embed a component that provides a Jupyter notebook canvas allowing teams to add themes, languages, etc. to their applications.

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 Health: Azure Service Health is a suite of experiences that provide personalized guidance and support when issues in Azure services are affecting or may affect customers in the future.

Azure Service Manager (RDFE)[8]: 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 SMAPI. All requests from the user go through Azure Service Manager (RDFE) or the newer ARM.

Azure Singularity[13]: Azure Singularity is a managed High Performance Computing infrastructure service that provides highly reliable, low-cost infrastructure for AI training and inferencing. It provides lowest cost AI training and inferencing by driving high utilization via Secure, fine-grained multi-tenancy of 1P and 3P tenants; multiplexing of inferencing and training workloads; and Azure-wide, topology and workload-aware scheduling. It ensures high reliability through transparent and consistent checkpoint/restore, live migration, and elasticity, and global distribution of inferencing endpoints for single digit millisecond latencies and high availability. It

[13] Examination period for this offering / service was from October 1, 2023 to March 31, 2024.

supports integration for both 1P and 3P hardware; and pluggable data-planes and cluster schedulers.

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 Diagnostics and Analytics Service[14]**:** Azure Stack Diagnostics and Analytics Service enables Azure Stack devices to upload telemetry and ingest the data into Kusto for edge observability.

Azure Stack Edge Service: 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 Support Center: Azure Support Center provides tools for the internal technical support team to diagnose and resolve support requests from Azure customers.

Azure System Lockdown: Azure System Lockdown is a feature within Azure Security Pack which monitors and audits applications running on other services in the execution environment.

Azure Throttling Solutions: Azure Throttling Solutions builds standardized throttling solutions for Microsoft Cloud Services. It partners with the Azure office of the Chief Technology Officer (CTO) (AOCTO) to deliver throttling solutions that best serve first-party Microsoft rate-limiting needs.

Azure Usage Billing: Azure Usage Billing (AUB or Oro) is the central service which enables collection and processing of billing usage across Azure. It is an analytics service designed to help customers analyze and process streams of billing and usage data that can be used to get insights, build reports or trigger alerts and actions.

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

Blueshift Analytics: Blueshift Analytics is a Big Data service for internal Microsoft allowing them to run large scale batch jobs on data stored in Azure Data Lake Store Gen2.

Cloudfit: Cloudfit is a service that provides machine utilization analysis and recommendations to improve cost of goods sold (COGS) for all Microsoft services.

CloudMine: CloudMine is a data pipeline and data store for engineering artifacts such as work items, builds, commit, or source code. It serves data spanning multiple systems, organizations, and years of history in a single data store, allowing users to query engineering data across the Microsoft enterprise.

CO+IE-Hardware Inventory: Cloud Operations and Innovation Engineering (CO+IE) Hardware Inventory provides users with information on metadata of physical assets in Cloud Operations and Innovation (CO+I) data centers.

Copilot Applied AI: Copilot Applied AI (formerly Dynamics 365 Insights Apps AI and B360 AI Platform) provides internal AI services to products built by other teams within Dynamics 365 Insights Apps (formerly Business 360). The Dynamics 365 Insights Apps AI service leverages Microsoft data sources (Search Logs, Browser Logs) and other 1st and 3rd party data to enrich consumer profiles (B2C).

[14] Examination period for this offering / service was from April 1, 2024 to September 30, 2024.

CoreWAN: CoreWAN is used to connect all Microsoft products worldwide to the Internet. It is composed of software, firmware, hardware devices, physical sites around the world, and terrestrial fiber optic cables, submarine fiber optic cables, and leased circuits from carriers.

CSCP-ReferenceSystems: CSCP Reference Systems enable the automation of capacity planning, management and execution with a set of data and services that are the "central source of truth" for Master Data with continuous validation of accuracy, freshness and completeness.

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.

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.

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.

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

Dynamics 365 Office Integration: Dynamics 365 Office Integration is used to capture Document Management using SharePoint, OneDrive for Business document recommendations, and OneNote Export to Excel within Dynamics CRM.

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

Environmental Sustainability Green SKU - Data Platform: Environmental Sustainability Green SKU - Data Platform provides science-based calculations for carbon emission computation for the Emission Impact Dashboard and Carbon platform.

Exotic & Private Cloud - Resource Providers: Exotic & Private Cloud - Resource Providers is an Azure Specialized resource provider, billing and validation service focused on baremetal networking scenarios. The service builds on existing Azure infrastructure and Azure Networking stack to enable workloads with external partners into Azure Cloud.

ExP - Managed: ExP - Managed Service is an A/B testing platform which provides Microsoft teams with a tool to easily run A/B experiments.

ExP Treatment Assignment Service: ExP Treatment Assignment service provides HTTP REST endpoints for customers to retrieve configuration for A/B testing and exposure control. This includes variants (flights), feature flags (treatment variables), assignment context and the experimentation blob.

Fabric Controller Fundamental Services: Fabric Controller Fundamental Services, earlier known as 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 their lifecycle. Subcomponents include the Service Manager (SM / Aztec), Tenant Manager, Container Manager and Allocator.

Fabric Network Devices: Fabric Network Devices is used to provide all datacenter connectivity for Azure. Fabric Network Devices is completely transparent to Azure customers who cannot interact directly with any physical network device. The Fabric Network Devices 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 Fabric Network Devices 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.

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 Microsoft 365.

Gateway Manager: Gateway Manager is a control plane for VPN, ExpressRoute, Application Gateway, Azure Firewall, and Bastion. It is a critical component in Hybrid Azure Networking.

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 Analytics Orchestration: The Geneva Analytics Platform (Cloud Analytics Service) includes Data Studio, the Geneva Catalog, Geneva Job Scheduler, Geneva Collector and satellite micro-services. The Geneva Analytics Platform provides tools for Data Discovery, Data Transformations and Data Movement to internal Microsoft Teams. It integrates with other Azure Cloud Engineering Systems: The Geneva Pipeline, IcM, Geneva Health, etc.

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

Groups and Experimentation (OSG): Groups and Experimentation (OSG) Supports assignment of users and devices into groups for experimentation and targeting for scenarios such as OS build flighting, Storefront UX experiments, and DevCenter app Betas.

Holmes Service: Holmes service provides resource management and controls to trigger and influence actions on resources. Holmes is agnostic to specific types of service-model, & type of inventory, and tries to optimize packing, reshape clusters, apply required policies, and tools for various scenarios.

IcM Incident Management Service: IcM is a unified incident management system for all Microsoft services and provides tools for managing live site and on call rotations across the world.

Interflow: Interflow is a threat intelligence exchange service. It collects threat data (botnet IPs, hashes of malicious files, etc.) from various Microsoft teams and from various third parties, and then shares that data back out to Microsoft teams so they can act on it in their own products and services.

JIT: Just In Time (JIT) access provides engineers temporary elevated access to production services when needed to perform servicing activities and support their services.

LENS APLU[14]: APLU (Account Profile Look Up) aims to improve CELA's response time to law enforcement requests. It consolidates the information gathering process and replaces multiple tools with a single efficient API. CELA users can use CRM to submit requests to APLU, which then retrieves information from various E+D services and the processed information is then delivered back to the CST Portal, streamlining the overall response process for CELA.

Lens Explorer: Lens Explorer is part of the Geneva Analytics offering. It allows users to quickly drill down into customer's data and build dashboards that tell them a story.

M365D Automated IR: MM365D Automated IR is a service that holds the logic for automated remediation of threats related to malicious or suspicious activity for customers using Microsoft Defender XDR (Extended Detection and Response).

M365D Investigation and Exploration: M365D Investigation and Exploration service is a web portal through which subscribers of M365D service can consume Threat Intelligence and the results of processed cyber event data including indications of attack, indications of compromise, etc.

M365D Management Service: M365D Management Service is a service which registers customers for the Microsoft Defender 365 service and allows them to onboard their organization's machines.

MDM: MDM (Multi-Dimensional-Metrics) is the component within Geneva Monitoring responsible for collection and aggregation of metrics, performing alerting and visualizing health information.

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.

Microsoft Bot Framework: Microsoft Bot Framework represents the offline tools, SDKs, CLIs, etc. that support the Azure AI Bot Service offering.

Microsoft Emissions Impact Dashboard: The Emissions Impact Dashboard helps Microsoft cloud customers understand, track, report, analyze, and reduce carbon emissions associated with their cloud usage.

Microsoft Email Orchestrator: Microsoft Email Orchestrator (formerly called Azure Email Orchestrator) is an internal service for managing email content and for sending email communications to customers across Microsoft.

MSaaS File Management (DTM V2): MSaaS File Management is required to exchange files between customers, CSS, and Agents.

MSFT.RR DNS: MSFT.RR DNS is the Microsoft internal Recursive DNS for internal consumption.

Network Billing: Network Billing service provides a reliable pipeline with low-latency for services in Azure Networking.

On-Premises Data Gateway: On-Premises Data Gateway provides connectivity to on-premises resources for Power BI, Power Apps, and LogicApps services.

OneBranch Release: OneBranch Release is the release manager for services to deploy to all clouds in a secure and compliant manner.

OneDeploy Deployment Infrastructure (DE): OneDeploy Development Infrastructure is an Azure Deployment Engine (DE) custom workflow execution for Azure Foundational / Core services.

OneDS Collector: OneDS Collector is the ingestion front end for the telemetry pipelines used by Microsoft Windows, Microsoft 365 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.

OneSettings: OneSettings service provides a command and control surface for numerous clients in the ecosystem. Primarily utilized to control the rate of Telemetry events collected by the Universal Telemetry Client (UTC) powering scenarios like Diagnostics, Experimentation and configuration.

PF-FC: PilotFish Fabric Controller (PF-FC) is the PilotFish hosted environment for managing the underlying hardware and services related to the Azure Fabric Controller. This includes buildout and management of the environments in PF, health of the nodes, FC role management and startup.

Pilotfish: Pilotfish is available to first-party customers (e.g., Microsoft 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.

PMI Foundation[14]: PMI Foundation provides customers with a hardened, trusted platform that is standardized and scalable to support baremetal identity services.

Resource Provider Service as a Service: Resource Provider Service as a Service is a platform for Microsoft teams to develop their resource providers internally. It hosts first/third party resource providers such as Oracle.

Service Tree: Service Tree enables Microsoft employees to model organizations, software, and offerings as a single system of record with associated metadata and resources. This service maintains an auditable and up-to-date directory of software, processes, and metadata to enable security, compliance, reliability, and automation.

SIPS ML Detections 2: SIPS ML Detections 2 service analyzes Azure logs to detect potential attacks compromises, such as account compromise, data breach, web attacks, compromised hosts, against Azure and Azure customers.

SQL Business Analytics: SQL Business Analytics is an internal tool that allows Azure SQL engineers to leverage service telemetry to aggregate data to generate reports identifying the usage, growth, and other business critical trends for Azure SQL and Open source database (OSS database) produ.

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

Unified Remote Scanning (URSA): Unified Remote Scanning (URSA) provides a unified and standardized platform for remote security scans across Azure.

Vulnerability Scanning & Analytics: Vulnerability Scanning & Analytics is a service that provides vulnerability management and analytics for physical / virtual machines in cloud environments.

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 (hop-box) 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 Microsoft 365 SharePoint Online service.

Microsoft Online Services

Appsource: Appsource is an enterprise app marketplace which integrates with other major Microsoft platforms including Dynamics and Microsoft 365 to allow an easy click-try-buy process.

Dynamics 365 Customer Voice: Dynamics 365 Customer Voice is a simple yet comprehensive survey solution that builds on the current survey-creation experience of Microsoft Forms in Microsoft 365. It offers new capabilities that make capturing and analyzing customer and employee feedback simpler than ever. Customers can respond to the surveys by using any web browser or mobile device. As responses are submitted, Power BI reports can be used to analyze them and make decisions in real time.

Endpoint Attack Notifications: Endpoint Attack Notifications 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.

Intelligent Recommendations: Intelligent Recommendations enables businesses to automate relevant recommendations, including personalized results for new and returning users, and the ability to interpret both user interactions and item or user metadata. In return, businesses receive tailored recommendations models based on their needs and business logic. Intelligent Recommendations frees companies from the tedious management of editorial collections. Instead, it helps drive engagement, run experiments, and build trust with consumers.

Microsoft Copilot Studio: Microsoft Copilot Studio 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 Defender for Cloud Apps: Microsoft Defender for Cloud Apps 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. Microsoft Defender for Cloud Apps provides Shadow IT discovery, information protection to cloud applications, threat detection and in-session controls.

Microsoft Defender for Endpoint: Microsoft Defender for Endpoint is unified platform for preventative protection, post-breach detection, automated investigation, and response. Microsoft Defender for Endpoint protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture.

Microsoft Defender for Identity: Microsoft Defender for Identity 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.

Microsoft Graph: Microsoft Graph exposes multiple APIs from Microsoft 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 Microsoft Entra ID, Exchange Online as part of Microsoft 365, SharePoint, OneDrive, OneNote, and Planner.

- Navigate between entities and relationships.
- Access intelligence and insights from the Microsoft cloud (for commercial users).

Microsoft Intune: Microsoft Intune 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 Managed Desktop: Microsoft Managed Desktop combines Microsoft 365 Enterprise with an IT-as-a-Service 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 Azure AI 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.

Nomination Portal: Nomination Portal is an optimized customer relation management solution for Azure On-boarding and Nomination to Engagement Customer Lifecycle. It provides increased transparency on Azure services offered and what the customer is taking to production, a clearer idea of where IPs are needed with improved assignment and activity redecoration, as well as capturing effort towards customer engagements.

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 resource provider (RP) is an ARM RP, 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.

Windows Update for Business reports: Windows Update for Business reports is a cloud-based solution that provides information about the customer's Microsoft Entra ID-joined devices' compliance with Windows updates. Windows Update for Business reports is offered through the Azure portal, and it's included as part of the Windows 10 or Windows 11 prerequisite licenses. Windows Update for Business reports helps customers monitor security, quality, driver, and feature updates for Windows 11 and Windows 10 devices, report on devices with update compliance issues, and analyze and display the customer's data in multiple ways.

Microsoft Dynamics 365

Chat for Dynamics 365: Chat for Dynamics 365 is one of the primary channels for customers to interact with support agents because of its simplicity and ease of use. Customer service centers prefer customers to connect via Chat for Dynamics 365 because it allows service agents to be more productive by simultaneously engaging with multiple customers.

Dataverse: Dataverse securely stores and manages data that is used by business applications. Data within Dataverse is stored within a set of entities (An entity is a set of records used to store data, similar to how a table stores data within a database). Dataverse includes a base set of standard entities that cover typical scenarios, but also lets the customer create custom entities specific to their organization and populate them with data using Power Query. App makers can then use Power Apps to build rich applications using this data.

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 Athena - CDS to Azure Data Lake: Export to Data Lake (Athena) is a pipeline to continuously export data from the Dataverse to Azure Data Lake Gen2. It is designed for enterprise big data analytics, is cost-effective, scalable, has high availability / disaster recover capabilities and enables best in class analytics performance. Data is stored in the Common Data Model format which provides semantic consistency across apps and deployments. The standardized metadata and self-describing data in an Azure Data Lake Gen2 facilitates metadata discovery and interoperability between data producers and consumers such as Power BI, Azure Data Factory, Azure Databricks, and Azure Machine Learning service.

Dynamics 365 Business Central: Dynamics 365 Business Central, formerly known as Dynamics NAV, is Microsoft's Small and Medium Business 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 Contact Center: Dynamics 365 Contact Center is a Copilot-first contact center solution that works with existing customer relationship management systems (CRMs). It supports contact centers by providing channels of communication, self-service functions, intelligent routing and agent-assisted services.

Dynamics 365 Customer Insights - Data: Dynamics 365 Customer Insights - Data (formerly Dynamics 365 Customer Insights Engagement insights) enables customers to understand interactively how their customers are using their services and products - both individually and holistically - on websites, mobile apps, and connected products. Customers can combine behavioral analytics with transactional, demographic, survey, and other data types from Dynamics 365 Customer Insights.

Dynamics 365 Customer Insights - Journeys: Dynamics 365 Customer Insights - Journeys (formerly Dynamics 365 Marketing) is a marketing-automation application that helps customers turn prospects into business relationships. Dynamics 365 Customer Insights - Journeys 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 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 Guides: Dynamics 365 Guides is a mixed-reality application for Microsoft HoloLens that lets operators learn, during the flow of work by providing holographic instructions when and where they are needed. These instruction cards are visually tethered to the place where the work must be done, and can include images, videos, and 3D holographic models. Operators see what must be done, and where. Therefore, they can get the job done faster, with fewer errors and greater skill retention.

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 Intelligent Order Management: Dynamics 365 Intelligent Order Management enables customers to manage the orchestration of orders through to fulfillment helping organizations orchestrate order flows across different platforms and apps. Intelligent Order Management is designed to operate in complex environments where there are many internal and external systems and partners that enable the supply chain processes. The platform is designed to scale up and down with a business, regardless of the organization size.

Dynamics 365 Project Operations: Dynamics 365 Project Operations connects sales, resourcing, project management, and finance teams in a single application to win more deals, accelerate project delivery, and maximize profitability.

Dynamics 365 Remote Assist: Dynamics 365 Remote Assist enables customers to collaborate more efficiently by working together from different locations on HoloLens, HoloLens 2, Android, or iOS devices.

Dynamics 365 Resource Scheduling Optimization: Dynamics 365 Resource Scheduling Optimization is an Add-in for Dynamics 365 Field Service that automatically schedules jobs to the resources that are best equipped to complete them. For example, Resource Scheduling Optimization can schedule work orders for field technicians

or cases for customer service reps. While the schedule board and the schedule assistant help schedule a single job, this add-in can schedule multiple jobs at once. It maximizes resource use and minimizes travel time.

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.

Dynamics 365 Sales Insights: Dynamics 365 Sales Insights empowers sellers to deliver personalized engagement and build profitable relationships. Capabilities include supercharging sales with a prioritized list of everything that needs to be done and optimizing the sales cadence for different types of prospects with sequences.

Microsoft Power Platform on Azure: Microsoft Power Platform on Azure services are enabled in Dynamics 365 Relevance Search (RS) by default. Microsoft Power Platform on Azure provides additional backend features to improve Dynamics 365 Relevance Search. These features include natural language search with Intent understanding, knowledge-based query annotation, semantic parsing to create structured queries, spell checking, query rewriting to normalize synonyms and abbreviations, and world common knowledge to understand location, date, time, holiday, and popular organizations. Additional features include multi-level ranking and a customer feedback loop which consumes user clicks to train and improve the rankers.

Nuance Conversational IVR: Nuance Conversational IVR is a Microsoft first party multi-tenant SaaS platform that provides an enterprise-grade robust interactive voice response (IVR) service. It integrates with telephony and contact center systems to provide callers natural, human-like self-service interactions and advanced IVR capabilities by utilizing the latest Microsoft and Nuance Conversational AI technologies.

Power Pages: Power Pages is a secure, enterprise-grade, low-code software as a service (SaaS) platform for creating, hosting, and administering modern external-facing business websites. Power Pages empowers customers to rapidly design, configure, and publish websites that work across web browsers and devices.

Additionally, Dynamics 365 Life Cycle Services and Power Platform Admin Center are underlying features across multiple Dynamics 365 offerings. Dynamics 365 Life Cycle Services is a collaboration portal that provides an environment and a set of regularly updated services that can help customers manage the application lifecycle of their implementations of finance and operations apps. The Power Platform Admin Center provides a unified portal for administrators to manage environments and settings for Power Apps, Power Automate, and customer engagement apps.

Microsoft Cloud for Financial Services

Microsoft Cloud for Financial Services: Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft's partners and customers to extend the value of the platform with additional solutions to address the financial industry's most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value. Microsoft Cloud for Financial Services and its capabilities (Unified Customer Profile, Customer Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Microsoft 365 related offerings are not in the scope of this examination.

Unified Customer Profile: Unified Customer Profile helps banks tailor their customer experiences via a 360-degree view of the customer and, bringing together financial, behavioral, and demographic data.

Customer Onboarding: Customer Onboarding provides customers with easy access loan apps and self-service tools, helping to streamline the loan process to enhance customer experience and loyalty while increasing organizational and employee productivity. Helps customers efficiently apply for and keep track of a loan by streamlining the application process. Additionally, it empowers loan officers to manage loan applications with workflow automation, streamlining and customizing operations to meet specific lending needs.

Collaboration Manager: Collaboration Manager helps banks bring collaboration seamlessly into their lending workflows enabling them to improve process orchestration from front office to back office and facilitate omnichannel communications with customers. This capability helps banks improve organization and employee productivity, unlock value creation, and enhance customer experience. The portions of this capability covered by Microsoft 365 are not in scope for this examination.

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. **Feedback** is data provided as part of a review or feedback for one of Microsoft's products and services that includes personal data.
6. **Account Data** is information about payment instruments. This type of data is not stored in the Azure platform.
7. **Public Personal Data** is publicly available personal information that Microsoft obtains from external sources.
8. **End User Pseudonymous Identifiers (EUPI)** are identifiers created by Microsoft, tied to the user of a Microsoft service.
9. **Managed Service Data** is all data provided to Microsoft by the Managed Service customer and / or the Managed Service personnel as part of a Managed Service engagement.
10. **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.
11. **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.
12. **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 4: Principal Service Commitments and System Requirements

Section 4: Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers, business partners and vendors, 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, Product 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 including the following:

- 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 are documented on how to carry out specific manual and automated processes required in the operation and development of various Azure services and offerings.
- Procedures are in place so that the access, collection, use, and deletion of customer data is in accordance with the service commitments.
- Cryptographic controls are implemented to protect customer data. Access to cryptographic keys is restricted to only authorized personnel.
- Policies and instructions for controlling and monitoring third parties (e.g. service providers or suppliers) whose services contribute to the provision of the cloud service are documented and communicated.
- Azure services are designed to maintain high availability through redundancy and automatic failover to minimize disruption to services.
- Critical systems are monitored through third-party and internal tools to maintain availability.

- Access to physical and logical assets is limited to authorized users and is provisioned based on job requirements to mitigate risk of unauthorized access.
- Automated logging and alerting capabilities are implemented for Azure services to detect potential unauthorized activity and security events.
- Incidents impacting internal and customer systems are detected, escalated and resolved.
- Development of new features and major changes to Azure services are performed in accordance with policies and procedures.
- Azure offerings and services are configured be interoperable with industry standards.

Such requirements are communicated in Azure's system policies and procedures, system design documentation, and contracts with customers. Microsoft's service commitments and system requirements are designed based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality, and other frameworks.