Deployment, Security, and Cloud Management

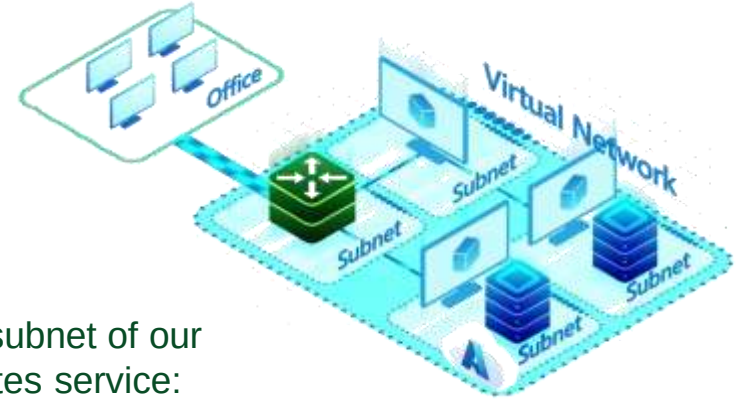
DSBA 6190-U90 | Colby T. Ford, Ph.D.

Deploying Azure Resources

- Basics of Networking
- Infrastructure as Code
  - ARMs and Biceps
  - Terraform
- GitHub Actions / DevOps Build Pipelines

Networking

Virtual Networks and Subnets

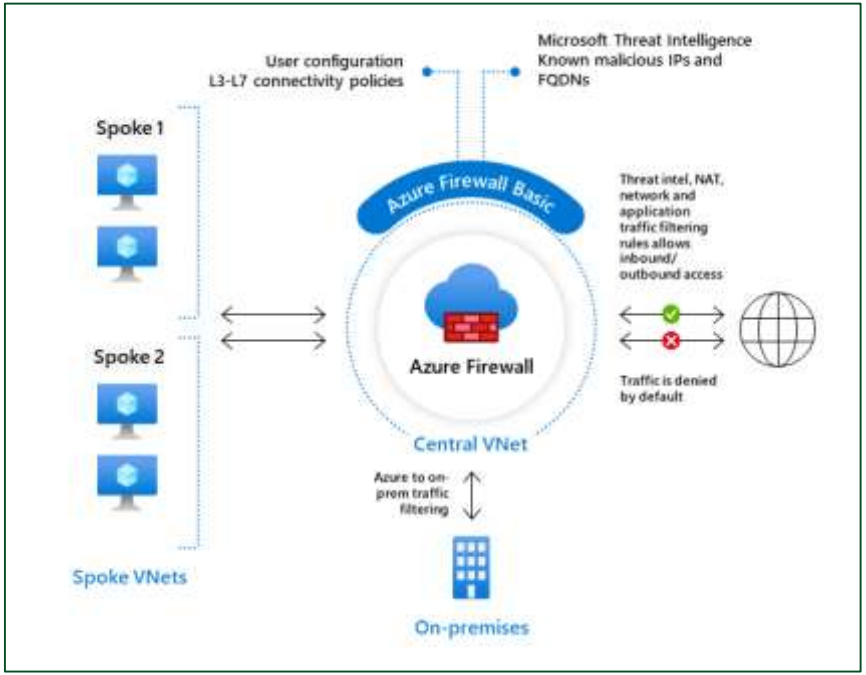


- Virtual networks, like real networks, control the communication between cloud services, the internet, and on-prem resources
- Other features:
  - Control and filter internet vs. internal routing
  - DDoS protection
  - Network Peering
- Subnets relate to a specific service, giving an address space to each (CIDR block)

Example: the subnet of our class Kubernetes service:

Subnet ID	/subscriptions/e9bc187a-e9a1-46be-822e-e955a2563601/resourceG
Subnet purpose ⓘ	Default
Name * ⓘ	aks-subnet
IPv4	
Include an IPv4 address space	☑
Choose a starting address and size within your IPv4 address range: 10.224.0.0/12 (10.224.0.0 - 10.239.255.255)	
Starting address * ⓘ	10.224.0.0
Size ⓘ	/16 (65,536 addresses)
Subnet address range ⓘ	10.224.0.0 - 10.224.255.255

Firewalls and Private Endpoints



Firewalls:

- Firewalls all you to communicate with multiple networks (including virtual networks) and control access (certain IPs, ports, etc.)
- Also, it provides some enhanced threat detection, and traffic filtering, etc.

Private Endpoints:

- Normally, Azure services have a public endpoint (a public URL where you can access the service from the open internet). For security reasons, you can make an endpoint for certain services as part of your vnet.

Infrastructure-as-Code

Deployment is ~~Easy~~ Necessary

- “Infrastructure as Code” – The ability to deploy all your services in the cloud from code rather than manually.
- Important for:
  - IT management of resources
  - Geo-replication / Global availability and scale
  - Security
  - Promotion of infrastructure changes from:

    development → staging → production

Infrastructure as Code Options

ARM Templates

Pro: Azure can generate them.

Con: Difficult to read and edit.

Templates overview - Azure Resource Manager | Microsoft Docs

Bicep Language

Pro: From Microsoft. Easy to read.

Con: Lacking in examples and docs.

Bicep language for deploying Azure resources - Azure Resource Manager | Microsoft Docs

Terraform

Pro: From HashiCorp. Multicloud.

Con: Proprietary and Pricey

Docs overview | hashicorp/azurerm | Terraform Registry

IaC Language Learning Curve

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-
04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "location": {
      "type": "string",
      "defaultValue": "[resourceGroup().location]"
    },
    "storageAccountName": {
      "type": "string",
      "defaultValue": "[format(myStorage{0}',
uniqueString(resourceGroup().id))]"
    }
  },
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2021-06-01",
      "name": "[parameters('storageAccountName')]",
      "location": "[parameters('location')]",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "StorageV2",
      "properties": {
        "accessTier": "Hot"
      }
    }
  ]
}
```

ARM (JSON)

```
param location string = resourceGroup().location
param storageAccountName string =
myStorage${uniqueString(resourceGroup().id)}'

resource storageAccount
'Microsoft.Storage/storageAccounts@2021-06-01' = {
  name: storageAccountName
  location: location
  sku: {
    name: 'Standard_LRS'
  }
  kind: 'StorageV2'
  properties: {
    accessTier: 'Hot'
  }
}
```

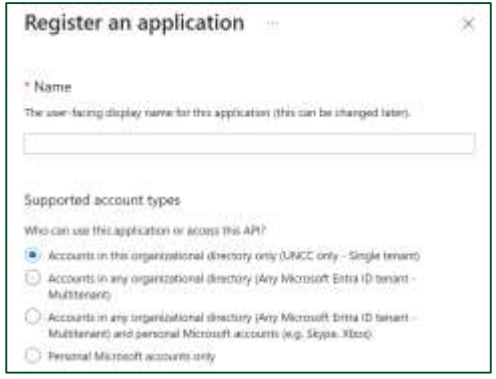
BICEP

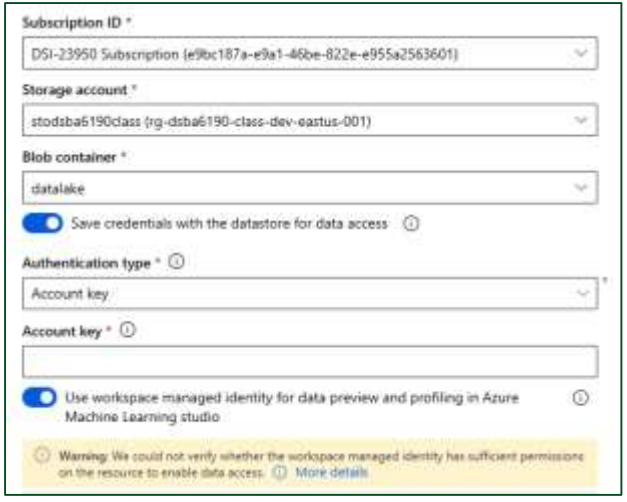
```
resource "azurerm_storage_account" "mystorage" {
name = "myStorage${random_integer.id.result}"
resource_group_name = azurerm_resource_group.rg.name
location = azurerm_resource_group.rg.location
account_tier = "Standard"
account_replication_type = "LRS"
tags = { environment = ”dev" }
}
```

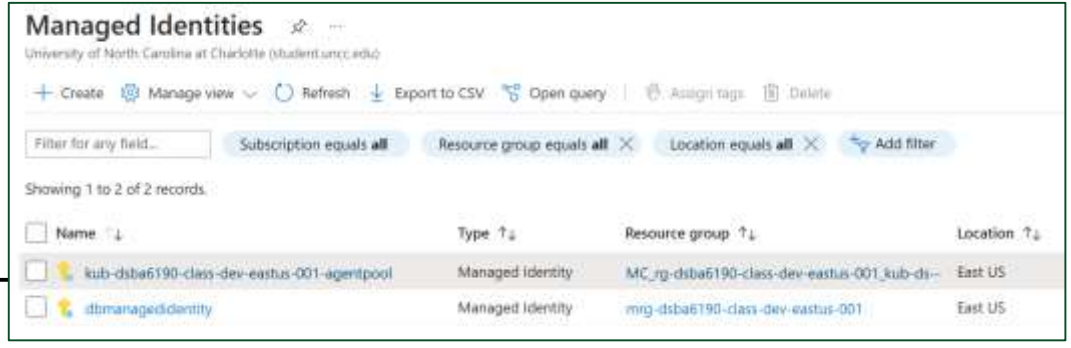
TF (HCL)

Service Principals and Managed Identities

- Service Principals are like user accounts, but for services.
  - “Azure-representation of a non-Azure object”
  - Usually assigned for a specific application or purpose.
- Managed Identities are a type of Service Principal that operates on behalf of other services (usually other Azure resources)
  - System-assigned managed identities share a lifecycle with various Azure services
- Both can be given roles and permissions like users.

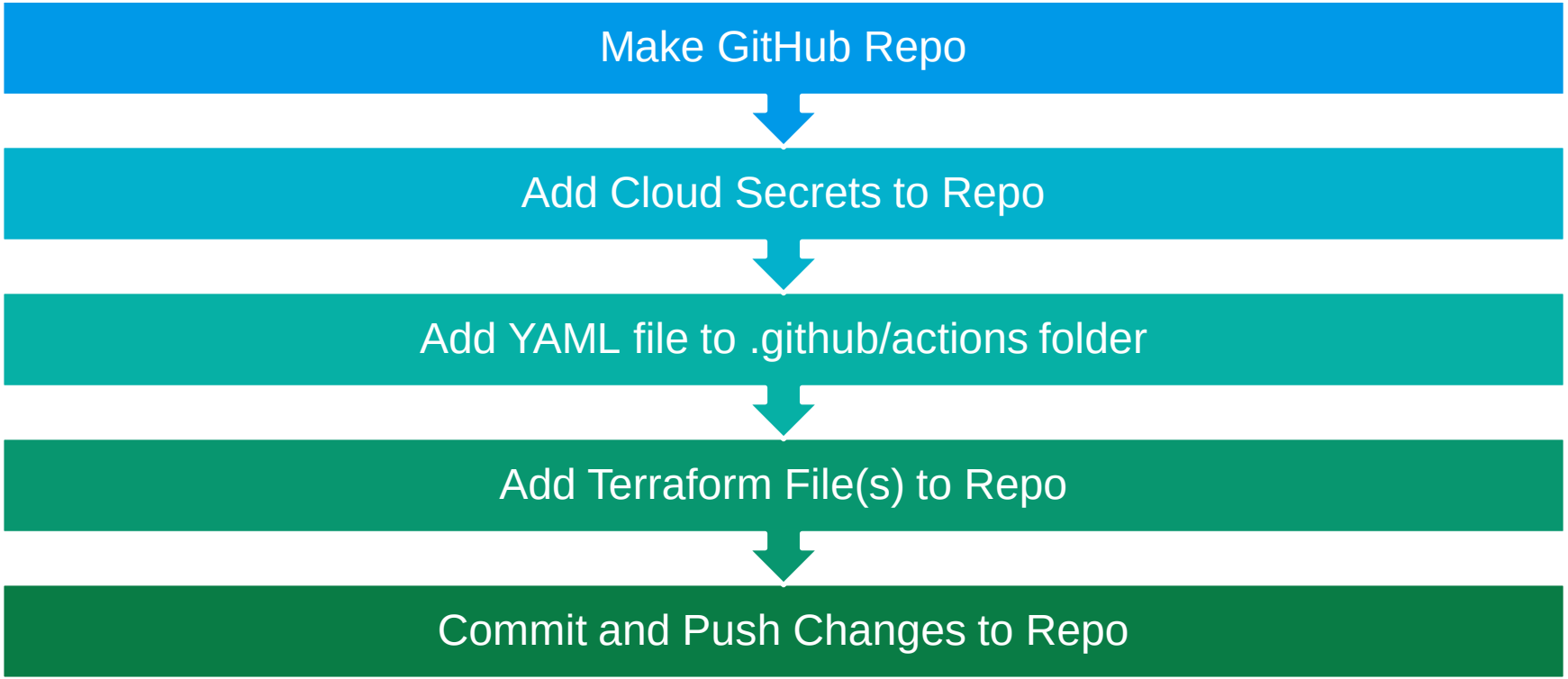






Deploying with GitHub Actions

Steps to Deploy with Terraform in GitHub Actions

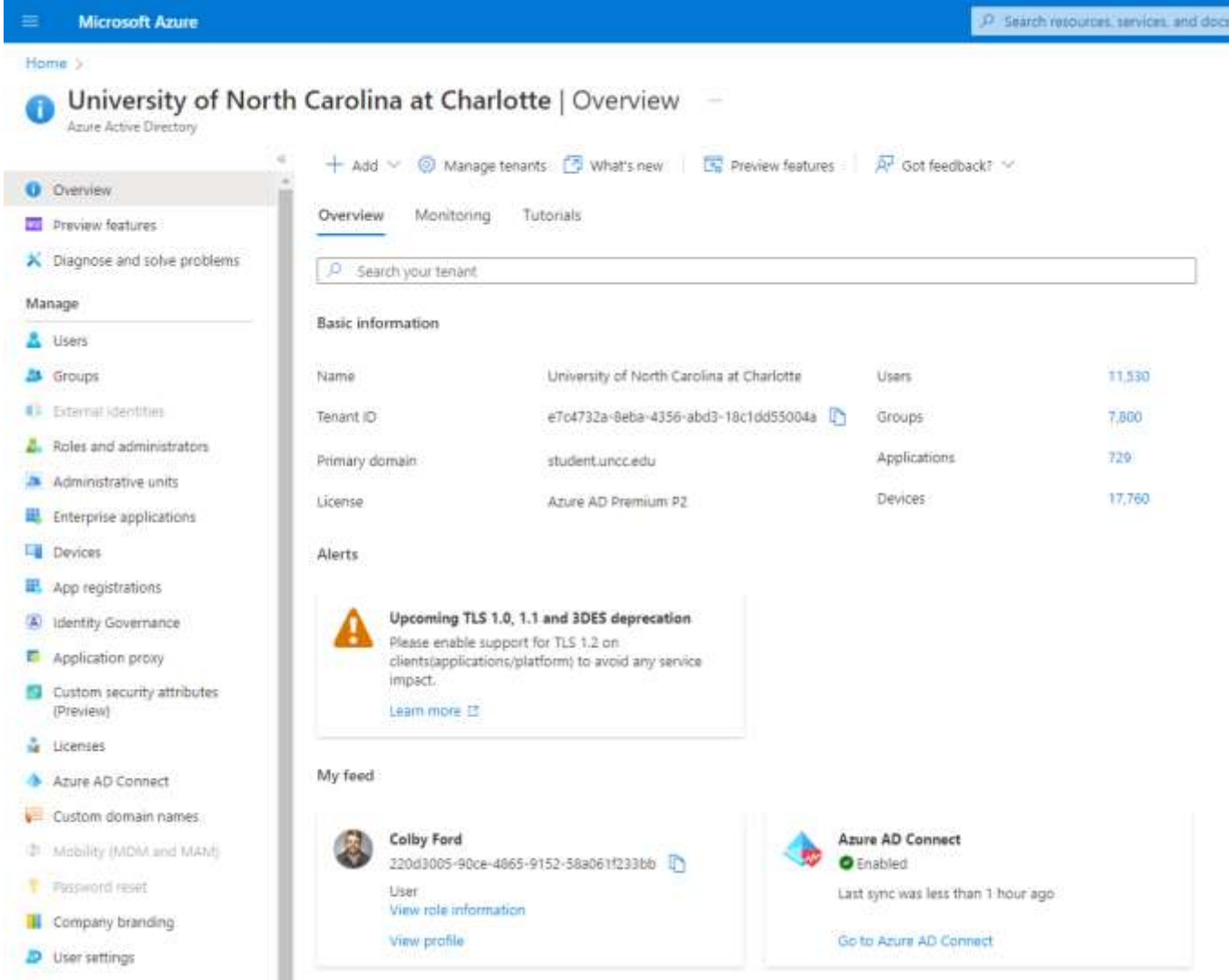


Security, Compliance, and Data Governance

- Role-Based Access Controls
  - Azure Active Directory
  - Access Control Lists in Azure Storage
- Compliance
  - HIPAA, HITRUST, SOX, ISO
  - Defender for Cloud
  - Blueprints, etc.
- And more...
  - Data Governance: Azure Purview
  - Azure Chaos Studio
  - Subscriptions

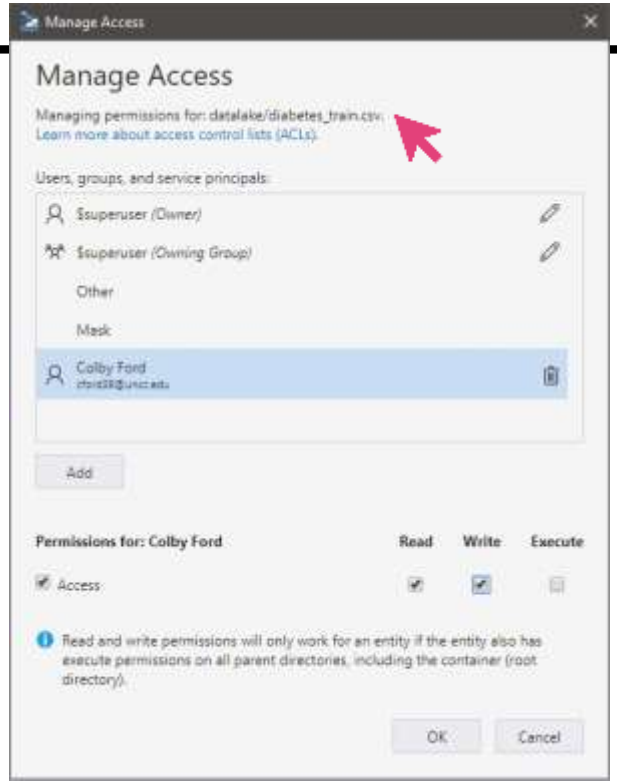
Azure Active Directory (Entra ID)

- Identity management for users and applications.
  - Single Sign-On (SSO)
  - App registrations
    - External applications
    - Service Principals and Managed Identities
  - Role assignments
  - Group organization



RBAC and Access Control Lists

- Common Role-Based Access Controls:
  - Owner
    - Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
  - Contributor
    - Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC
  - Reader
    - View all resources but does not allow you to make any changes.



- RBAC: Broad Access to Resources
- ACLs: Finer Access to Data

Compliance

**noun - com·pli·ance | \ kəm-ˈplī-ən(t)s **

“Conformity in fulfilling official requirements”

Azure Compliance Offerings

Global
CIS benchmark
CSA STAR Attestation
CSA STAR Certification
CSA STAR self-assessment
SOC 1
SOC 2
SOC 3
ISO 20000-1
ISO 22301
ISO 27001
ISO 27017
ISO 27018
ISO 27701
ISO 9001
WCAG

Healthcare and life sciences
ASIP HDS (France)
EPCS (US)
GxP (FDA 21 CFR Part 11)
HIPAA (US)
HITRUST
MARS-E (US)
NEN 7510 (Netherlands)

US government
CJIS
CMMC
CNSSI 1253
DFARS
DoD IL2
DoD IL4
DoD IL5
DoD IL6
DoE 10 CFR Part 810
EAR
FedRAMP
FIPS 140
ICD 503
IRS 1075
ITAR
JSIG
NDAA
NIST 800-161
NIST 800-171
NIST 800-53
NIST 800-63
NIST CSF
Section 508 VPATs
StateRAMP

Financial services
23 NYCRR Part 500 (US)
AFM and DNB (Netherlands)
AMF and ACPR (France)
APRA (Australia)
CFTC 1.31 (US)
EBA (EU)
FCA and PRA (UK)
FFIEC (US)
FINMA (Switzerland)
FINRA 4511 (US)
FISC (Japan)
FSA (Denmark)
GLBA (US)
KNF (Poland)
MAS and ABS (Singapore)
NBB and FSMA (Belgium)
OSFI (Canada)
OSPAR (Singapore)
PCI 3DS
PCI DSS
RBI and IRDAI (India)
SEC 17a-4 (US)
SEC Regulation SCI (US)
SOX (US)
TruSight

Automotive, education, energy, media, and telecommunication
CDSA
DPP (UK)
FACT (UK)
FERPA (US)
MPA
GSMA
NERC (US)
TISAX

Regional - Americas
Argentina PDPA
Canada privacy laws
Canada Protected B
US CCPA

Regional - Asia Pacific
Australia IRAP
China GB 18030
China DJCP (MLPS)
China TCS
India MeitY
Japan CS Gold Mark
Japan ISMAP
Japan My Number Act
Korea K-ISMS
New Zealand ISPC
Singapore MTCS

Regional - EMEA
EU Cloud CoC
EU EN 301 549
ENISA IAF
EU GDPR
EU Model Clauses
Germany C5
Germany IT-Grundschutz workbook
Netherlands BIR 2012
Russia personal data law
Spain ENS High
Spain LOPD
UAE DESC
UK Cyber Essentials Plus
UK G-Cloud
UK PASF

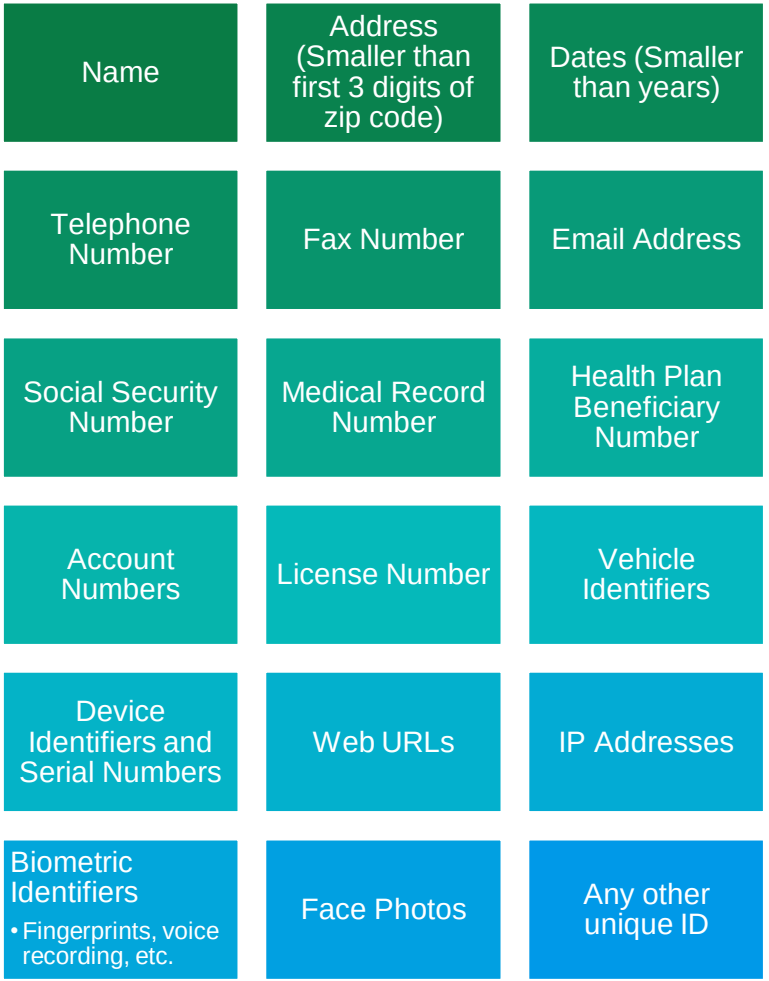
HIPAA, HITECH, and HITRUST

- **HIPAA:** Health Insurance Portability and Accountability Act of 1996
  - Sets requirements for using, disclosing, and handling protected health information (PHI)

- **HITECH:** Health Information Technology for Economic and Clinical Health Act of 2009
  - Extends HIPAA for electronic health records and more modern, data-driven technology in healthcare

- **HITRUST:** Health Information Trust Alliance
  - A private company that sets standards, based on HIPAA/HITECH, and provides certification.

HITRUST



https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-hipaa-us

SOX

- Sarbanes-Oxley Act of 2002
  - US federal law from the Securities and Exchange Commission (SEC)
  - Mandates financial record keeping practices
  - Thanks to the ENRON and WorldCom scandals

Retain data for the req'd amount of time

- Offsite backups

Manage security and access controls

- Physical and electronic access

Know when something is deleted or changed (version control)

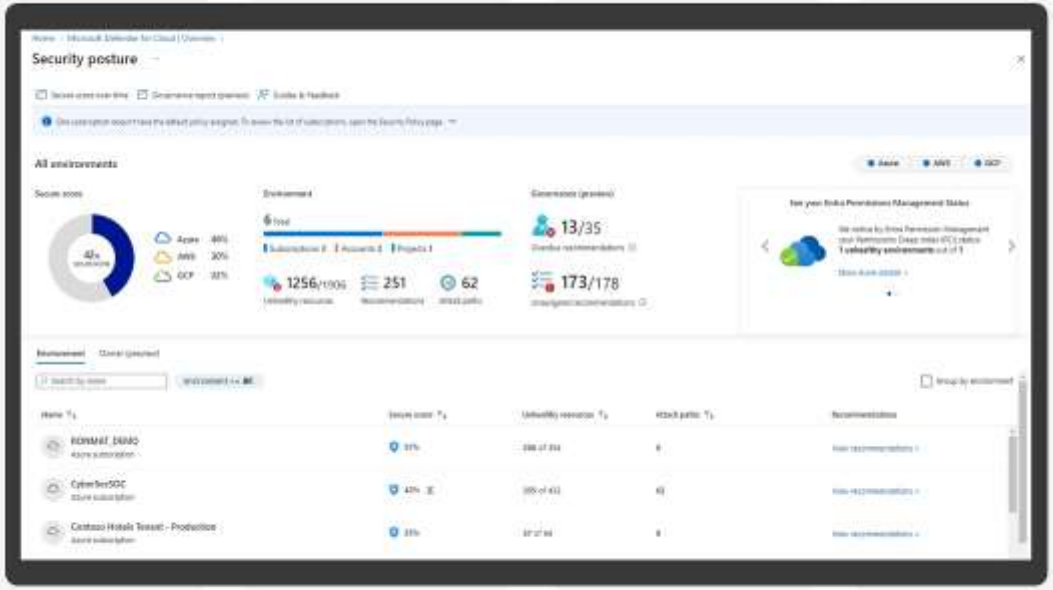
- Prevent data tampering
- Audit trails, logs

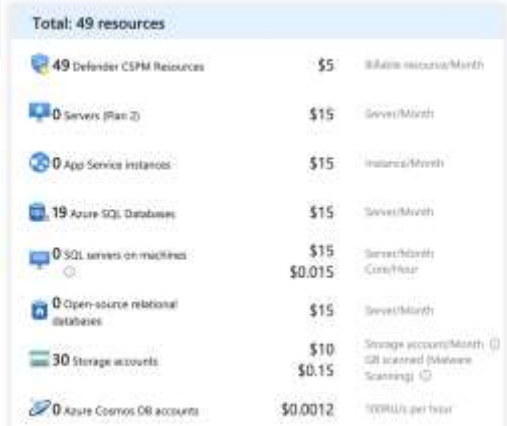
Prove you've retained compliance for a rolling 90 days

- Visibility into system and org compliance

Defender for Cloud

- Reviews your various services to check for vulnerabilities
- Assesses your compliance to various security standards
- Works across clouds
- Pay by the resource

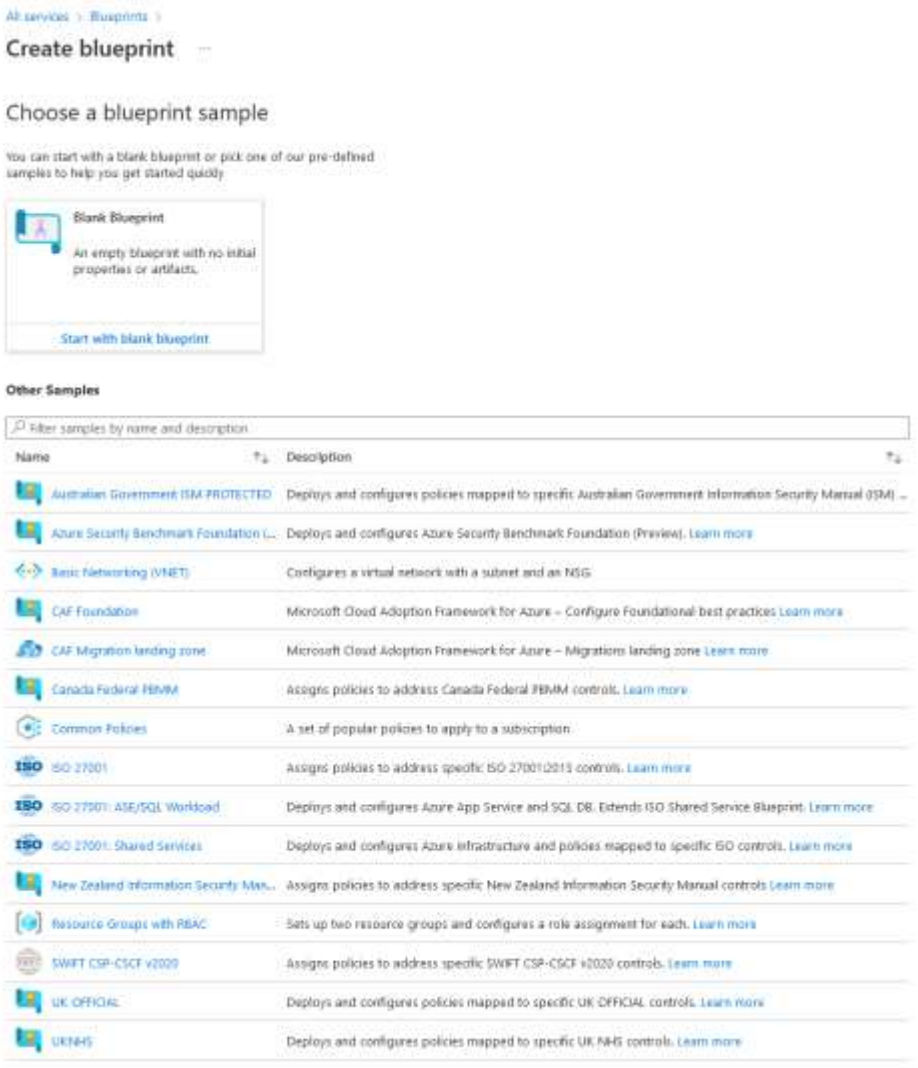




Azure Blueprints

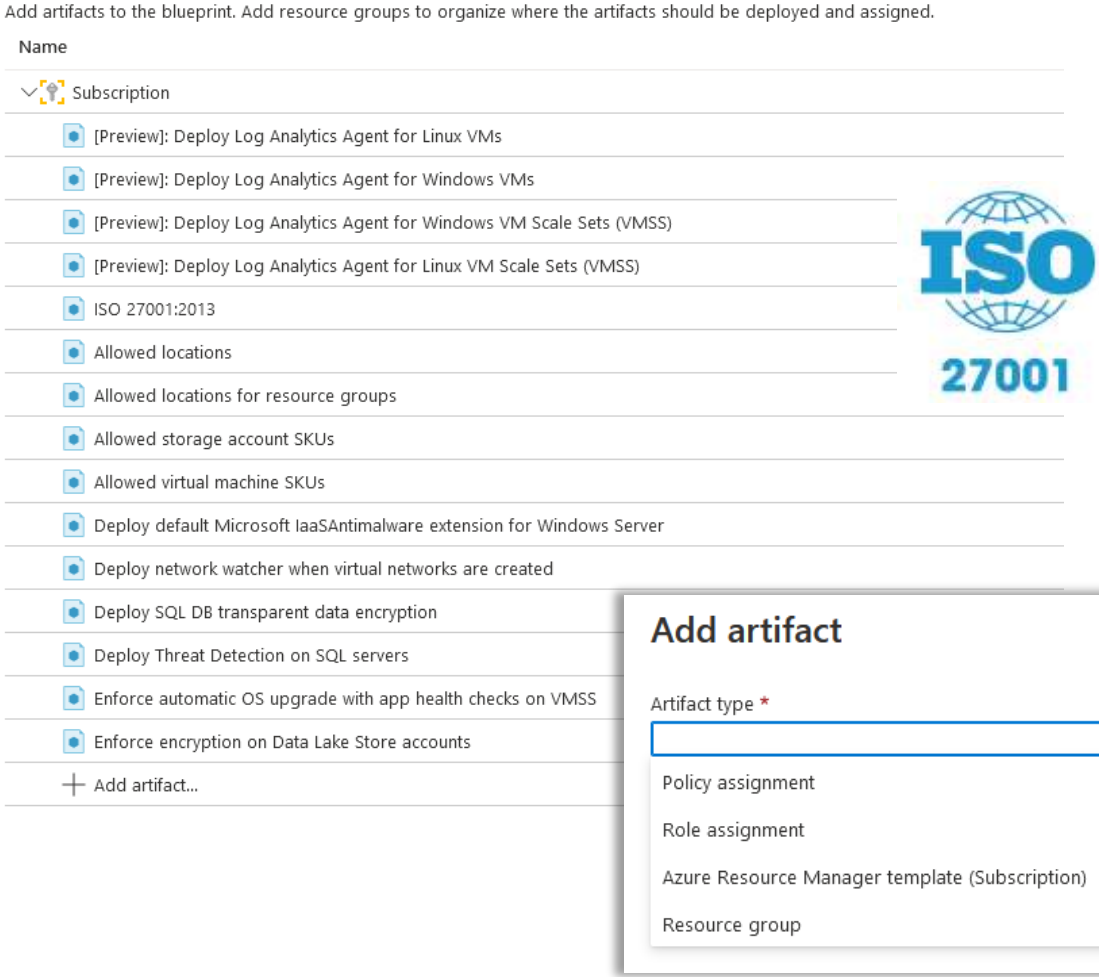
- Set of organizational standards and requirements for compliance or policy adherence.

- Orchestrate the deployment of artifacts:
  - Role Assignments
  - Policy Assignments
  - Azure Resource Manager templates (ARM templates)
  - Resource Groups



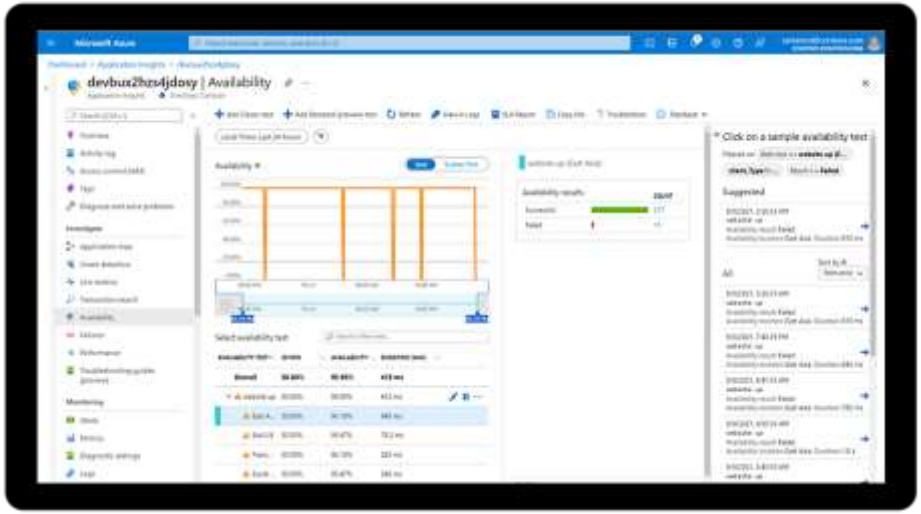
ISO 27001

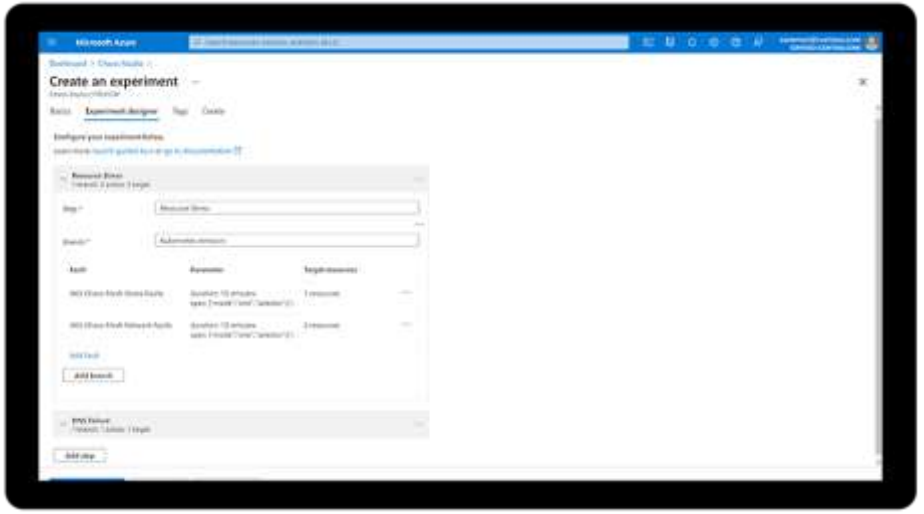
- International Standard for *information security*
- 14 main Controls
    - Information security policies, HR security, asset management, access control, cryptography, physical security, etc.



Azure Chaos Studio

- Run experiments to see how your infrastructure handles certain scenarios
    - Disaster recovery
    - Fault injections
    - Code optimizations

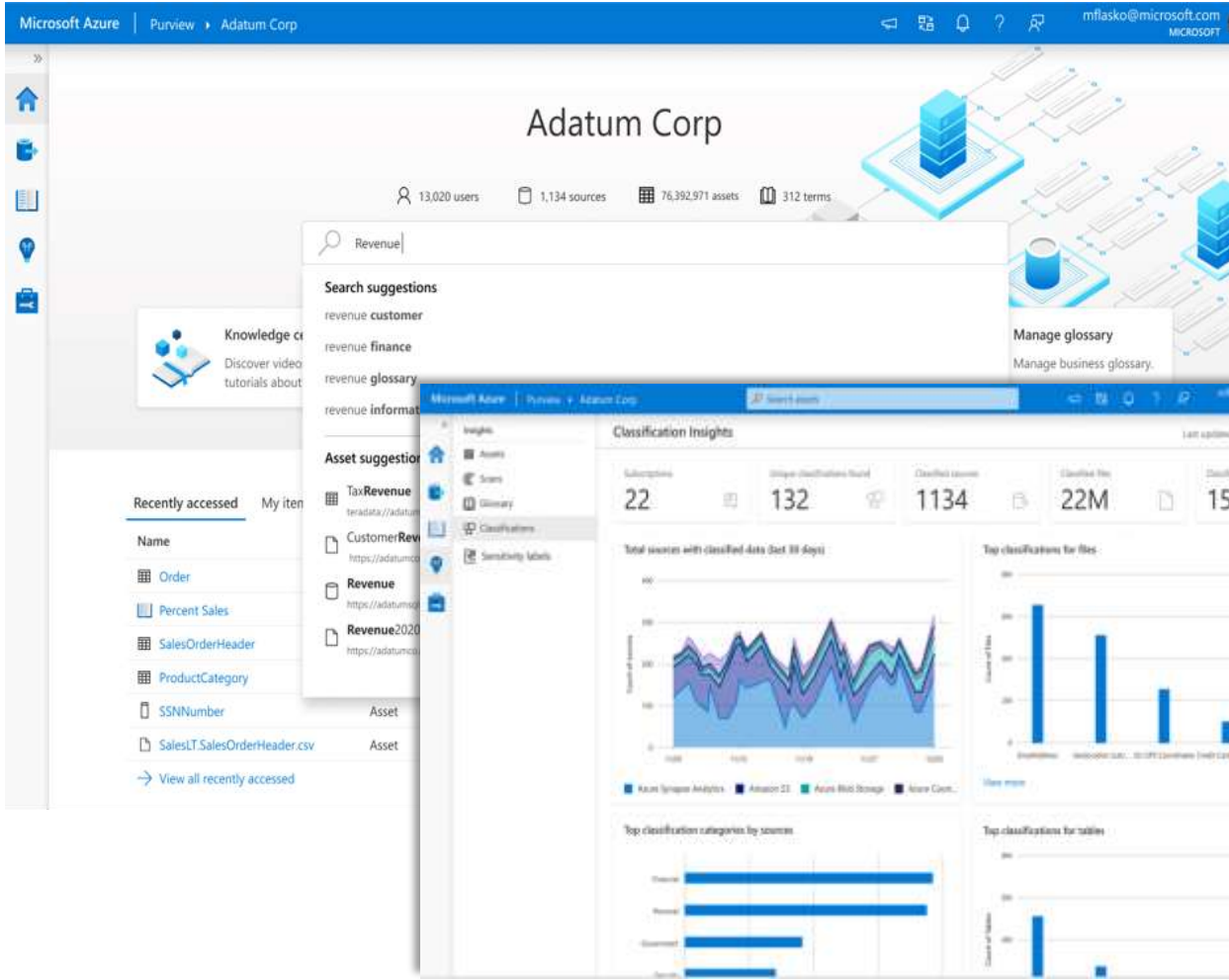


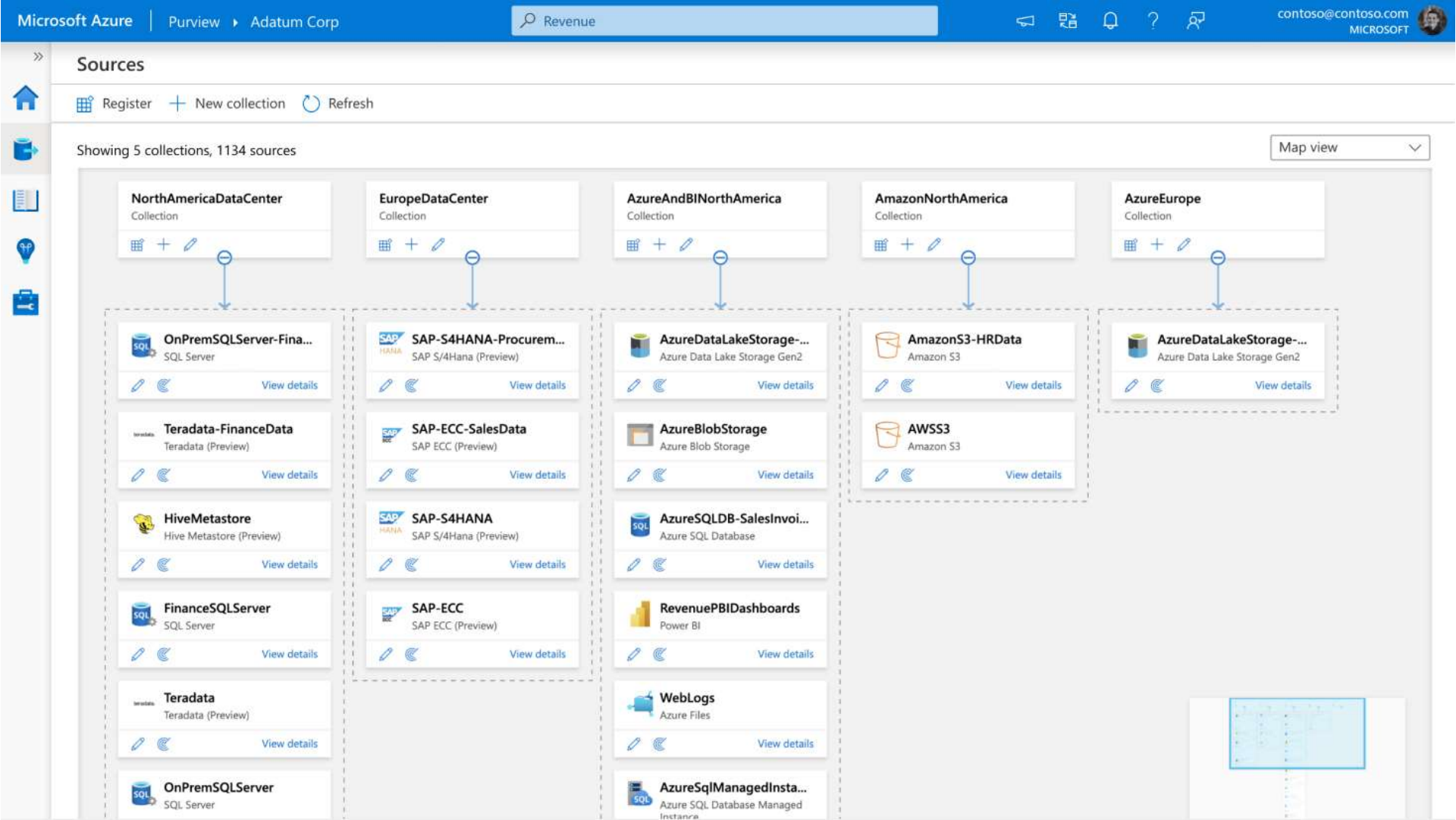


Now that I have a bunch of stuff in the cloud, how do I see it all?

Azure Purview

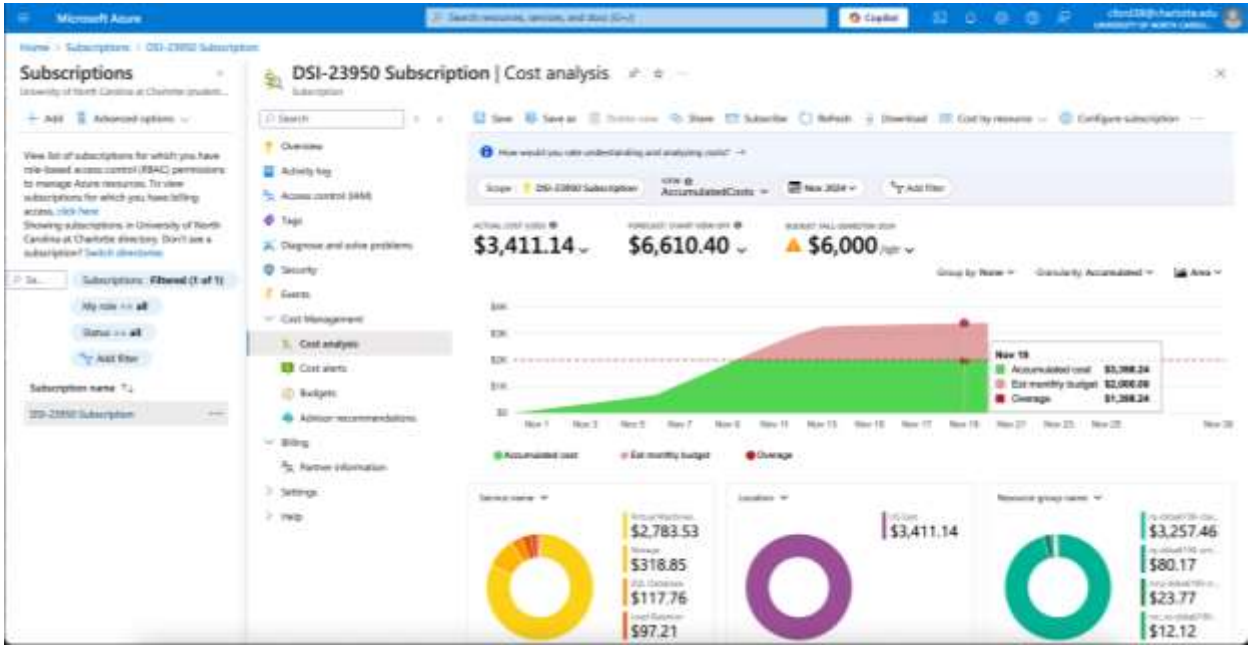
- Data governance platform in Azure that allows us to manage on-prem and multicloud data and services.
    - Create a map of your data estate – “Data Catalog”
    - Find, label, and track sensitive data.
    - See how data flows through your platforms




Microsoft Azure
Purview
Adatum Corp
Revenue
contoso@contoso.com
MICROSOFT
Sources
Register
New collection
Refresh
Showing 5 collections, 1134 sources
Map view
NorthAmericaDataCenter
Collection
EuropeDataCenter
Collection
AzureAndBINorthAmerica
Collection
AmazonNorthAmerica
Collection
AzureEurope
Collection
OnPremSQLServer-Fina...
SQL Server
View details
Teradata-FinanceData
Teradata (Preview)
View details
HiveMetastore
Hive Metastore (Preview)
View details
FinanceSQLServer
SQL Server
View details
Teradata
Teradata (Preview)
View details
OnPremSQLServer
SQL Server
SAP-S4HANA-Procurem...
SAP S/4Hana (Preview)
View details
SAP-ECC-SalesData
SAP ECC (Preview)
View details
SAP-S4HANA
SAP S/4Hana (Preview)
View details
SAP-ECC
SAP ECC (Preview)
View details
AzureDataLakeStorage-...
Azure Data Lake Storage Gen2
View details
AzureBlobStorage
Azure Blob Storage
View details
AzureSQLDB-SalesInvoi...
Azure SQL Database
View details
RevenuePBIDashboards
Power BI
View details
WebLogs
Azure Files
View details
AzureSqlManagedInsta...
Azure SQL Database Managed Instance
AmazonS3-HRData
Amazon S3
View details
AWSS3
Amazon S3
View details
AzureDataLakeStorage-...
Azure Data Lake Storage Gen2
View details

Subscriptions

- Subscriptions are the place where cloud services are billed
- In smaller organizations, it's common to see a single Subscription for the whole company
- In larger organizations, you may see Subscriptions set up for individual groups or applications
    - Also, maybe even separate Subs for dev, staging, and production.



- There are different "offer types" that may affect pricing.
    - Pay-as-you-Go vs. Enterprise Agreement

https://azure.microsoft.com/en-us/support/legal/offer-details