Microsoft

January 30, 2019 — 8:30 AM - 5:00 PM | Detroit, Michigan

Azure Dev Day

Learn, architect, and develop solutions on Azure

#AzureDevDays

for developers, by developers

Learn.

Connect.

Explore.

Microsoft

Azure App Service

Randy Pagels
Azure Technical Specialist – App Dev

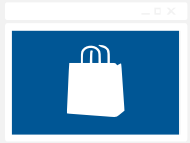
Learn.

Connect.

Explore.

Industry-leading Application PaaS Platform

Solutions



Transactional Apps

Digital Marketing

LoB App Modernization

Services

Web Apps

Web App for Containers

API Apps

Mobile Apps

IDE

Enterprise Integration

Serverless compute

Data /Storage

Intelligence

Application Insights

Platform

App Service

Fully Managed Platform • High Productivity Development • Enterprise Grade Apps

App Service

App Service

Web apps

Web app for containers*

API apps

Mobile apps

DevOps productivity

Source code control integration

CI/CD build and deploy

Staged deployments with slots

Auto scale on demand

Monitoring and diagnosis

Application templates

Umbraco

Orchard

Episerver

WordPress

DNN Platform

Joomla

Drupal

Multiple languages and frameworks

ASP.NET

ASP.NET Core

Java

python

nodeJS

Ruby

php

Enterprise workloads

Industry standards

Global scale

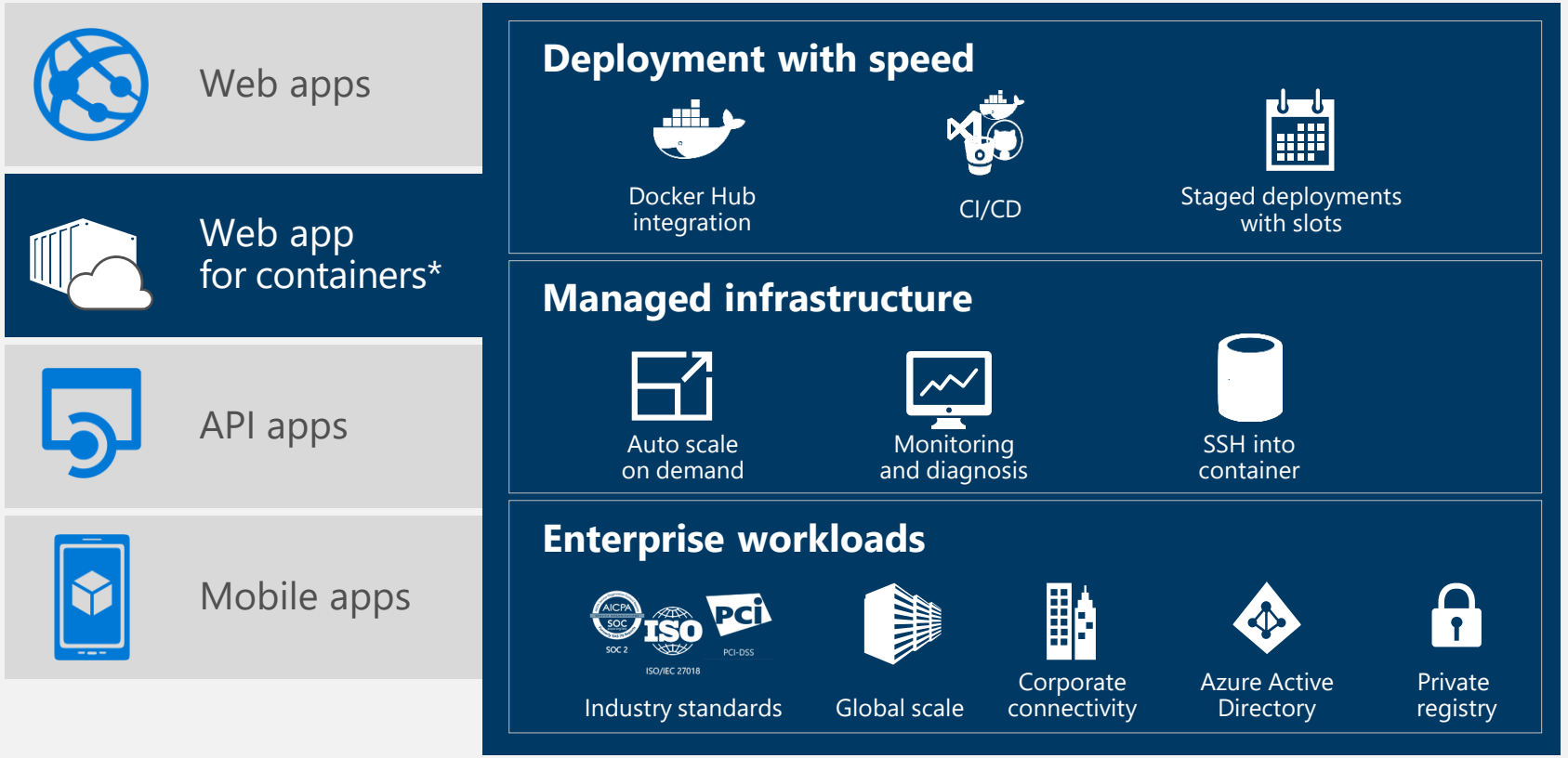
Corporate connectivity

Azure Active Directory

Dedicated environments

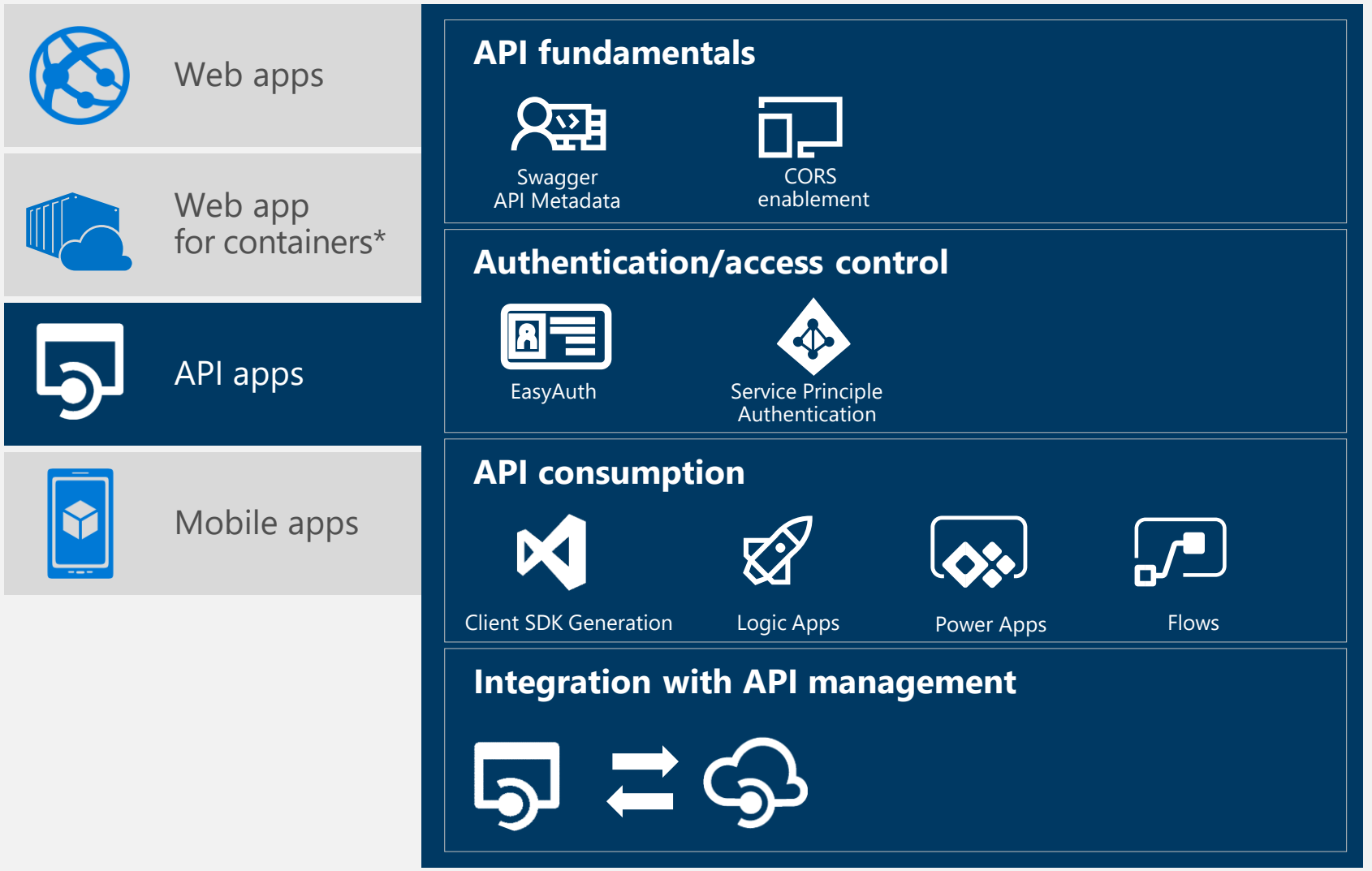
App Service

App Service



App Service

App Service



App Service

App Service

Web apps

Web app
for containers*

API apps

Mobile apps

Offline sync

User authentication

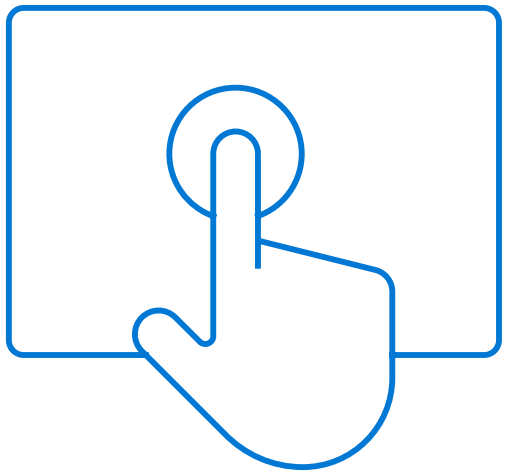
Facebook Twitter Microsoft Google Azure Active Directory

Push notifications

Apple iOS OSX Android Windows Kindle In-App

Data connections

Azure SQL database Mongo DB Document DB Office 365 Azure tables



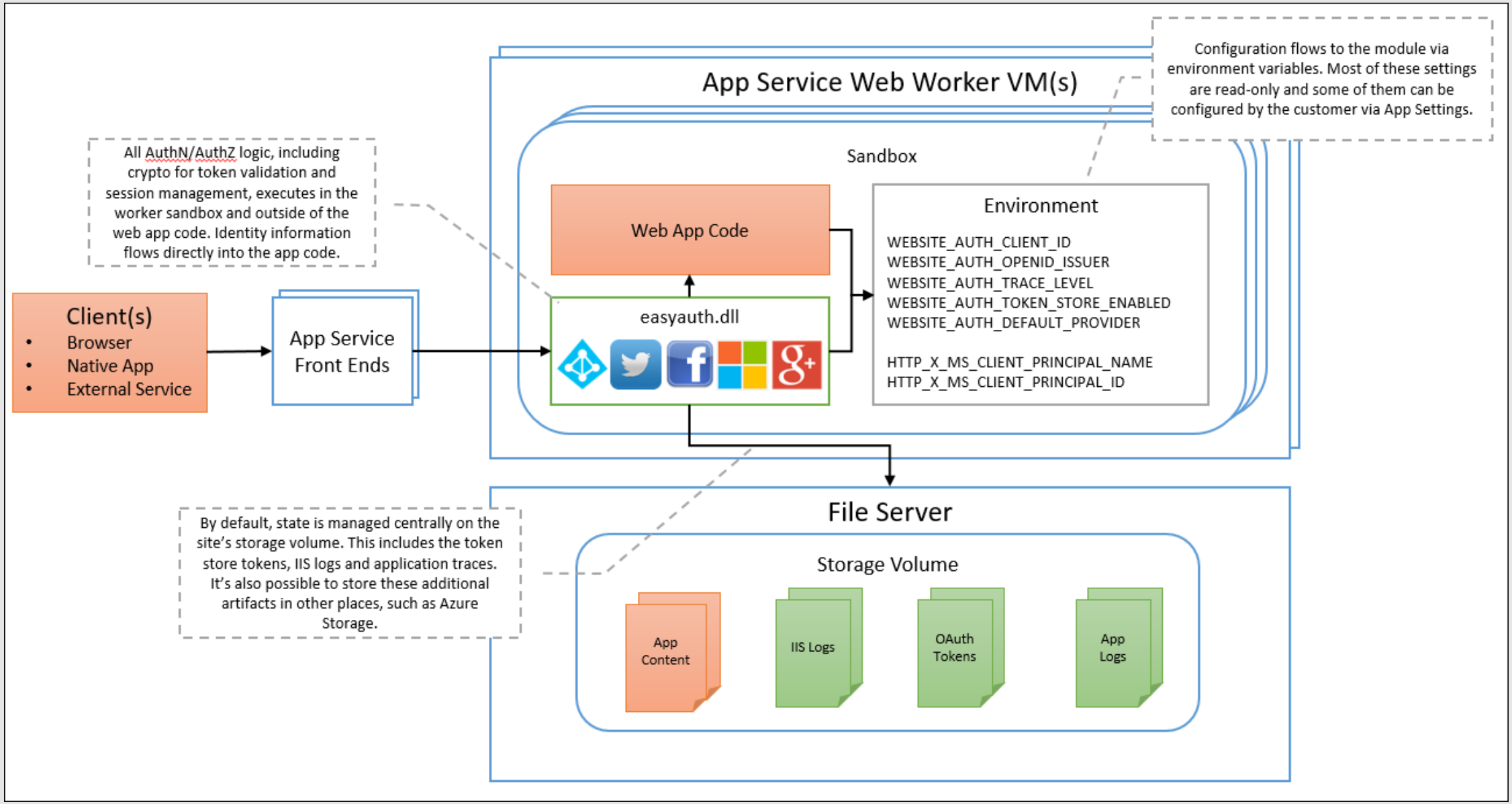
Getting Started Demo

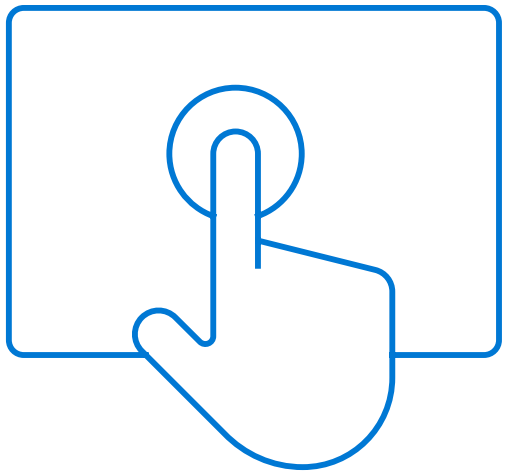
Create a simple web app

Broad set of capabilities

Staging Slots

App Service Architecture

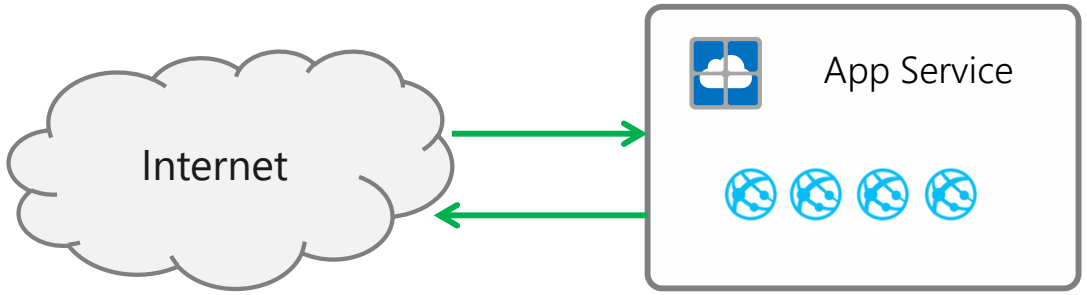




App Service Networking

Getting started with DevOps Project

Default behavior

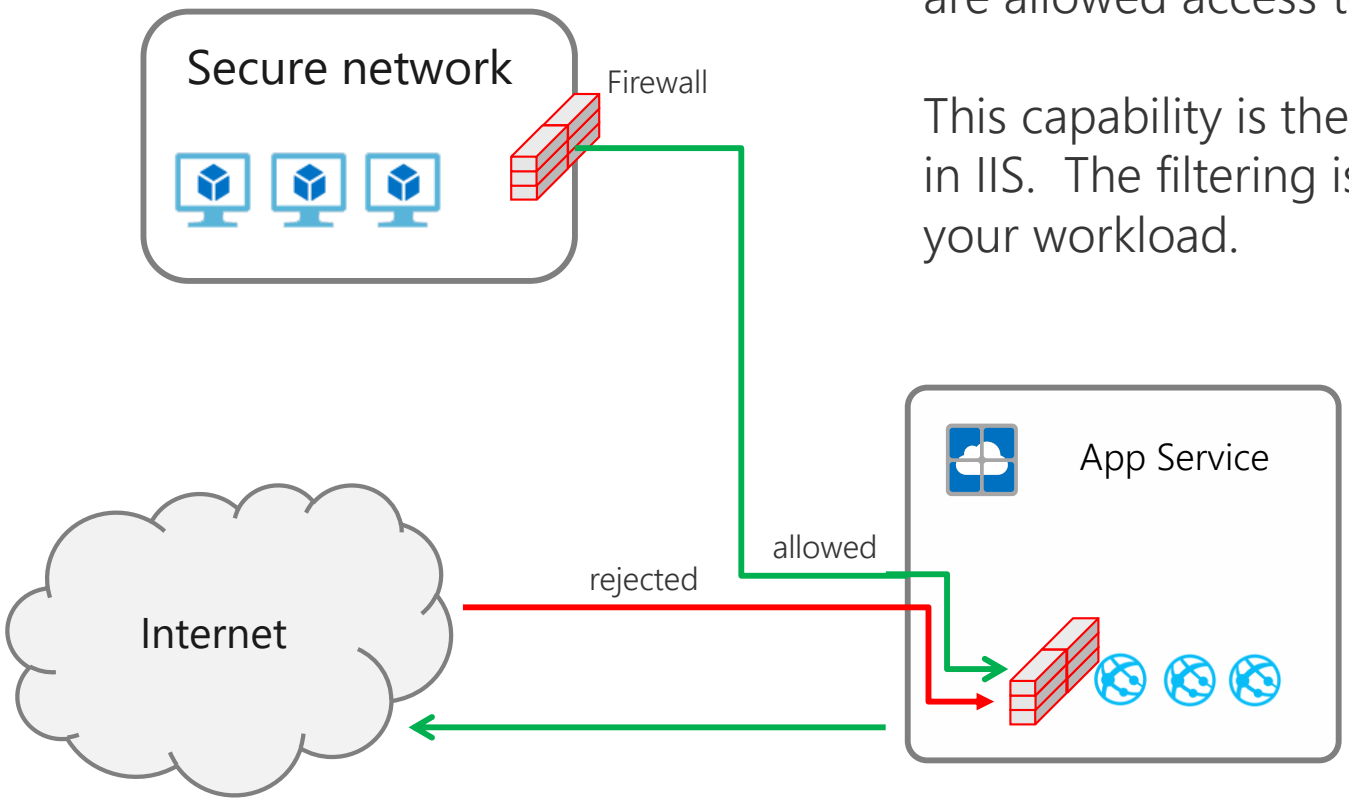


Inbound traffic to your app hits an IP address that is shared with the other apps.

Outbound backend calls from your app can only go out to the internet through a set of addresses shared with other apps. There are anywhere from 4 to 11 addresses used for outbound traffic

IP Restrictions

Scenario: Restrict access to your app at the web server. Can combine with app assigned address for a dedicated channel to your app.



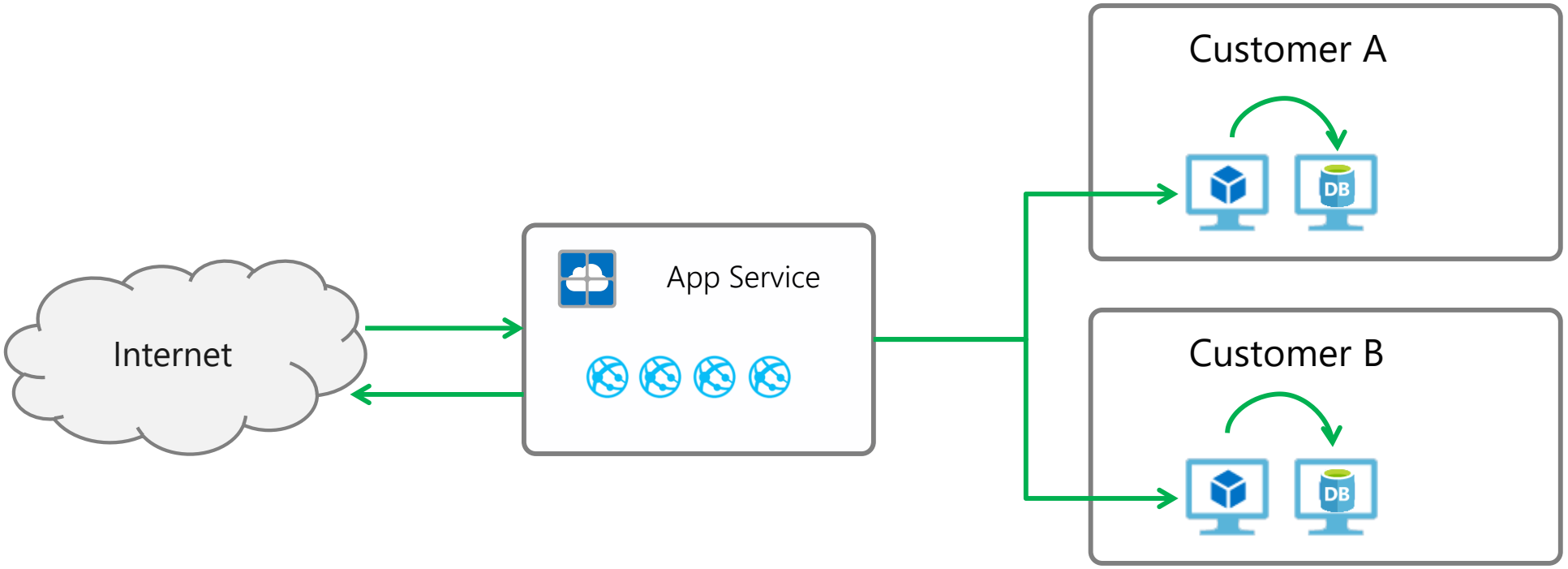
This capability allows you to define a set of IP ranges that are allowed access to your app.

This capability is the same as the IP filtering capability seen in IIS. The filtering is enforced at the web server hosting your workload.

Hybrid Connections

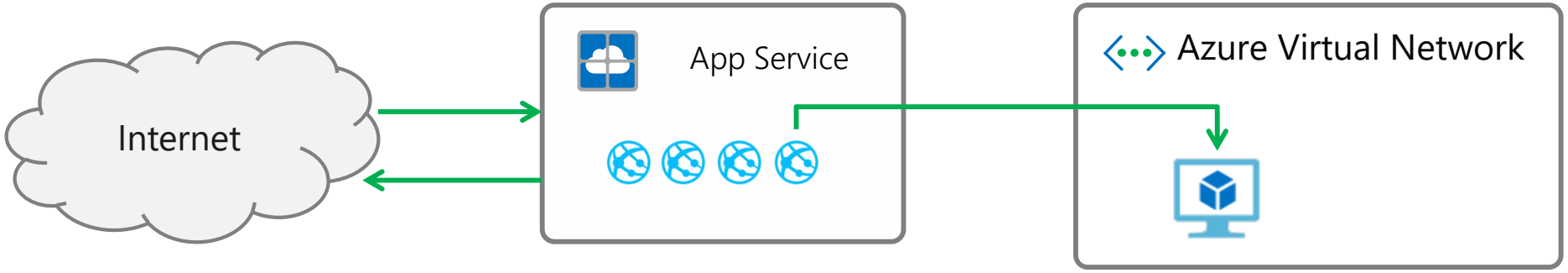
Scenario: Access into networks lacking a VPN to Azure
Examples: Inventory management service that needs access into customer databases

Outbound backend calls from your app can reach TCP endpoints (host:port) in your any network that can access the internet.



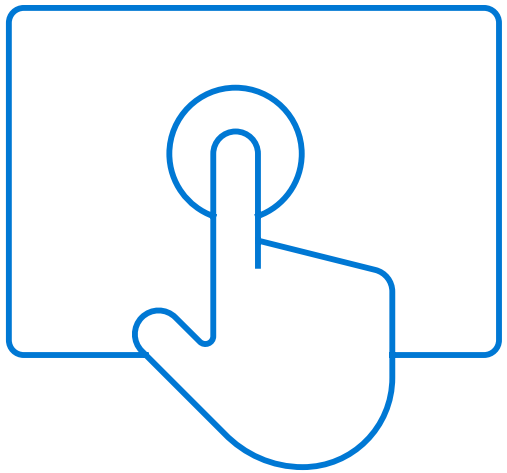
VNet Integration

Scenario: Access resources in your Azure VNet
Example: Wordpress site with the database on a VM in your VNet



Outbound backend calls from your app can go to private IP addresses in your Azure Virtual Network or go out to the internet through a set of addresses shared with other apps.

You can reach on premises resources if VNet uses a Site to Site VPN to reach the on premises network. This does not work with ExpressRoute.



App Service w/
Front Door / Traffic Manager

App Service Load Balancing

Front Door

Azure Front Door Service is Microsoft's highly available and scalable web application acceleration platform and global HTTP(s) load balancer. It provides built-in DDoS protection and application layer security and caching.F ront Door enables you to build applications that maximize and automate high-availability and performance for your end-users.

Use Front Door with Azure services including Web/Mobile Apps, Cloud Services and Virtual Machines – or combine it with on-premises services for hybrid deployments and smooth cloud migration.

Below are some of the key scenarios that Azure Front Door Service addresses:

- Use Front Door to improve application scale and availability with instant multi-region failover
- Use Front Door to improve application performance with SSL offload and routing requests to the fastest available application backend.
- Use Front Door for application layer security and DDoS protection for your application.

App Service Load Balancing

Traffic Manager

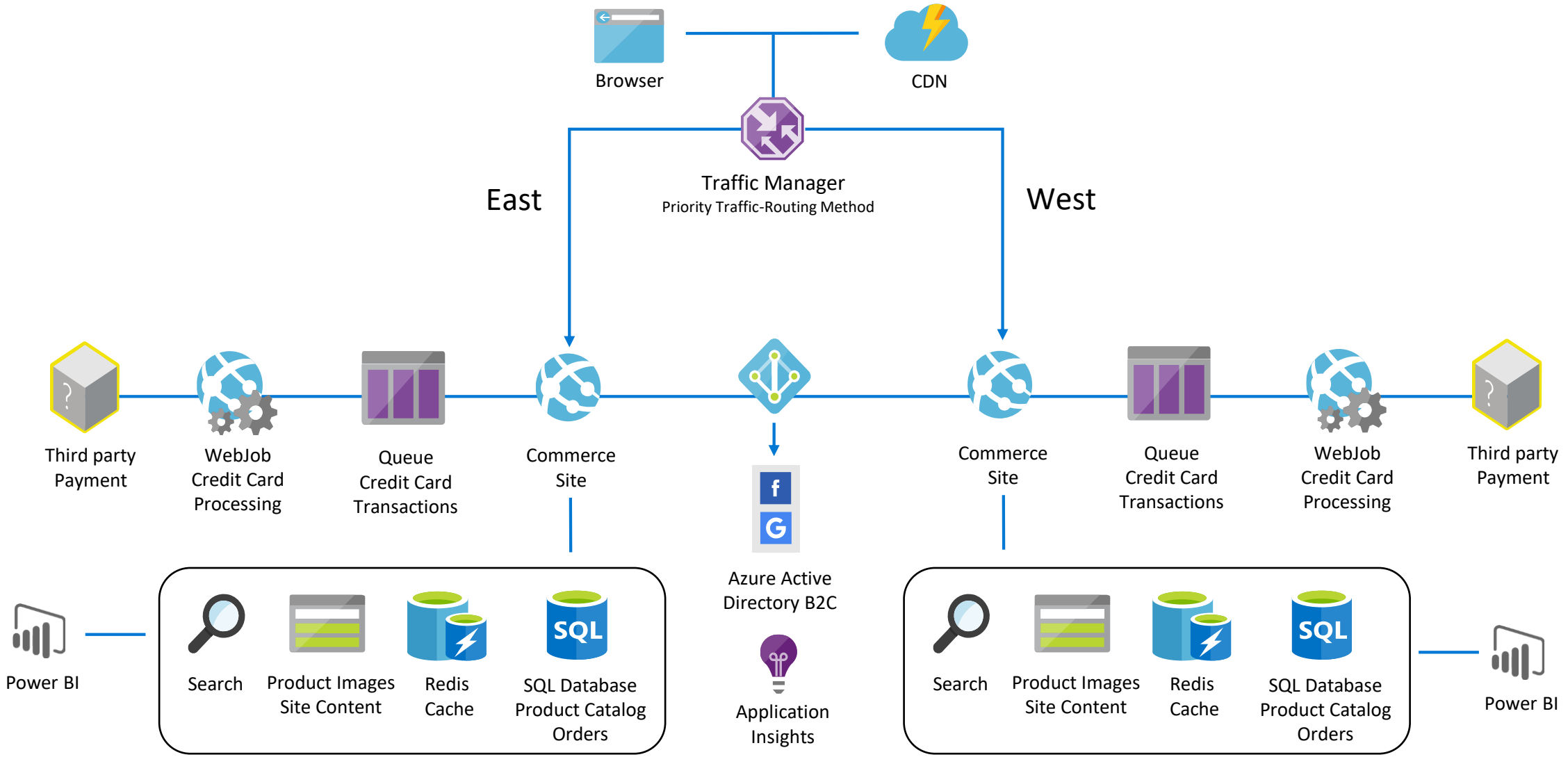
Azure Traffic Manager helps reduce downtime and improve responsiveness of important applications by routing incoming traffic across multiple deployments in different regions. Built-in health checks and automatic re-routing help ensure high availability if a service fails.

Use Traffic Manager with Azure services including Web Apps, Cloud Services and Virtual Machines - or combine it with on-premises services for hybrid deployments and smooth cloud migration.

Use Traffic Manager to:

- Improve app availability with automatic failover.
- Increase your app's responsiveness by routing end users to the Azure location with lowest network latency.
- Seamlessly combine on-premises and cloud.

Fault-tolerant E-Commerce with personalized recommendations



App Service

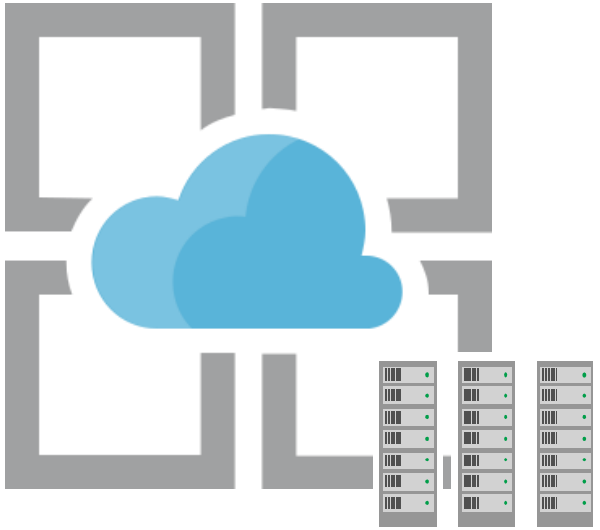
From on-premises to the cloud

AZURE APP SERVICE (MULTI-TENANT)

Get your Web, API, or Mobile App created in seconds in the cloud. We provide the infrastructure, you provide your application code.

APP SERVICE ENVIRONMENT

Run your apps in virtual network at high scale. Manage all of the resources behind your public endpoint creating an isolated environment specifically for your organization.



AZURE STACK

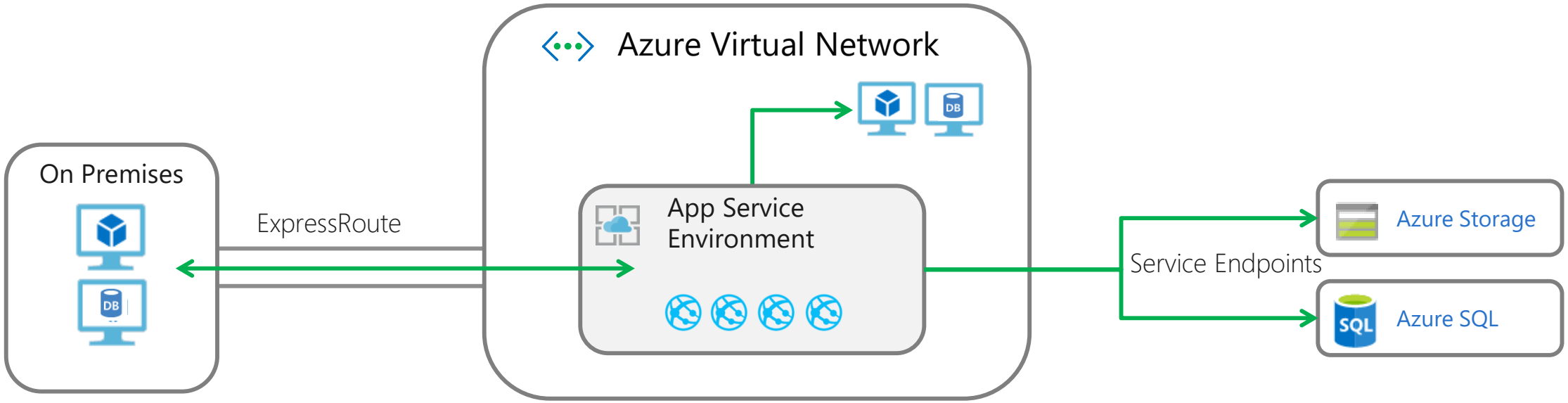
Leverage cloud innovations in on-premises infrastructure. App Service on Azure Stack brings the power of Azure App Service to your own data centers.

App Service Environment (ASE)

Scenario: Access resources in your Azure VNet

Example: Line of business sales application that is on a private IP address and uses SQL and Storage

ExpressRoute makes the Azure VNet a part of your on premises network. Access to your apps should be automatic unless blocked. By using an ILB ASE you can host internal applications on the public cloud but isolated from the internet.



Thank You!