Government of Canada | Gouvernement du Canada

Canada

TBS Workload migration

Leveraging Azure App Services and DevOps to deploy PBMM workloads

GC ESA

ASI GC

18 June 2019

Content

Purpose:
To provide an overview of TBS Web Application Services workload migration to Azure App Services.

1. WLM Project
2. Context
3. TBS Web App Security
4. DevOps Integration Overview
5. Azure App Services & DevOps

Workload migration at TBS

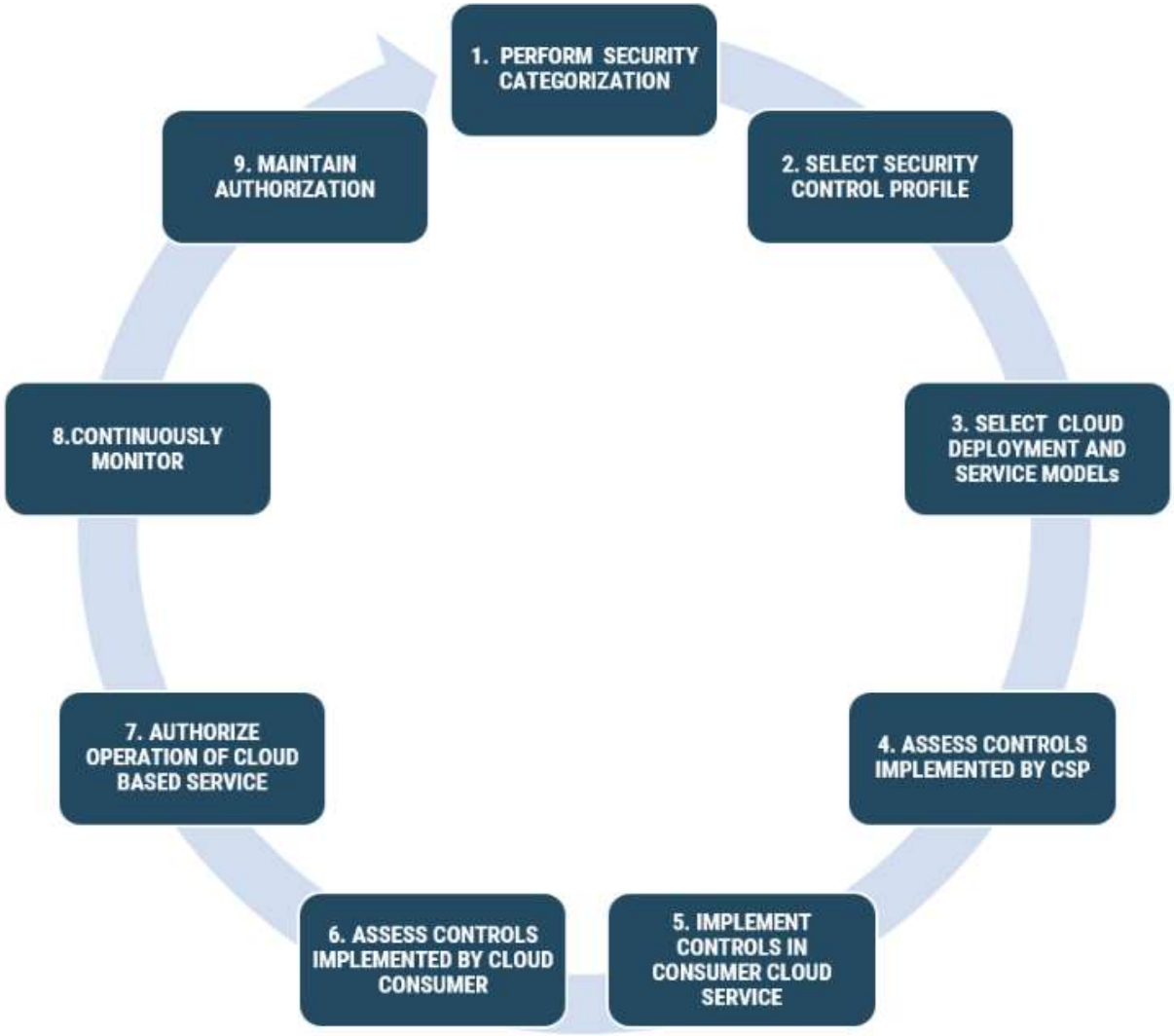
~150 custom web applications at TBS
- Classic ASP, many flavours .NET
- TBS only, GC Only, and Public facing
- Some SMTP dependencies
- Some SAML integration
- Web apps integration with IaaS based DB's

Waves 1 thru 4 – Q1 / Q2 / Q3 / Q4 2019
- Waves are based on dependencies and complexity: Mail, AD, auth, etc.

Context


Policy
GC Cloud Computing Direction & Standards
People
Collaborative & Skilled Community
Process
Cloud Security Risk Management, Secure SDLC, DevSecOps, etc.
Technology
Modern Tooling & Practices

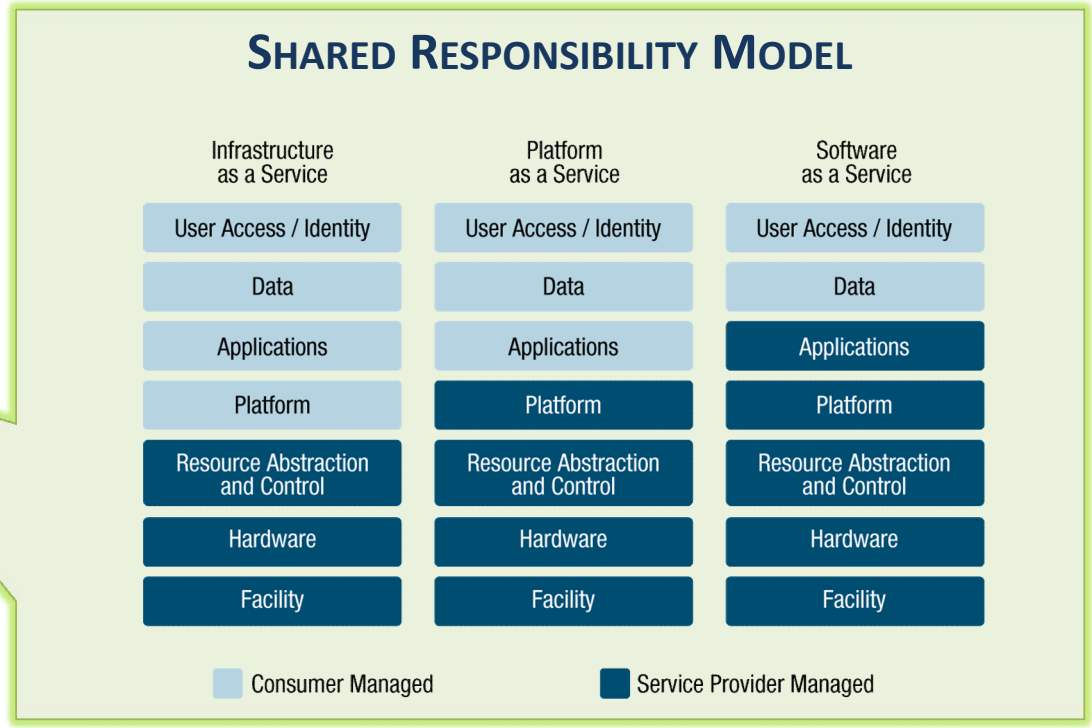
Cloud Security Risk Management approach



CCCS ITSM 50.062

Shared Responsibility Model

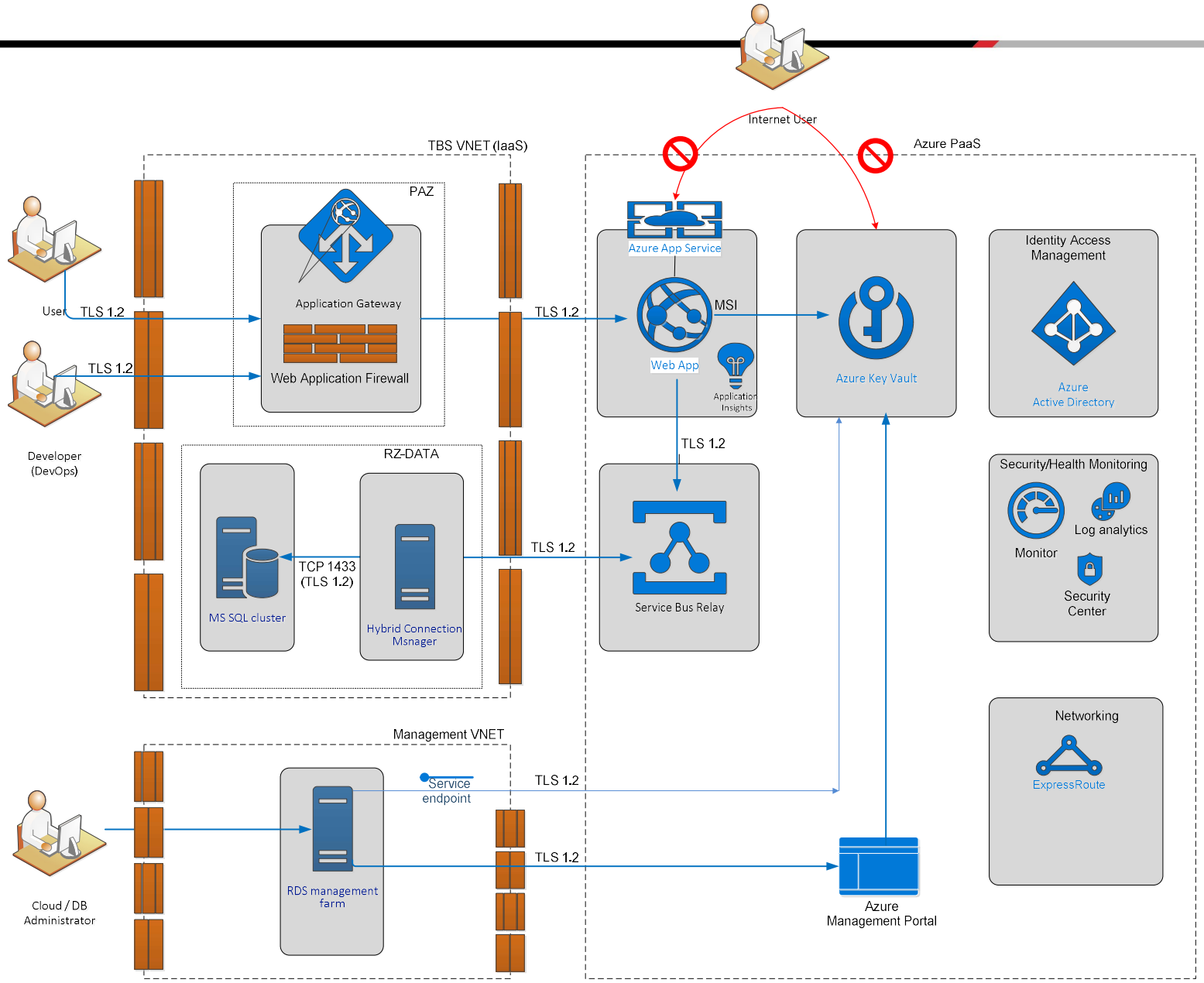
DIRECTION ON SECURE USE OF COMMERCIAL CLOUD SERVICES: SPIN 2017-01



TBS Web Application Services

- Web application hosting solution in an Azure cloud environment that supports Protected B workloads
- Secure environment that leverages Azure platform as a service (PaaS) and Infrastructure as a Service (IaaS) capabilities.
- Public and Internal Web Apps are separated from each other on separate App Service Plans
- MS SQL relational database deployed on IaaS support the Web Apps deployed on Azure App Services
- All connections are encrypted through TLS 1.2 to ensure data confidentiality and integrity

TBS Web Apps (Hybrid Paas/IaaS solution)



Design components

The TBS Web Application Services is an hybrid solution and includes IaaS and PaaS components.

PaaS

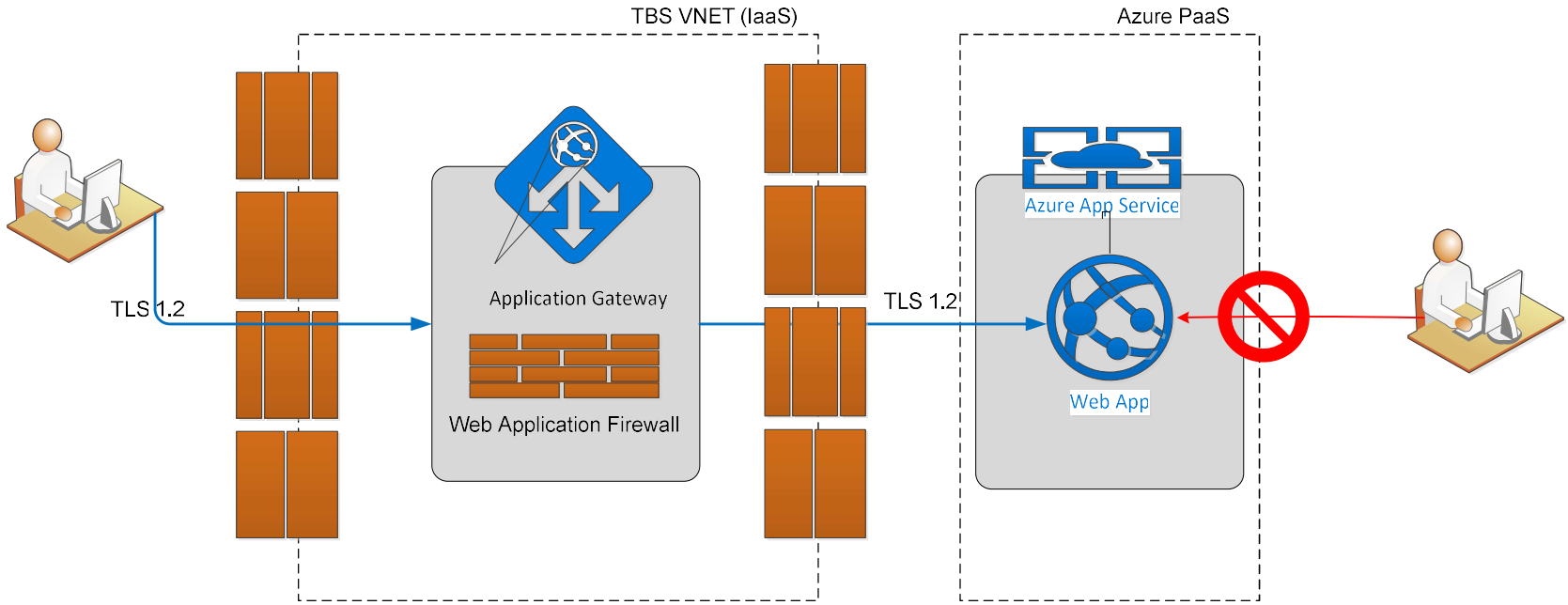
Azure Application Gateway (L7 LB + WAF)
Azure KeyVault (Secret management)
Azure Relay Hybrid connection (PaaS to IaaS)
Azure App Services
Azure Storage (Data migration)
Azure Active Directory (Identity and Access)
Azure Application Insight (App telemetry)
Azure Monitor (logs)
Azure Log Analytics
Service endpoint

IaaS

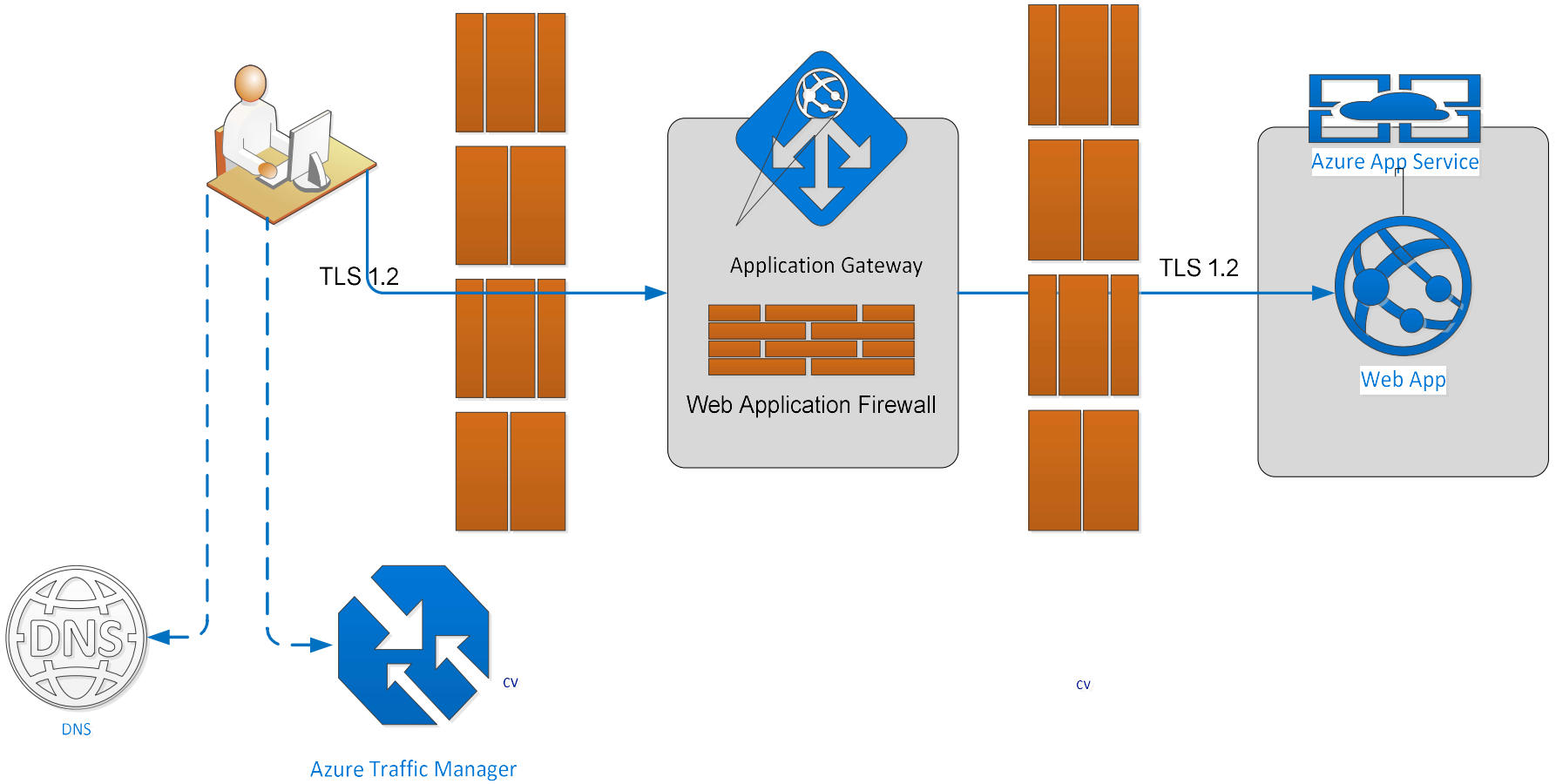
VNET
Azure IaaS VMs (SQL/ SMTP)
Hybrid Connection Manager
Network Virtual Appliances

Azure Application Gateway

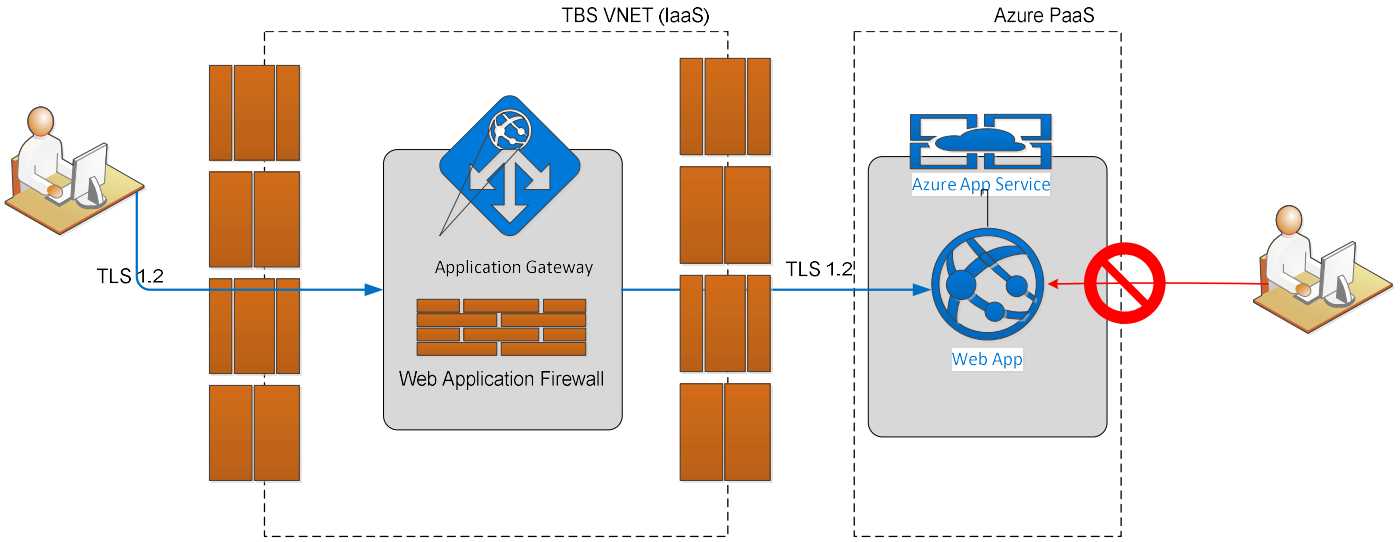
- Centralized protection from common exploits and vulnerabilities (WAF)
- SSL termination, traffic inspection, and re-encrypts the traffic to support end to end SSL encryption.
- TLS 1.2 and strong ciphers
- Restrict access to Web App based on user source address (TBS only, GC only, public)



Azure Application Gateway + Traffic Manager

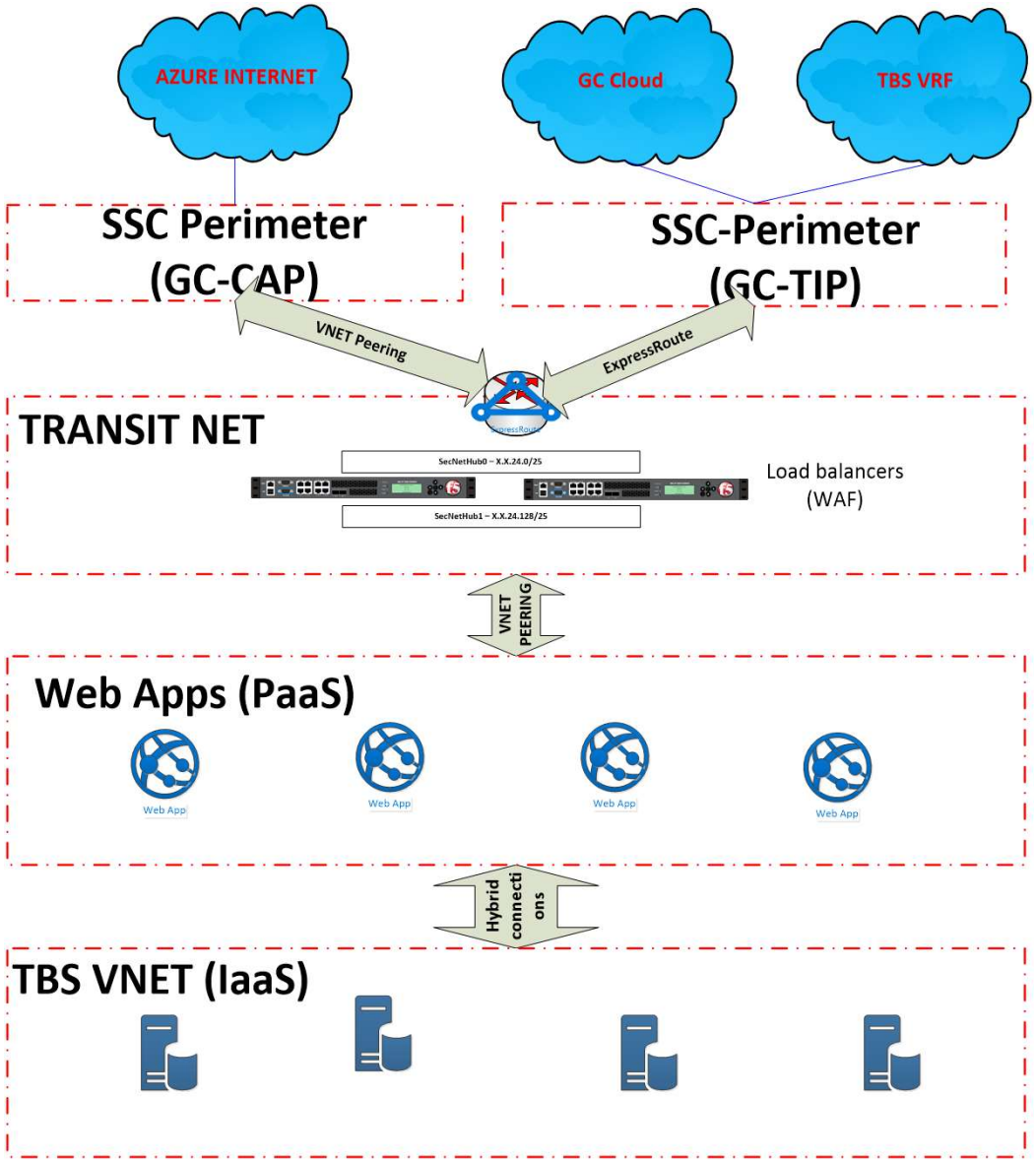


Azure Application Gateway – Security controls



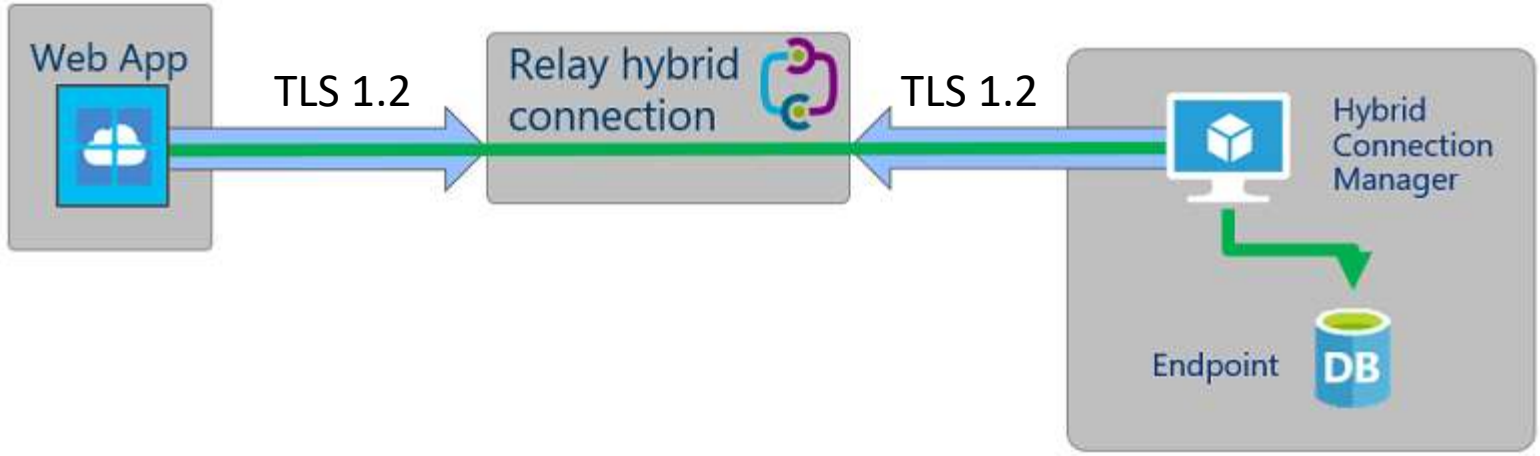
AC-04	Information Flow Enforcement	Restrict access by source address, destination URI and port
SI-04	Information System Monitoring	Enable Web App Firewall (OWASP)
SC-07	Boundary Protection	Limit access point, default deny, and restrict source adrress
SC-08	Transmission confidentiality/Integrity	TLS encrypted communication
SC-13	Cryptographic Protection	TLS 1.2 and strong ciphers
SA-09	External In formation System	Provisionned in Azure Canadian Region

Transit Network

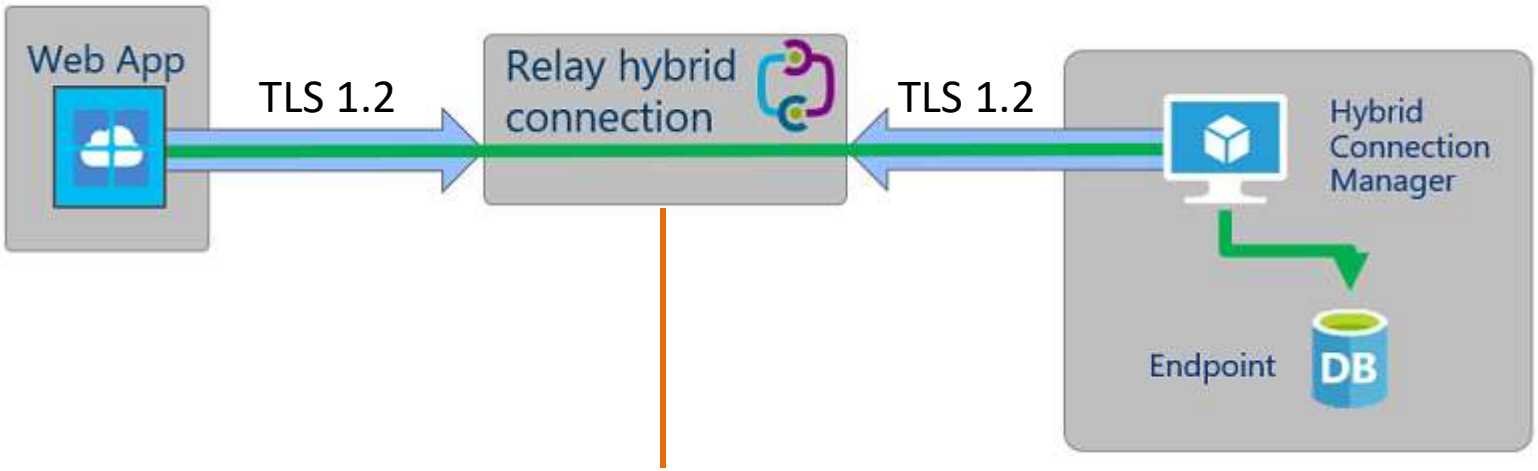


Azure Relay Hybrid Connection

- Used to access application resources in other network
- Each Hybrid Connection correlates to a single TCP host and port combination
- Consists of two outbound calls to Azure Service Bus Relay.
- The connection uses TLS 1.2 for security and shared access signature (SAS) keys for authentication and authorization
- When Webapps makes a DNS request that matches a configured Hybrid Connection endpoint, the outbound TCP traffic will be redirected through the Hybrid Connection.



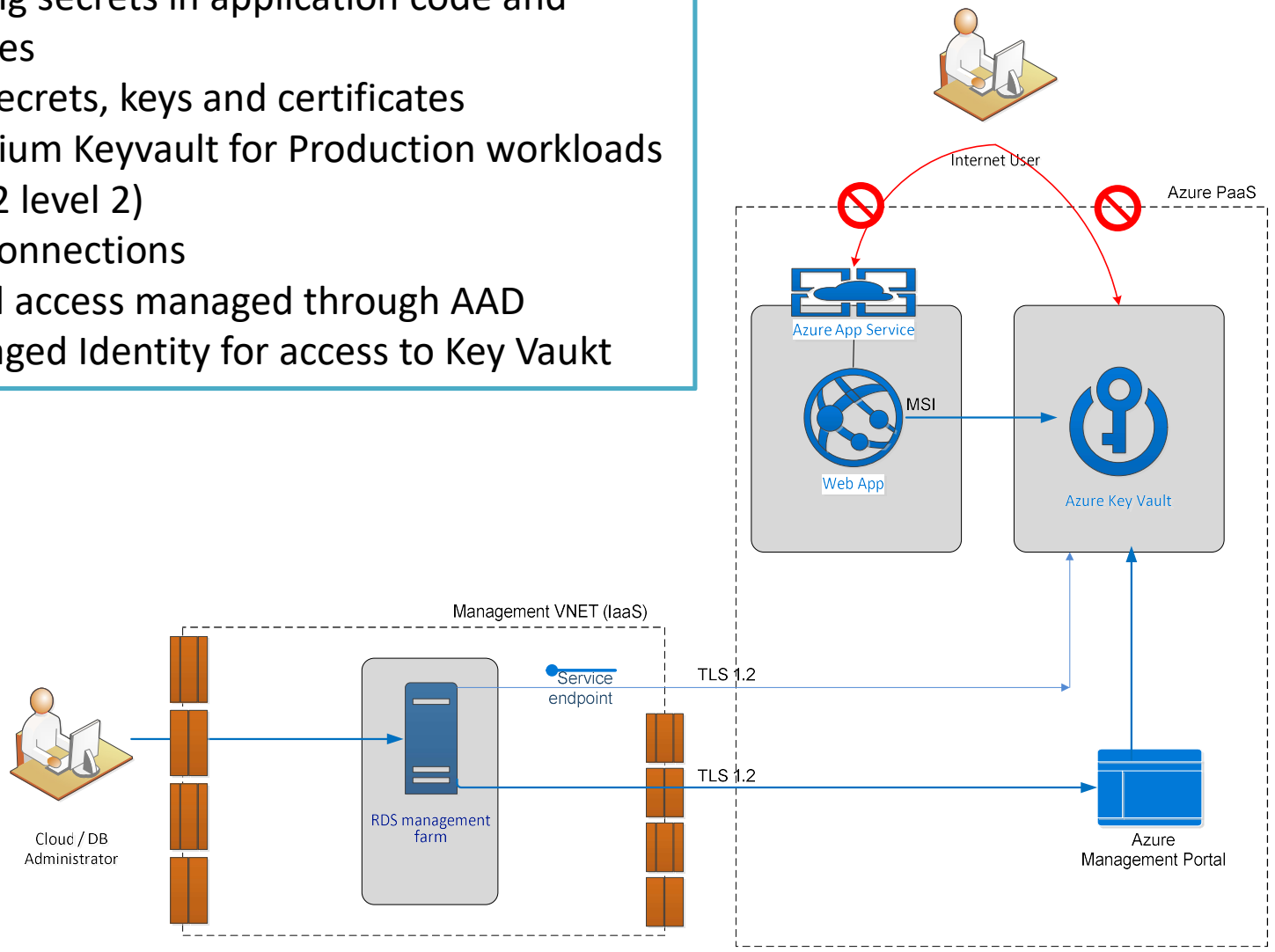
Azure Relay Hybrid Connection – Security controls



AC-03 Access Enforcement	Dedicated namespace protected by connection string
AC-04 Information Flow Enforcement	Flow enforcement by FQDN and port
IA-03 Device Identification And Authentication	Identification and authentication by SAS Key
SC-07 Boundary Protection	Limit access point, default deny, and restrict source adrress
SC-08 Transmission confidentiality/Integrity	TLS encrypted communication
SC-13 Cryptographic Protection	TLS 1.2 and strong ciphers
SA-9 External In formation System	Provisionned in Azure Canadian Region

Azure Key Vault

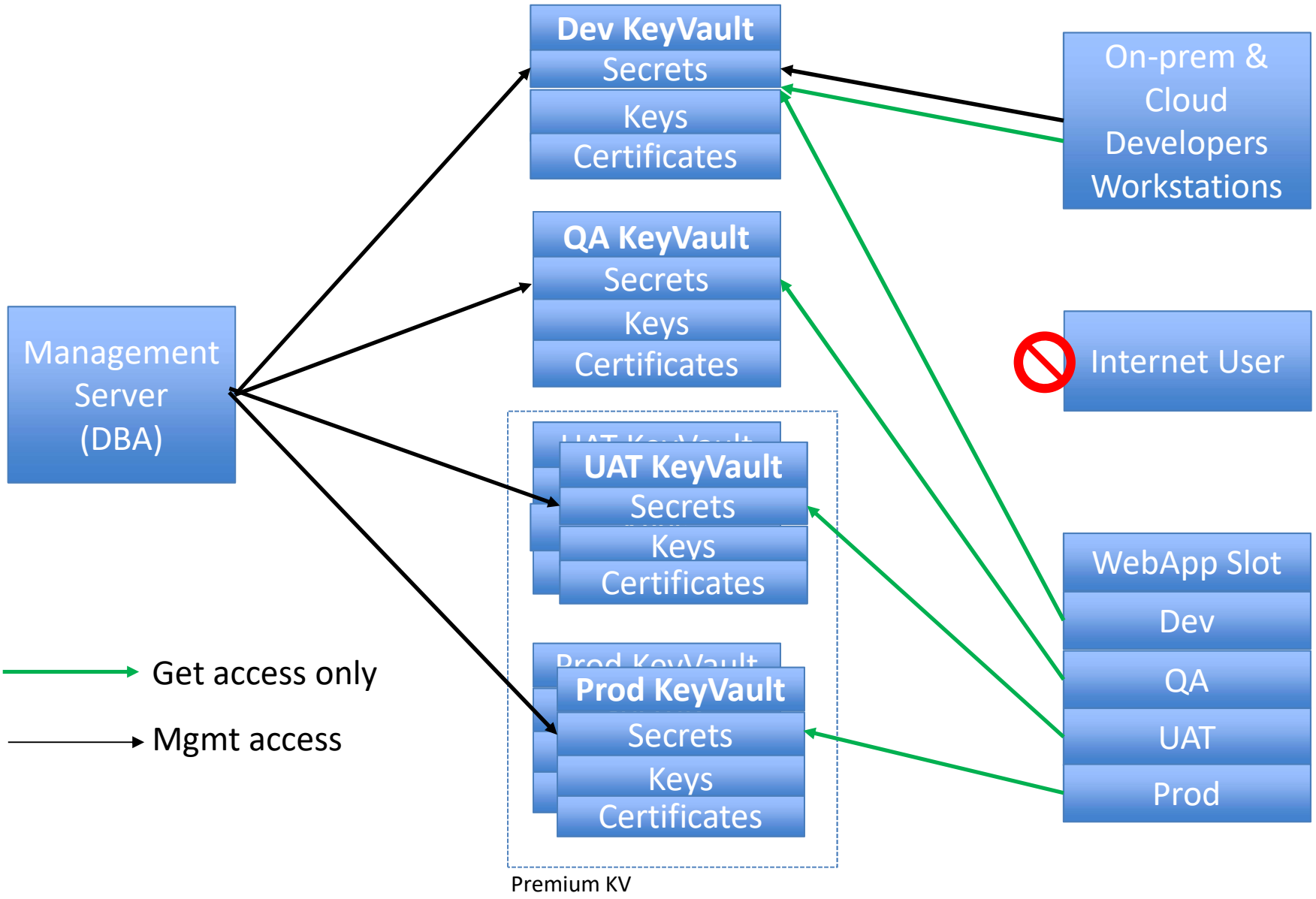
- Avoid embedding secrets in application code and configuration files
- Securely store secrets, keys and certificates
- Leverages premium Keyvault for Production workloads (HSM FIPS 140-2 level 2)
- TLS encrypted connections
- Permissions and access managed through AAD
- Leverages Managed Identity for access to Key Vaukt



Azure Key Vault – Security controls

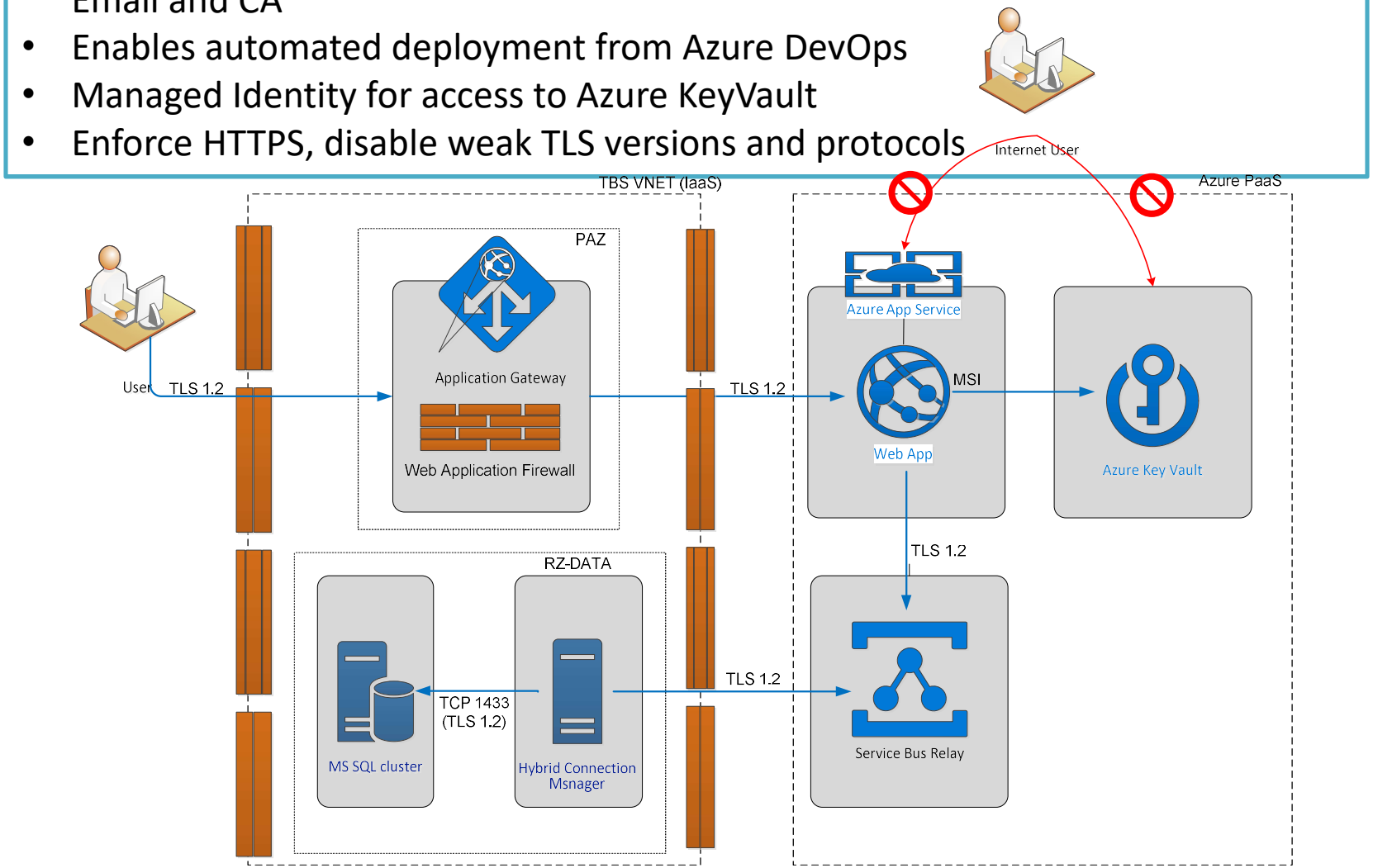
AC-03	Access Enforcement	Grant minimum permissions using RBAC and AAD groups
AC-04	Information Flow Enforcement	Limit access by source address. Use Service Endpoint
AC-06	Least Privilege	Grant minimum required access to keys/secrets based on roles and using KeyVault access policies
SC-07	Boundary Protection	Limit access by source address. Use Service Endpoint.
AU-04	Audit Storage Capacity	Enable collection of diagnosticts to log analytics workspace
AU-06	Audit Review, Analysis and Reporting	Diagnostic logs for Key Vault must be reviewed periodically
AU-12	Audit Review, Analysis and Reporting	Enable collection of diagnosticts to log analytics workspace
SA-09	External Information System	Provisionned in Azure Canadian Region

Azure Key Vault access policies

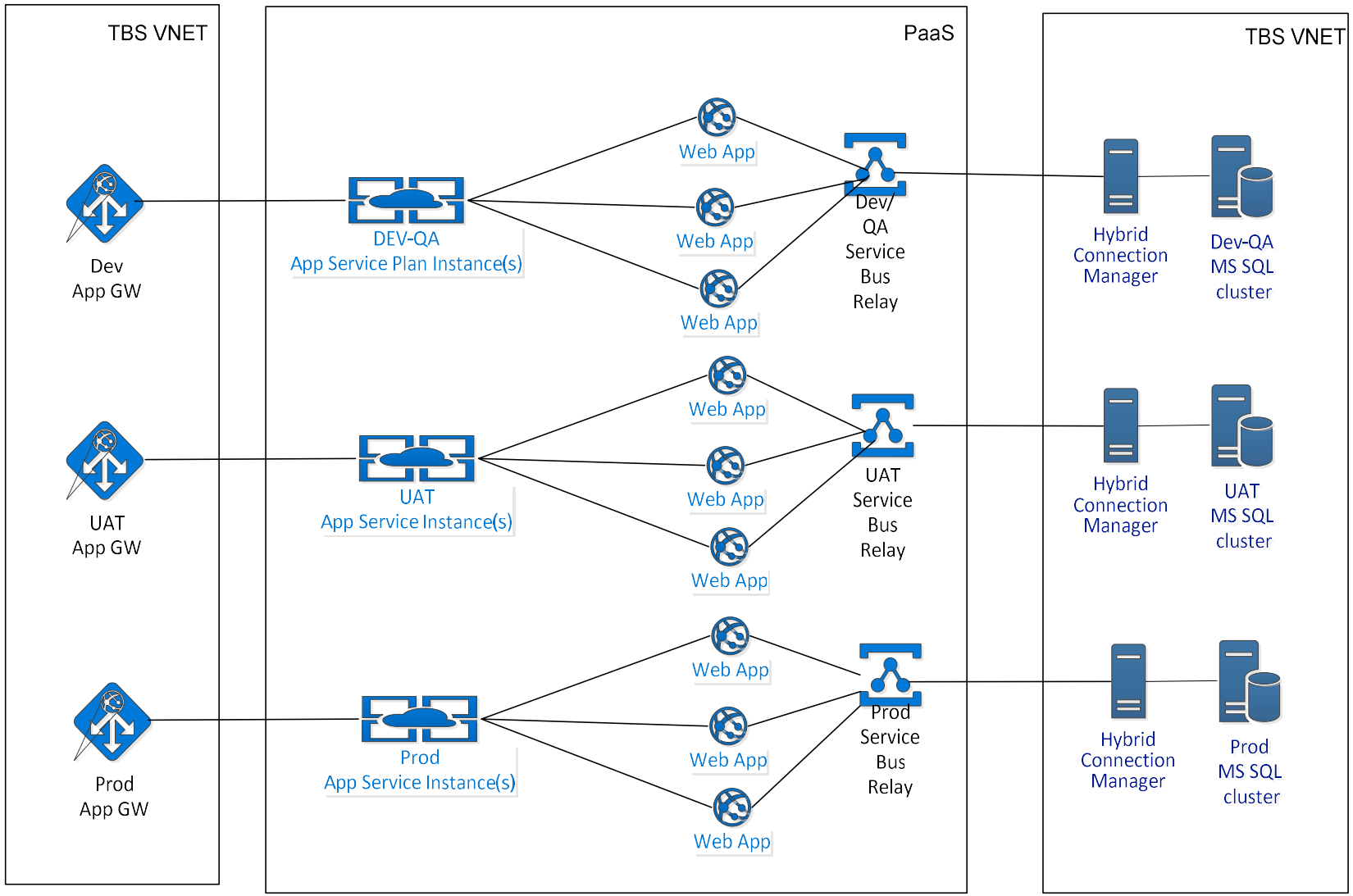


Azure App Service Web Apps

- Leverages the multi-tenant Azure Application Services (PaaS)
- Integration with the TBS IaaS VNET is required to enable connectivity to SQL, Email and CA
- Enables automated deployment from Azure DevOps
- Managed Identity for access to Azure KeyVault
- Enforce HTTPS, disable weak TLS versions and protocols



App Service Instances



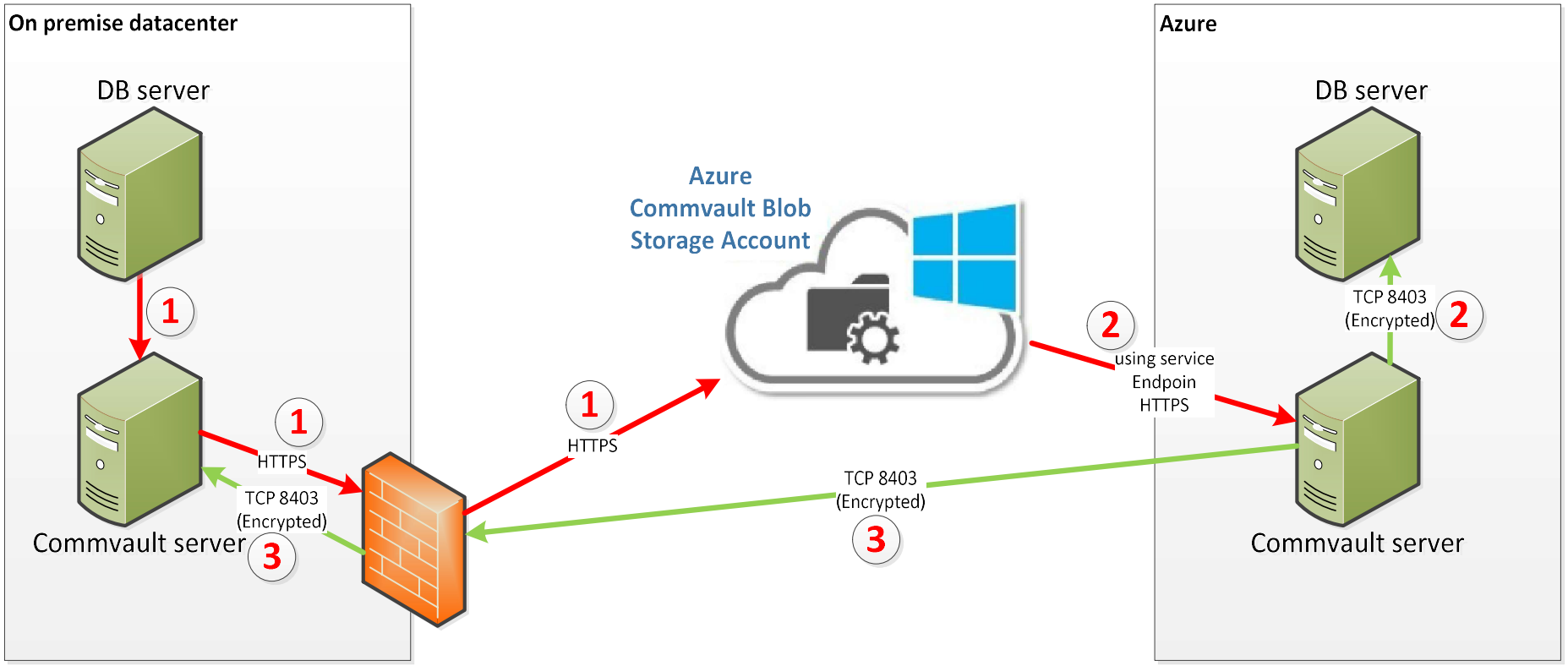
Web App sandbox

- Mitigates the risk of service disruption due to resource contention and depletion (Minimum garantee and service limits)
- Apps may not write to any location in the registry
- File System Restrictions
- Networking Restrictions
  - Apps only accessed via HTTPS (443), and HTTP (8) (if enabled)
  - Connection attempts to local addresses will fail (except within sandbox)
  - Cannot connect to private IPs (will work over Hybrid relay)
  - Restricted connections to outgoing ports (445, 137, 138, and 139)

App Service - Security controls

AC-03	Access Enforcement	Grant Developers access to KUDU in DEV, QA and UAT
AC-04	Information Flow Enforcement	Restrict access to traffic initiated from App Gateway. Disallow remote debugging, FTP
AC-06	Least Privilege	Restrict developer access to App Service instances, KUDU
CM-03	Configuration change control	Perform deployment using ARM templates, configure Azure policies, and limit Service connection scope and roles
CM-07	Least Functionality	Limit HTTP verbs, turn off remote debugging, FTP, Websocket
IA-02	Identification and Authentification	Use Managed Service Identity (MSI) for access to Key Vault
IA-4	Authenticator Management	Store App Service secrets in Key Vault. Publish profile credentials must not be used for deployments
IA-5(2)	Auth. Management – PKI Based Authentication	Use custom domains to protect Web Apps from phishing, session hijacking and other DNS-related attacks.
SC-07	Boundary Protection	Limit access by source address.
SC-08	Transmission Confidentiality & Integrity	Turn on HTTPS only
AU-04	Audit Storage Capacity	Enable collection of diagnostics to log analytics workspace
AU-06	Audit Review, Analysis and Reporting	Diagnostic logs for Web App must be reviewed periodically
AU-02	Auditable Events	Enable detailed error mesage
AU-12	Audit Review, Analysis and Reporting	Enable collection of diagnostics to log analytics workspace
SA-09	External Information System	Provisionned in Azure Canadian Region
SI-02	Flaw Remediation	Ensure last version of .Net is used

Data migration



1. On premise backups are copied to cloud storage account through the Commvault backup server.

2. Cloud backup server reads storage account and restores DB to cloud server.

3. Cloud servers communicate with the on premise backup infrastructure through the cloud backup server.

Identity and authentication

- Authentication for Cloud administration Activity and DevOps is based on Azure AD (ADFS + MFA)
- Azure AD Role-based Access Control enables least privilege access for subscription administration, and Azure Keyvault
- Managed identities for Azure resources to connect to Azure Key Vault
- Service Connections for DevOps deployment (AAD RBAC)
- Multi Factor Authentication (Cloud & DevOps Administrators)

Security and Malware Protection

- Platform level DDoS protection is transparent to the customer. TBS responsible to address DDOS at application layer
- Centralized view of Security state using Security Center, Azure policy and Azure DevOps Kit reports
- Anti-Malware is installed by default on the underlying PaaS virtual machine infrastructure

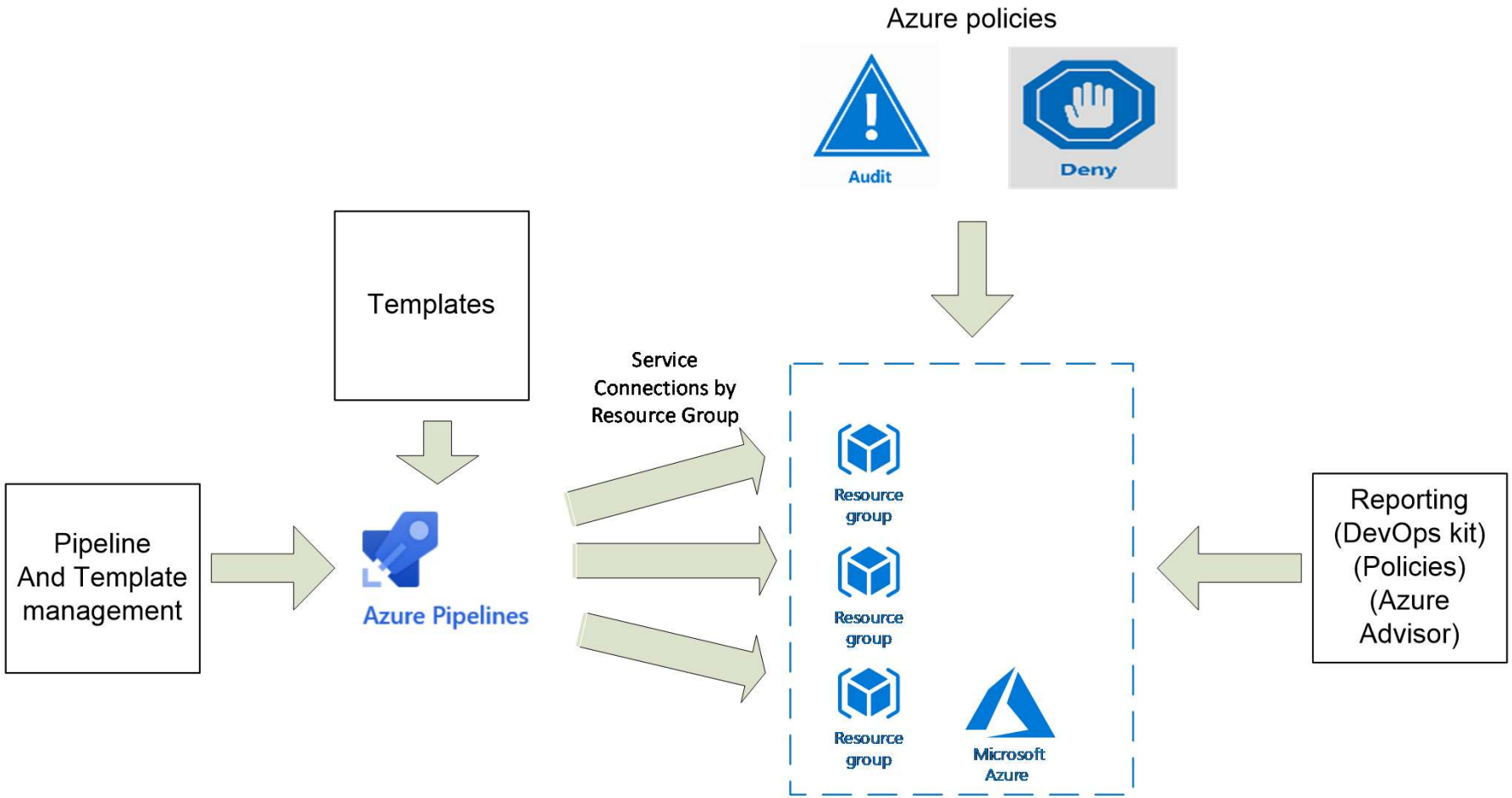
Auditing and monitoring

- Integration with Azure Application Insights to monitor performance
- Diagnostic Logs
- Metric alerts
- Activity logs
- DevOps to log analytics
- SQL assessment
- Azure log analytics

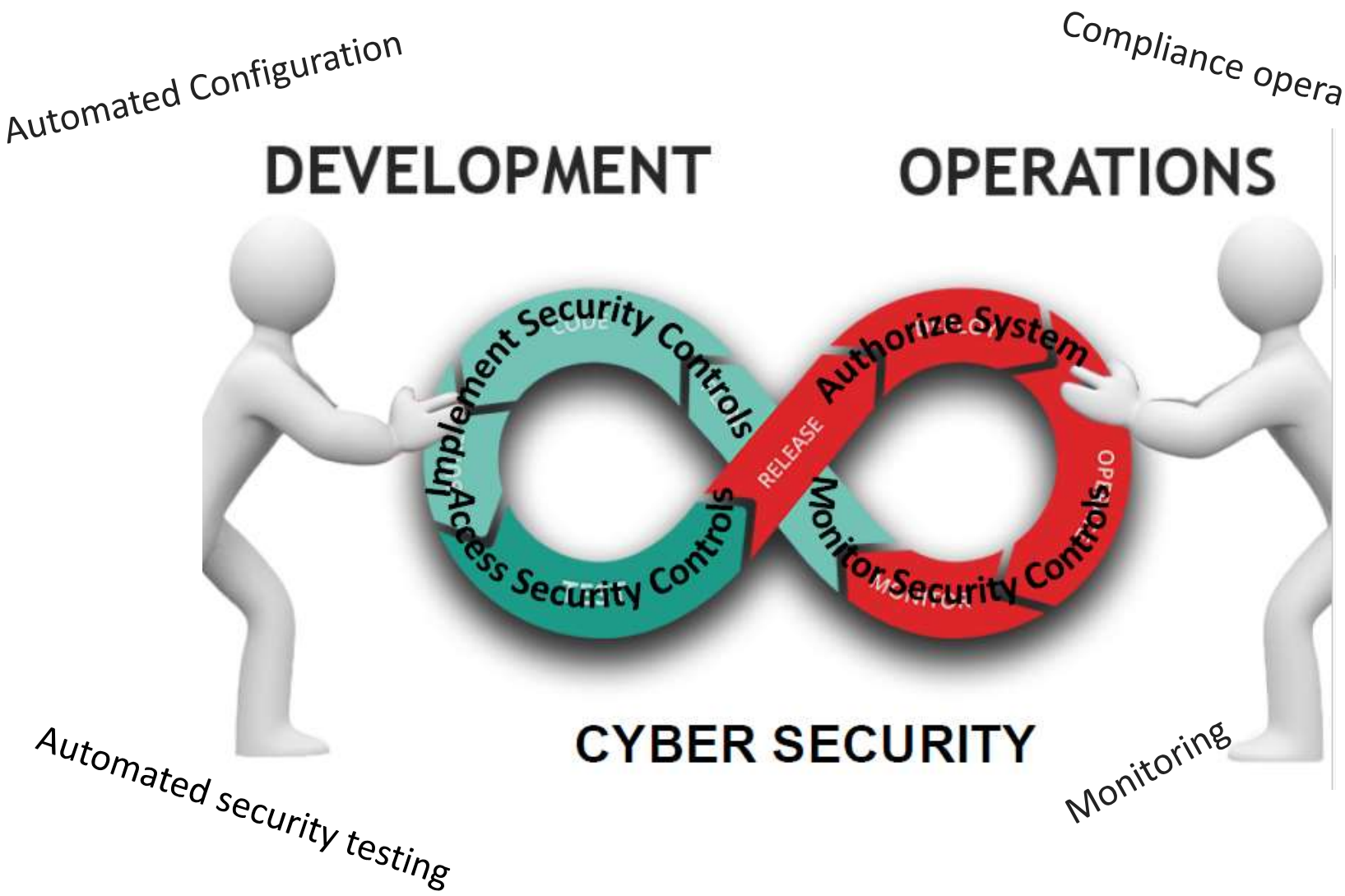
Configuration management

1) ARM templates – ensure resources are created using standard security baseline
2) Azure policies control WHAT can be created, which setting are allowed
3) Service connection – Where resources can be created + access
4) Pipeline security – Controls who can define templates, pipeline
5) Reporting – Azure Resource Kit, Azure Advisor

Service Connections & Pipeline permissions



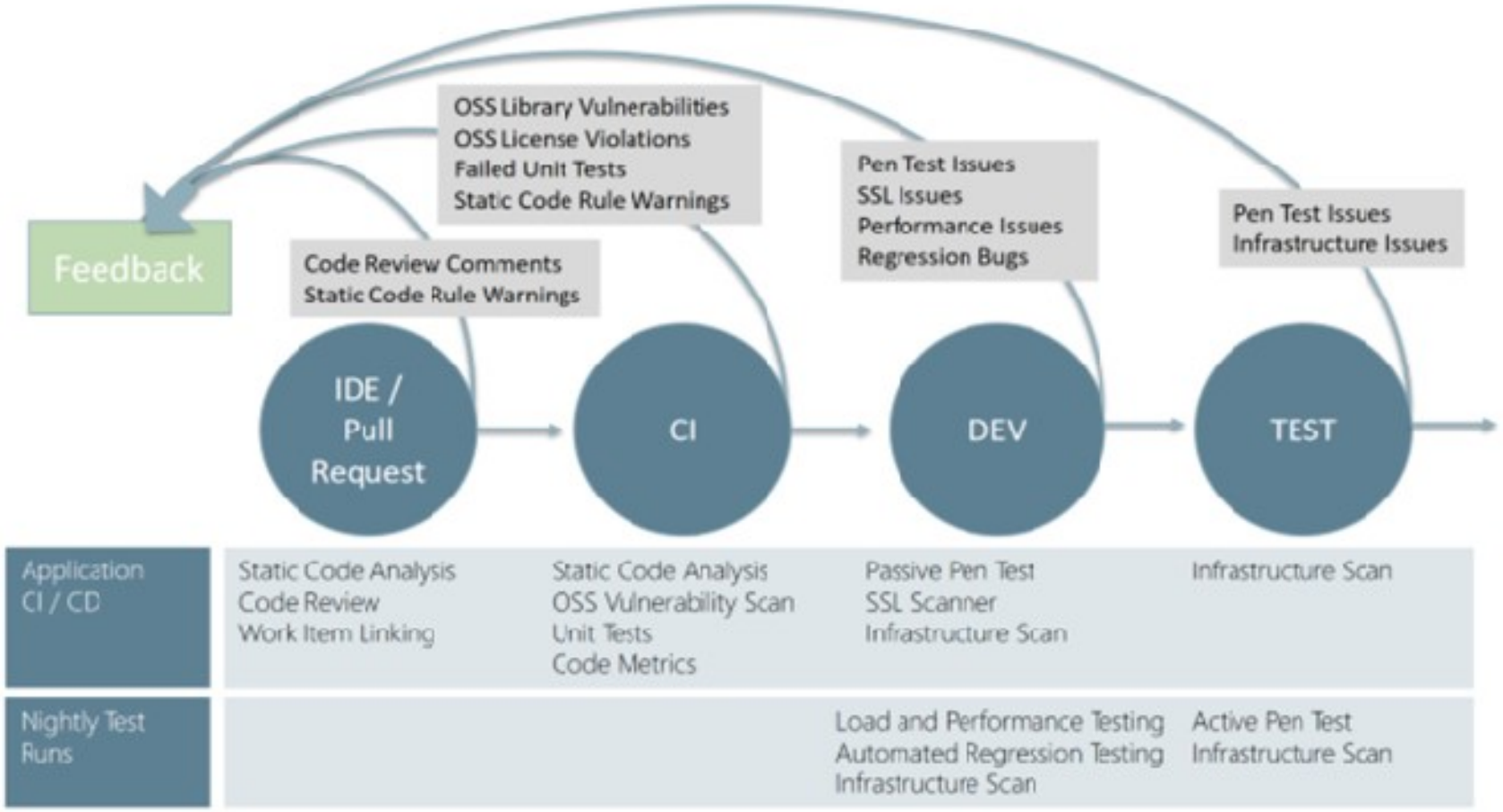
Modernization activities



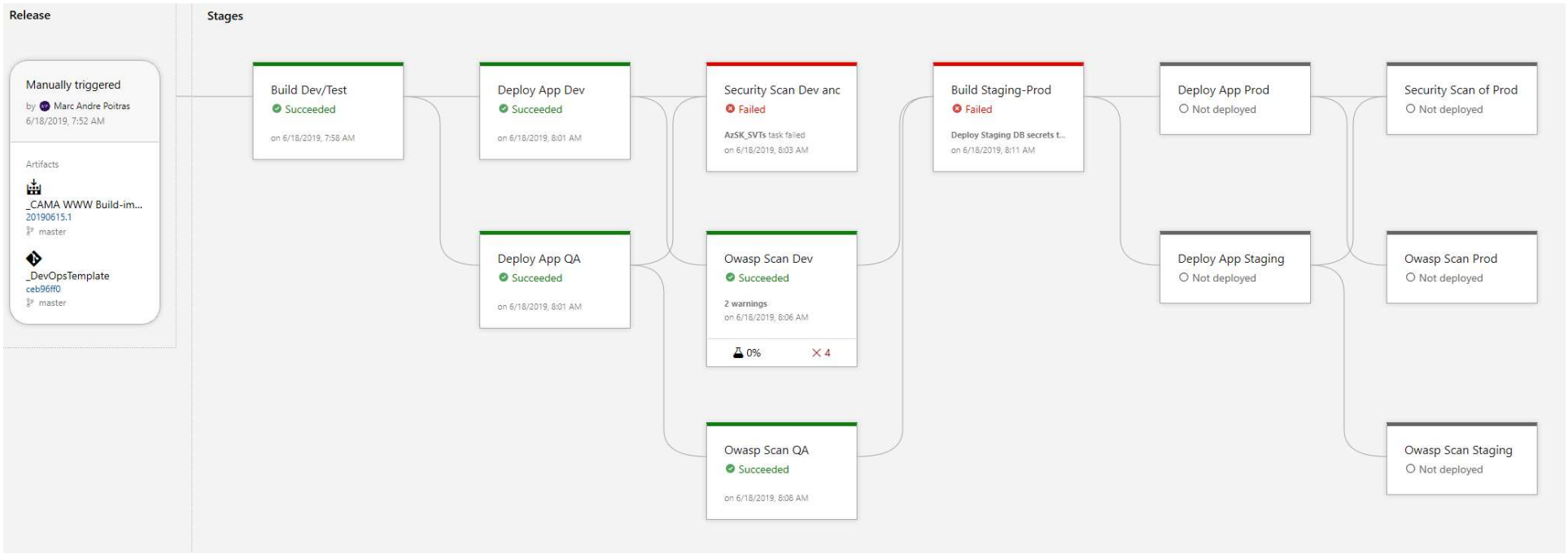
Compliance through automation

Organization	ITPIN Compliant	Enforces HTTPS	HSTS	Free of known weak protocols and ciphers	Uses approved certificates
Treasury Board of Canada Secretariat Show 14 domains	100%	100%	100%	100%	100%

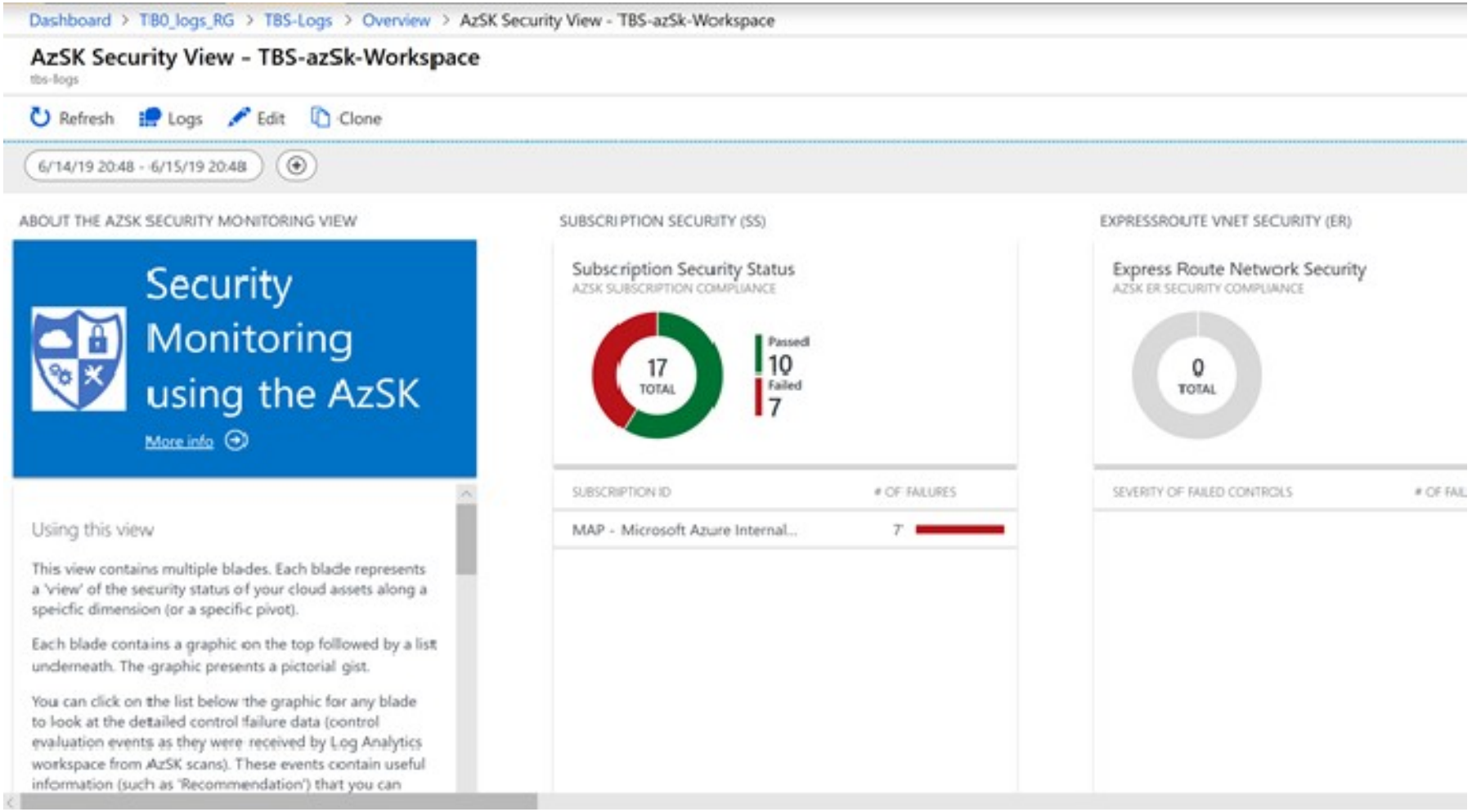
Azure DevOps



TBS Deployment Pipeline



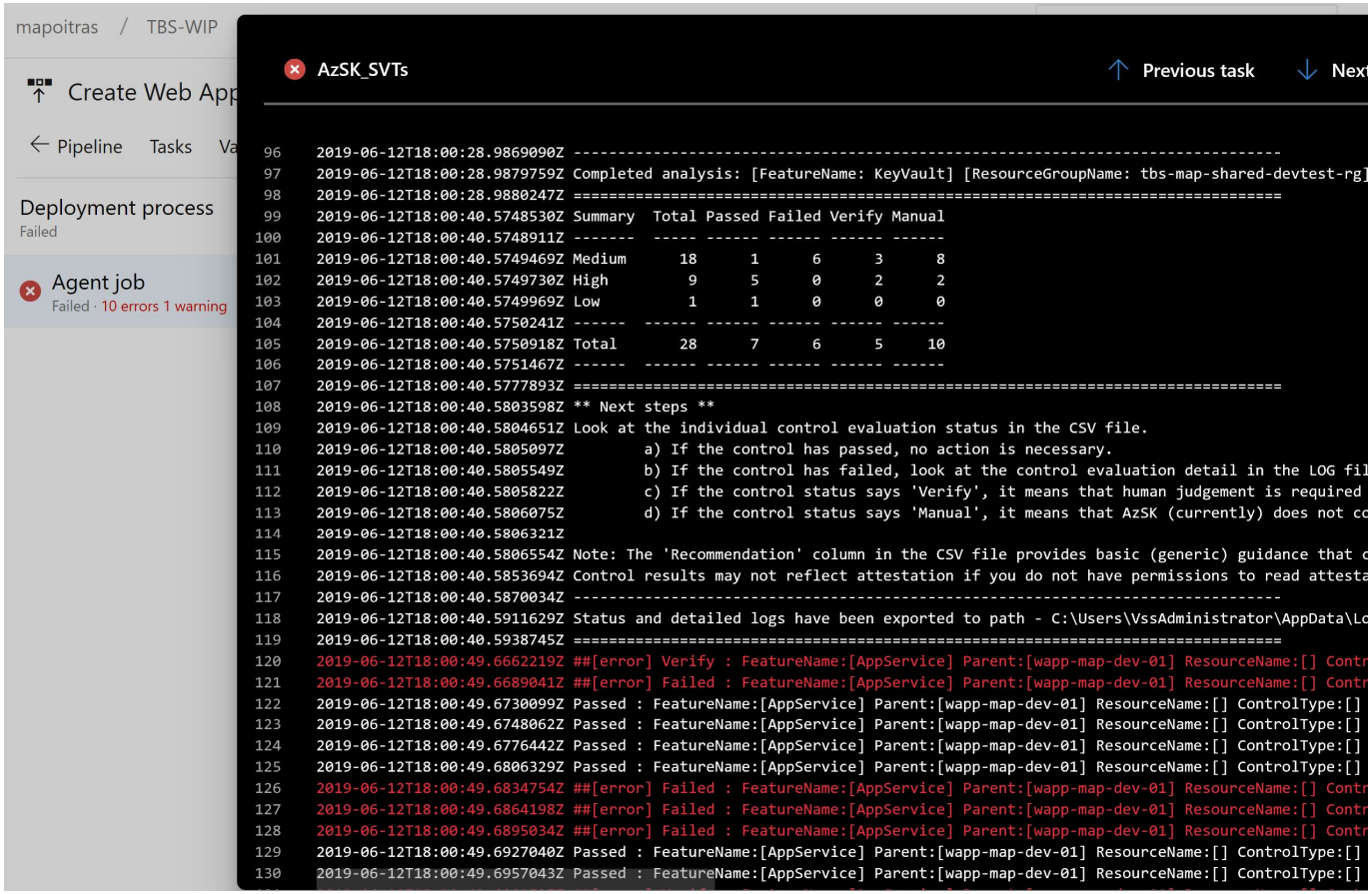
Secure DevOps Kit for Azure



Secure DevOps Kit for Azure

Description	ActualStatu
AA-031 - Related Controls[AC-2(7), AC-6] - All users/identities must be granted minimum required permissions using Role Based Access Control (RBAC)	Verify
AA-007 - Related Controls[IA-5(2)] - Custom domain with SSL binding must be configured for App Service	Failed
AA-003 - Related Controls[AC-4, CM7] - Remote debugging must be turned off for App Service	Passed
AS-004 - Related Controls[AC-4, CM7] - Web Sockets should be disabled for App Service	Passed
AA-022 - Related Controls[SC-6] - 'Always On' should be configured for App Service	Passed
AA-023 - Related Controls[SI-2] - The latest version of .NET framework version should be used for App Service	Passed
AA-025 - Related Controls[CP-10(5)] - App Service must be deployed on a minimum of two instances to ensure availability	Failed
AA-006 - Related Controls[CP-9] - Backup feature must be configured to backup data for App Service	Failed
AA-010 - Related Controls[AU-12] - Auditing and Monitoring must be enabled for App Service	Failed
AA-027 - Related Controls[SC-8] - App Service must only be accessible over HTTPS	Passed
AA-028 - Related Controls[AC-6] - WEBSITE_LOAD_CERTIFICATES parameter must not be set to "*" (i.e. all) for App Service	Passed

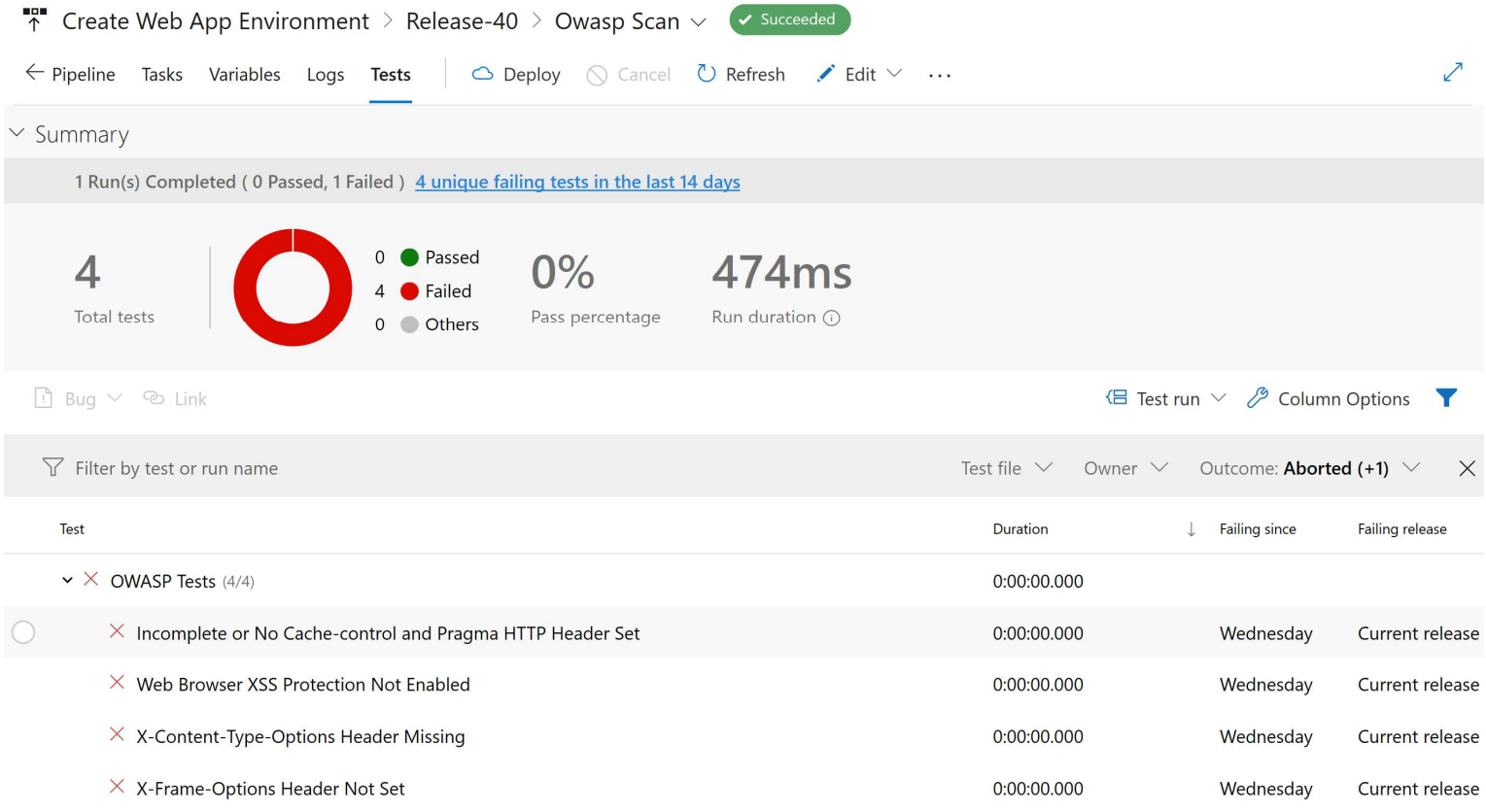
Secure DevOps Kit for Azure - Recommendations



Secure DevOps Kit for Azure - Exceptions

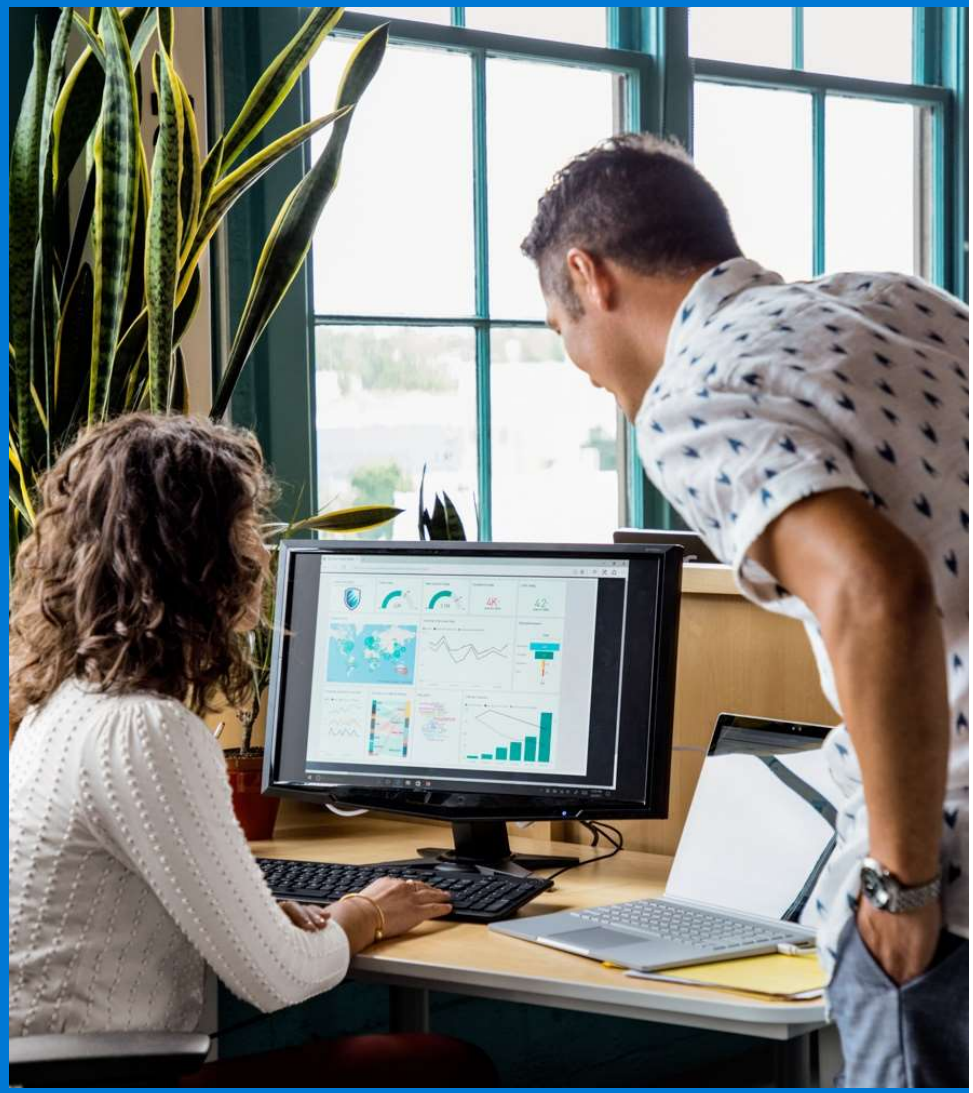
ActualStatus	AttestedSubStatus	AttestationExpiryDate	AttestedBy	AttesterJustification	F
Verify	NotAnIssue	9/11/2019	mapoitra@microsoft.com	Verified	F
Failed	NotAnIssue	9/15/2019	mapoitra@microsoft.com	I verified	C
Passed					C
Passed					F
Passed					C
Passed					F
Failed	WillNotFix	8/12/2019	mapoitra@microsoft.com	Not Needed	F
Failed	NotAnIssue	9/15/2019	mapoitra@microsoft.com	Not required for this application	F

OWASP ZAP


Create Web App Environment
Release-40
Owasp Scan
Succeeded
Pipeline
Tasks
Variables
Logs
Tests
Deploy
Cancel
Refresh
Edit
Summary
1 Run(s) Completed (0 Passed, 1 Failed)
4 unique failing tests in the last 14 days
4
Total tests
0 Passed
4 Failed
0 Others
0%
Pass percentage
474ms
Run duration
Bug
Link
Test run
Column Options
Filter by test or run name
Test file
Owner
Outcome: Aborted (+1)
Test
Duration
Failing since
Failing release
OWASP Tests (4/4)
0:00:00.000
Incomplete or No Cache-control and Pragma HTTP Header Set
0:00:00.000
Wednesday
Current release
Web Browser XSS Protection Not Enabled
0:00:00.000
Wednesday
Current release
X-Content-Type-Options Header Missing
0:00:00.000
Wednesday
Current release
X-Frame-Options Header Not Set
0:00:00.000
Wednesday
Current release

Azure App Service

Create powerful web apps
using a fully-managed cloud platform



Cloud application hosting continuum

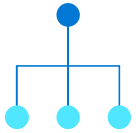
IaaS	CaaS	PaaS	FaaS
Infrastructure Platform	Container Platform	Application Platform	Serverless Platform
Challenges			
Patching, Management, Deployment	Management (Container & Pod)	Limitations of Execution environment	Cold start, long running process
What you get			
Curated VM Hosting	Curated Orchestration	Curated Execution Environment	Scale to 'zero'
Technology decisions			
IT/Infra focused Value Prop		Dev/App Admin focused Value Prop	

More Control of execution environment — **Less Control** of execution environment

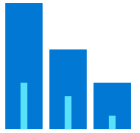
Less Agile development & deployment — **More Agile** development & deployment

Azure App Service capabilities

High-productivity for both devs & ops



Fully-managed



Enterprise-grade

Azure App Service benefits

High-productivity for devs & ops

- .NET, Node, Java, Docker, PHP, Ruby, Python
- Deploy containers on Windows & Linux
- Staging & deployment
- Testing in production
- App gallery marketplace

Fully-managed

- Auto scale & load balancing
- High availability w/auto patching
- Reduced operations costs
- Backup & recovery

Enterprise-grade

- Global data center footprint
- Hybrid support
- Azure Active Directory integration
- Secure & compliance

Migrate your way

Use the code, container, or OS of your choice on Azure App Service, our fully-managed platform

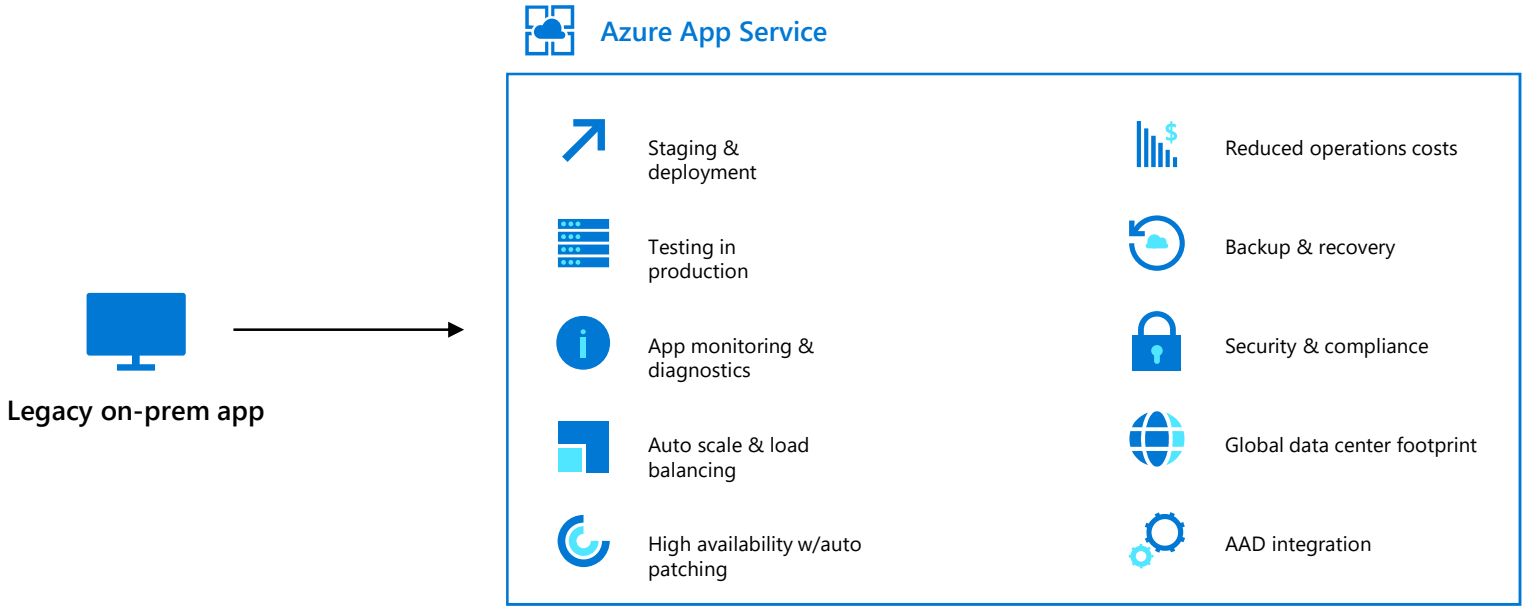
Code

Container

OS

Evolve by migrating

Migrated existing apps enjoy all the management and integration benefits of the Azure App Service platform



► Learn more about Azure App Service

Enable new opportunities for app modernization

Easily deploy & run container-based web apps at scale

Developer productivity

Tight integration w/ Docker Hub, Azure Container Registry

Built-in CI/CD w/ Deployment Slots

Intelligent diagnostics & troubleshooting, remote debugging

Fully managed platform

Scaling and load balancing

High availability w/ auto-patching

Backup & recovery

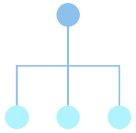
Flexibility & choices

From CLI, portal, or ARM template

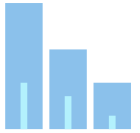
Single Docker image, multi container w/ Docker compose, or Kubernetes Pod Definition

IntelliJ, Jenkin, Maven, Visual Studio family

High-productivity
for both devs & ops



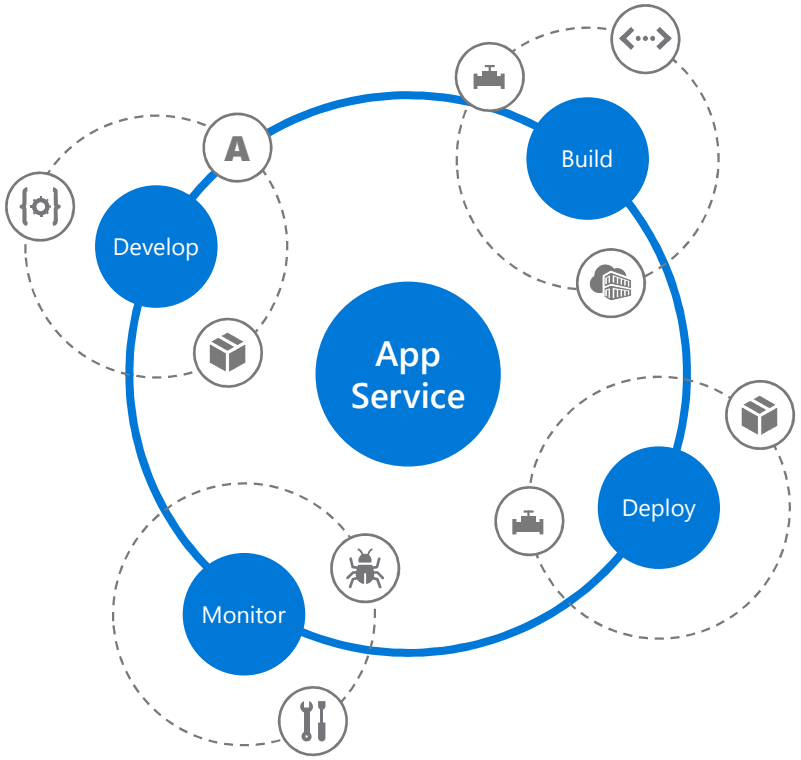
Fully-managed



Enterprise-grade

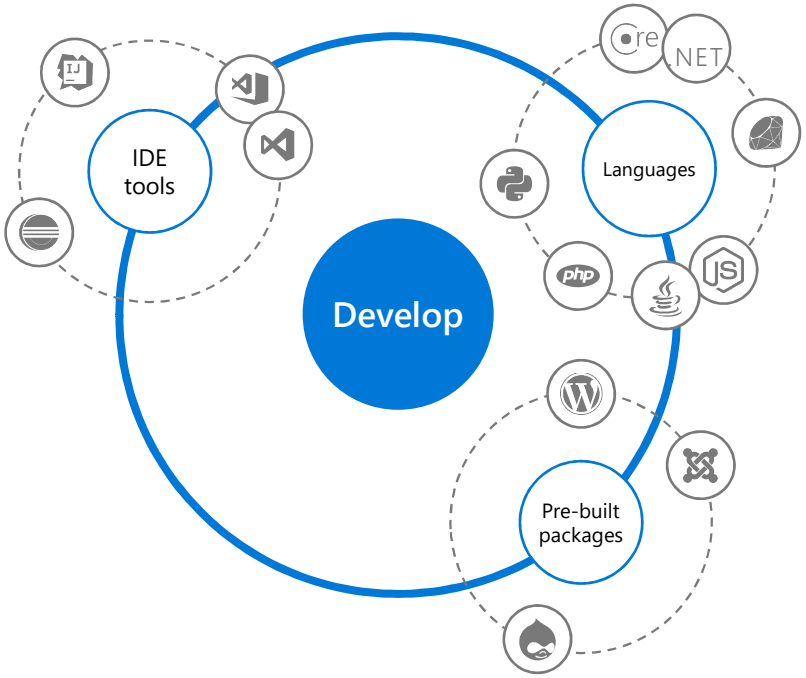
High productivity

Your choice of languages, pre-built packages, and tools



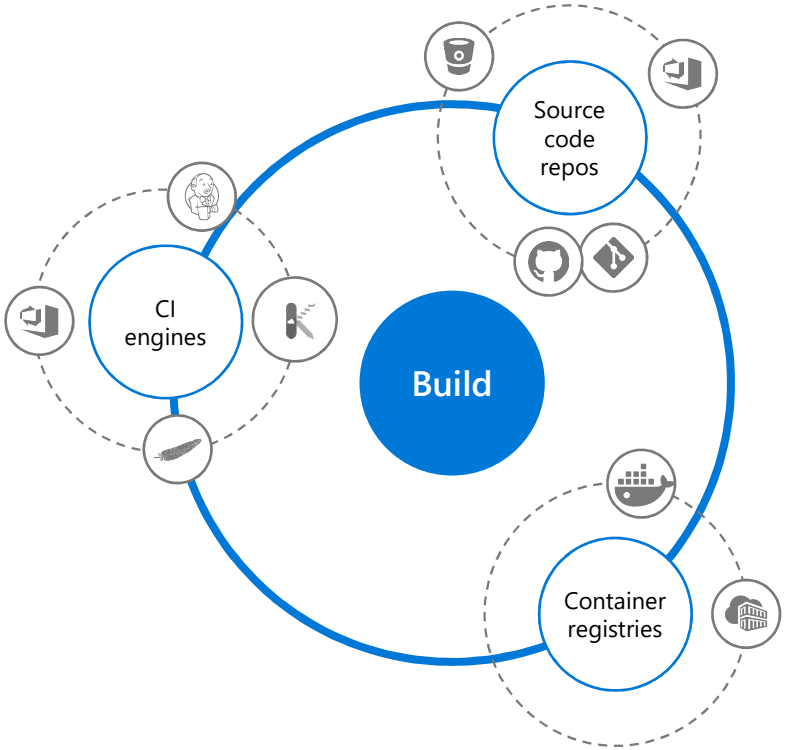
Develop

Choose your IDE tools, languages, and pre-built packages



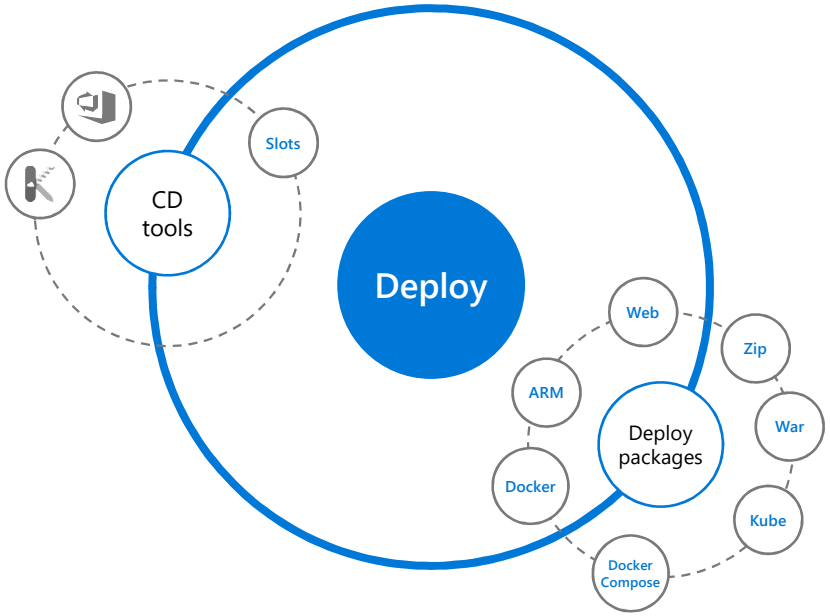
Build

Your choice of CI engines, source code repositories, and container registries



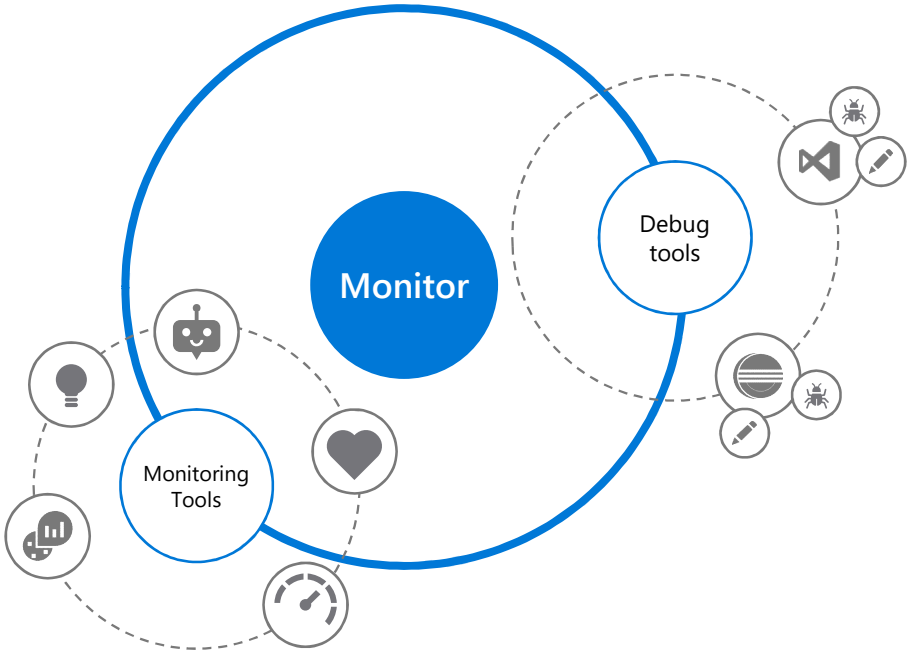
Deploy

Use Docker to Kube packages and CD tools like slots to increase your productivity

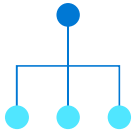


Monitor

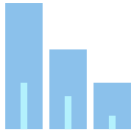
Choose your monitoring and debugging tools



High-productivity for both devs & ops



Fully-managed



Enterprise-grade

Start with the basics

Focus on your business logic, we'll handle the rest

Auto-scale &
load balancing

High availability
with auto patching

Reduced
operations costs

Backup &
recovery

App Service Differentiation

Benefits of App Service for . Developers

High productivity

Live production debugging with Visual Studio Snapshot Debugger

App telemetry, anomaly detection, and site diagnostics with App Insights

Site staging slots

Automatic OS and framework patching

Continuous integration/deployment with Git, Visual Studio, Docker Hub, and GitHub

Site extensions support & gallery

Auto-healing

Logging and auditing

Admin-site

Fully managed

Automated deployment

AutoScale

Built-in load balancing

WW datacenter coverage

End point monitoring and alerts

App gallery

DR site support

WildCard support

Dedicated IP address

HTTP compression

CDN support for websites

App Services Environments

Enterprise grade

Hybrid connections/VPN support

Scheduled backup

Azure Active Directory Integration

Site resiliency, HA, and DR

Web jobs

Role base access control

Audit/compliance

Enterprise migration

Client certs

Cache

IP restrictions/SSL

Web sockets

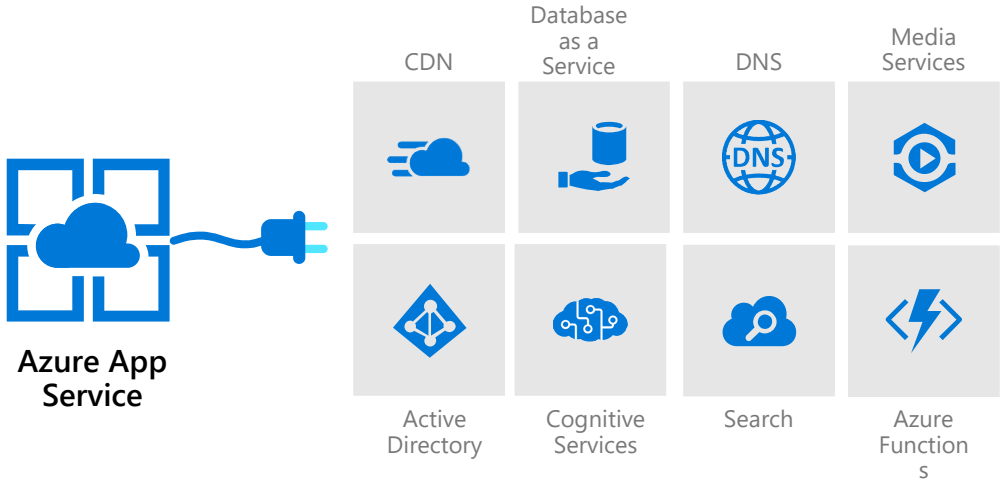
SQL, MySQL, CosmosDB

Sticky sessions

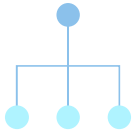
Authorization/authentication

Easily extend your application's capabilities

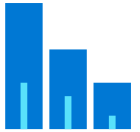
Connect to other managed services to meet specific web app needs



High-productivity
for devs & ops



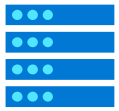
Fully-managed



Enterprise-grade

Enjoy full-service support

Worldwide services with full support: anytime, anywhere



54 data centers worldwide
2 data centers in Canada

Industry-verified compliance

Managed Service Identity support

Azure Active Directory integration

Azure Virtual Network integration

Hybrid support

Secure & compliance

Choose your hosting options

Our selection of hosting options give you the control you want

Azure App Service (multi-tenant)

Get your Web, API, or Mobile App created in seconds in the cloud. We provide the plumbing, you provide the application code or container(s).

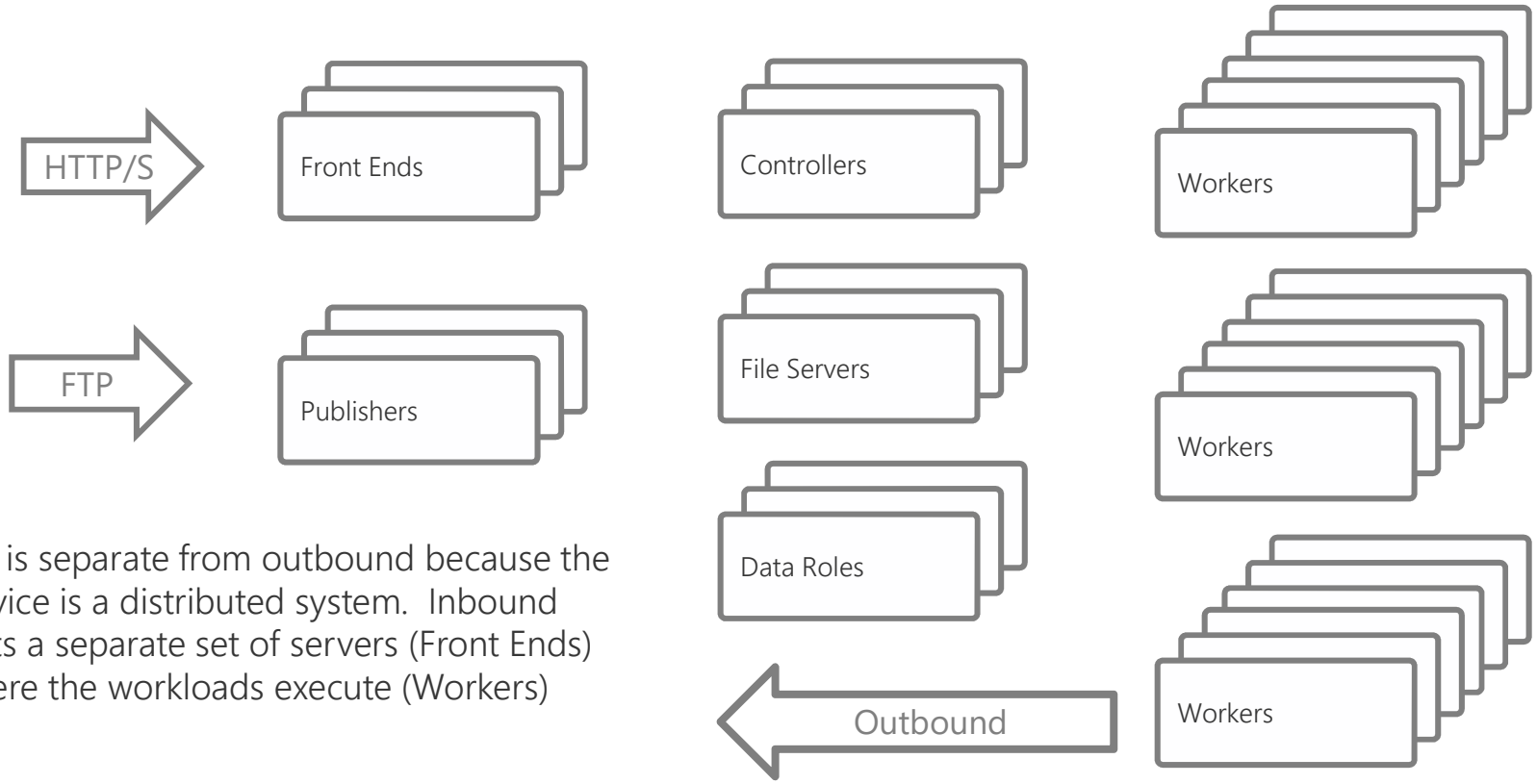
App Service Environment

Run your apps in virtual network at high scale. Create an isolated environment specifically for your organization and access/manage all of the resources behind your public endpoint.

Azure Stack

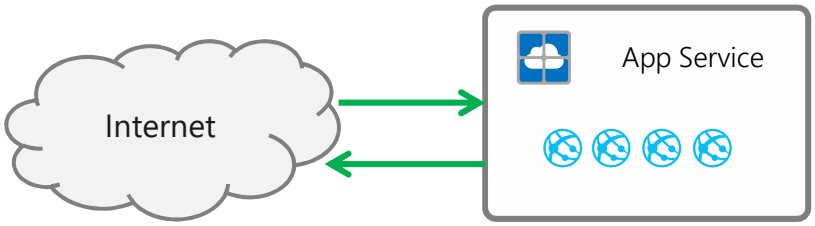
Leverage cloud innovations in on-premises infrastructure. Azure App Service on Azure Stack brings the power of Azure App Service to your own data centers.

Behind the scene – App Services



Inbound is separate from outbound because the App Service is a distributed system. Inbound traffic hits a separate set of servers (Front Ends) than where the workloads execute (Workers)

Default behavior

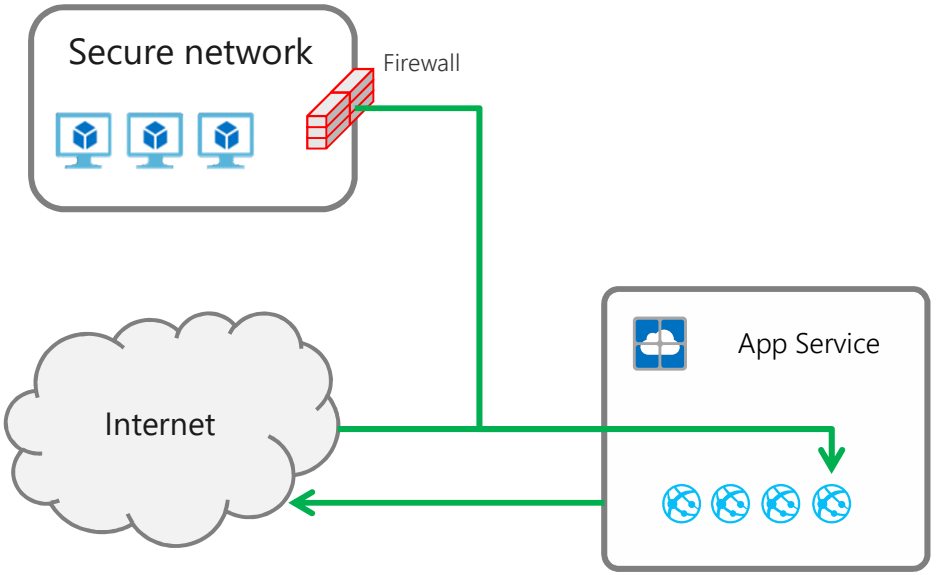


Inbound traffic to your app hits an IP address that is shared with the other apps.

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

App Assigned Address

Scenario: Security requirements require locking down access to an address that isn't shared



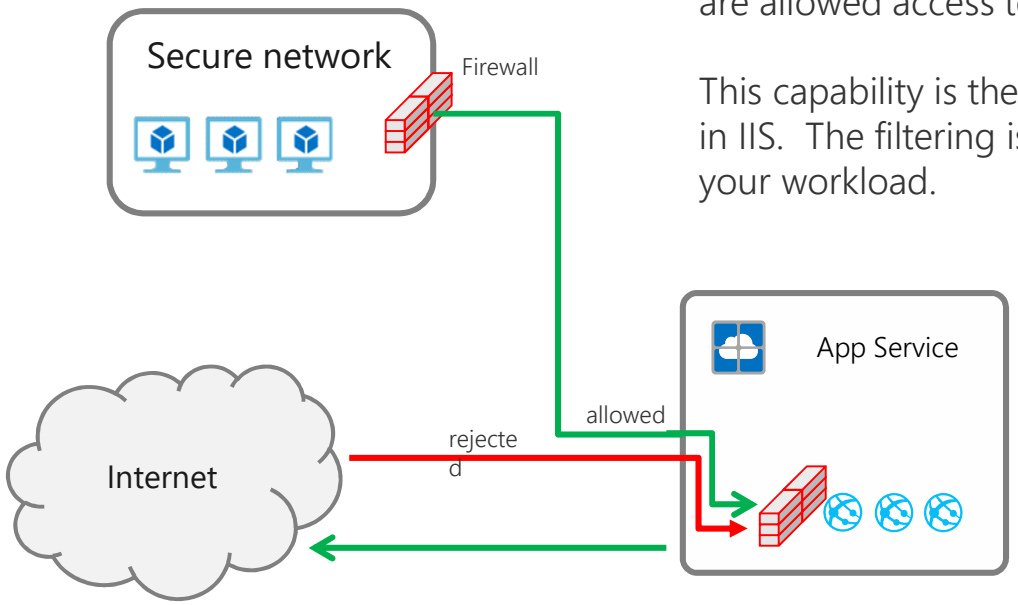
Your app has a dedicated IP address that is used for inbound traffic

This is configured when you set up IP based SSL with your application.

At this point your app is still accessible from the internet

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.



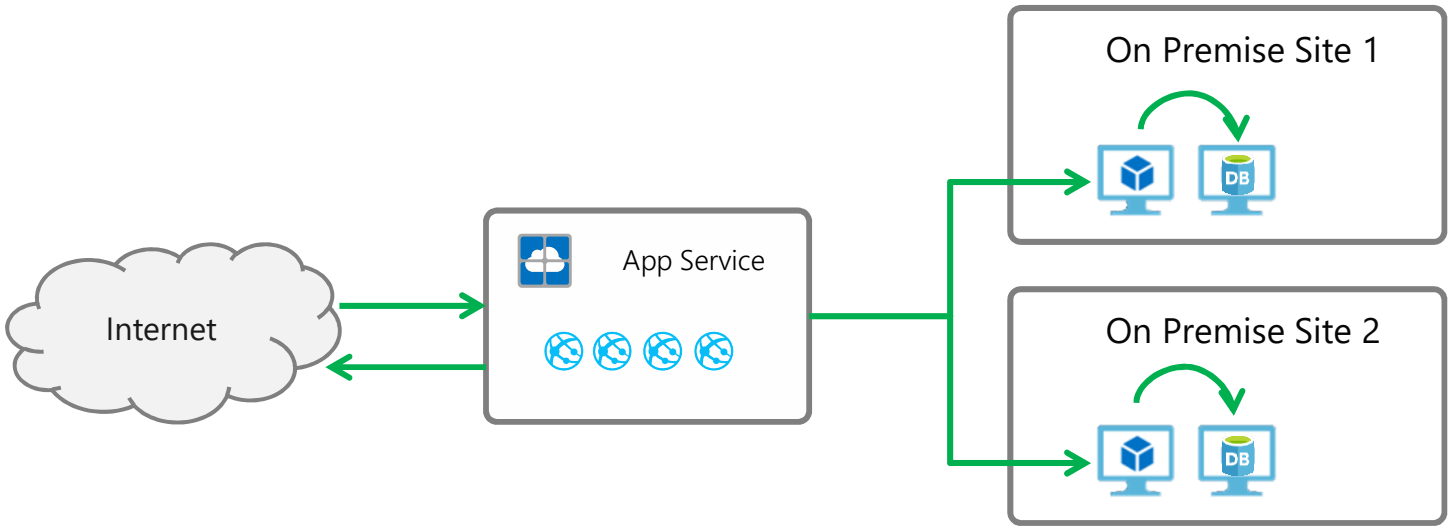
This capability allows you to define a set of IP ranges that are allowed access to your app.

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

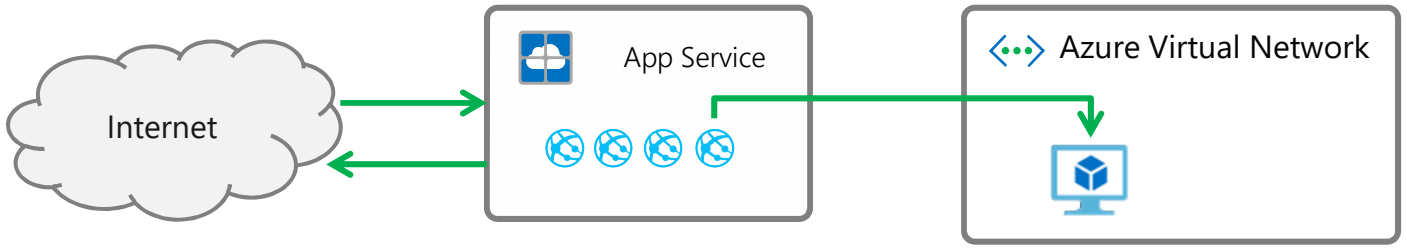
Scenario: Access into networks lacking a VPN to Azure
Examples: Access on premise databases

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



Old 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 Environment (ASE)

Some scenarios:

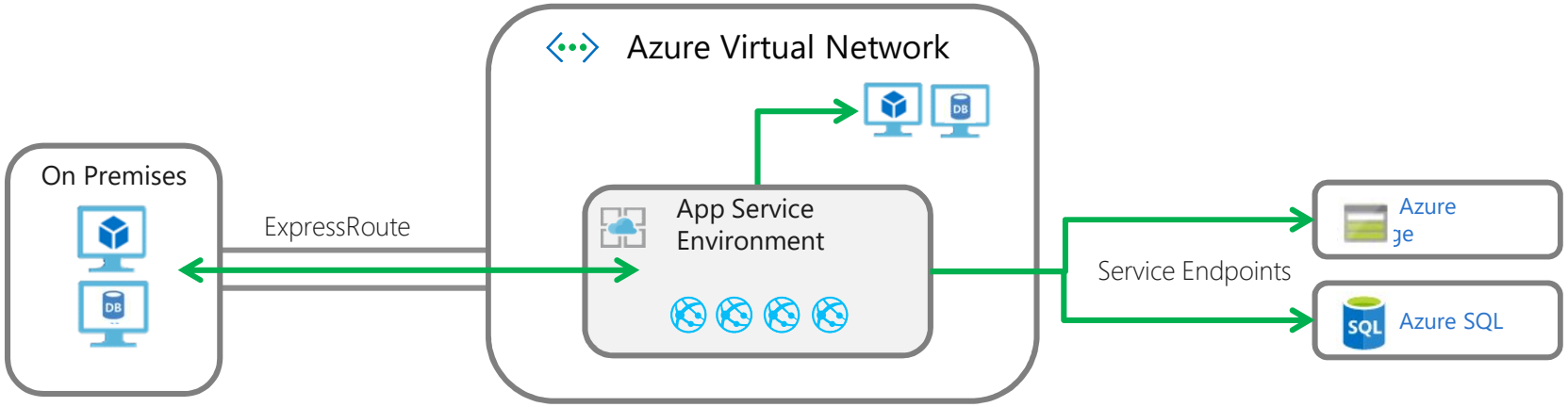
- Security and compliance applications
  - Numerous PCI and HIPPA applications run on ASE because it is single tenant and provides a measure of network isolation and access control.
- Line of business application hosting
  - For example, Microsoft hosts hundreds of internal apps and sites on ASE
- Large scale secure multi-tier applications
  - Large scale marketing campaigns
- Access resources across ExpressRoute or Service Endpoints
  - App Service today lacks alternative features to access resources across ExpressRoute or Service Endpoints

App Service Environment (ASE)

Scenario: Access resources in your Azure VNet

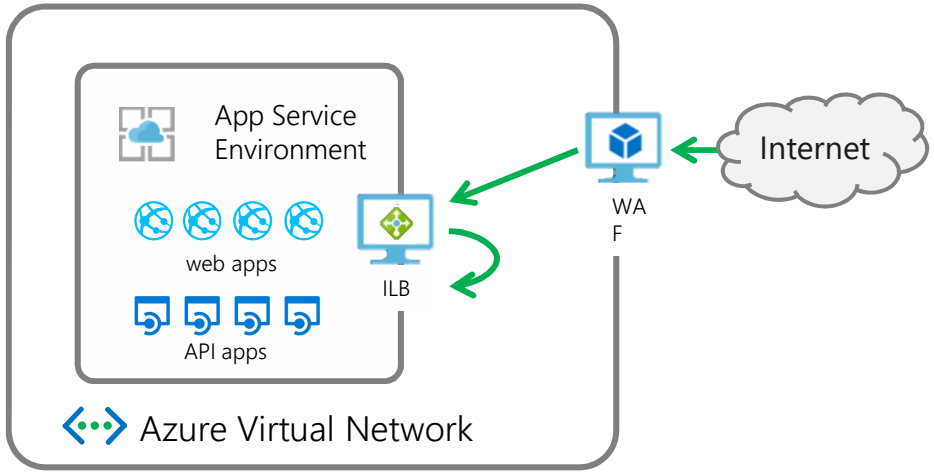
Example: Line of business sales application that is on a private IP address and uses SQL and Storage

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.



ILB App Service Environment (ASE) with WAF

Scenario: Access resources in your Azure VNet
Example: Line of business sales application that is on a private IP address



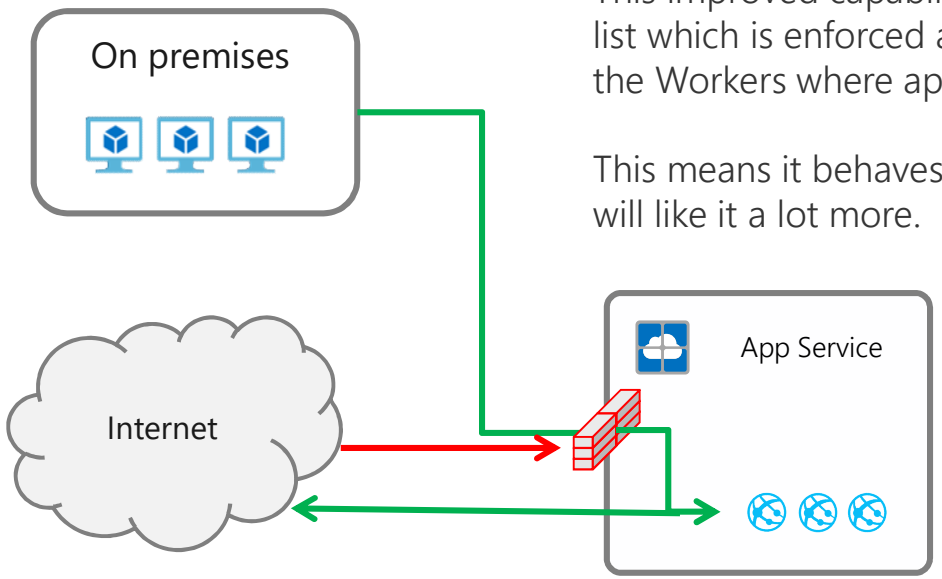
Expose your front end apps through a Web Application Firewall (WAF) for application security.

Host your second tier API applications on the same ILB ASE but do not expose them to the internet through the WAF.

Because the traffic between the web and API apps stays in the VNet it you have a secure multi-tier hosting platform that only exposes what you want.

IP Restrictions (new and improved)

Scenario: Restrict access to your app in a way that security teams will approve



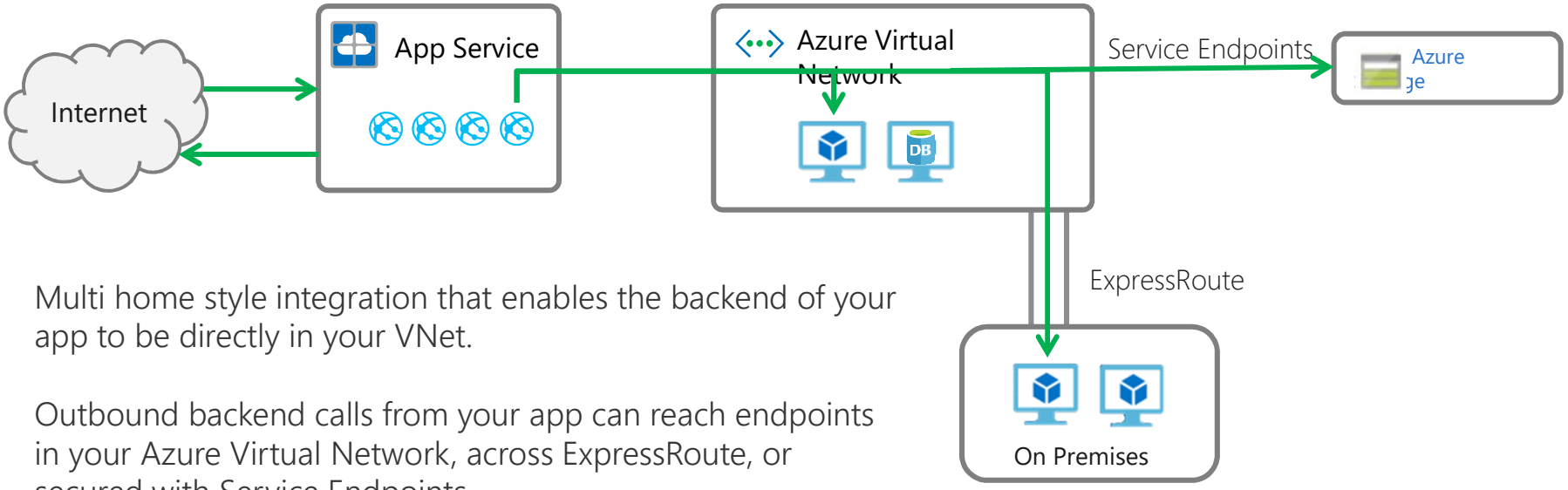
This improved capability enables you to define an allow/deny list which is enforced at the Front Ends which are upstream from the Workers where apps run.

This means it behaves like a network ACL and security groups will like it a lot more.

New features in work

New VNet Integration (In Preview)

Scenario: App access to resources in your VNet, across Service Endpoints and across ExpressRoute

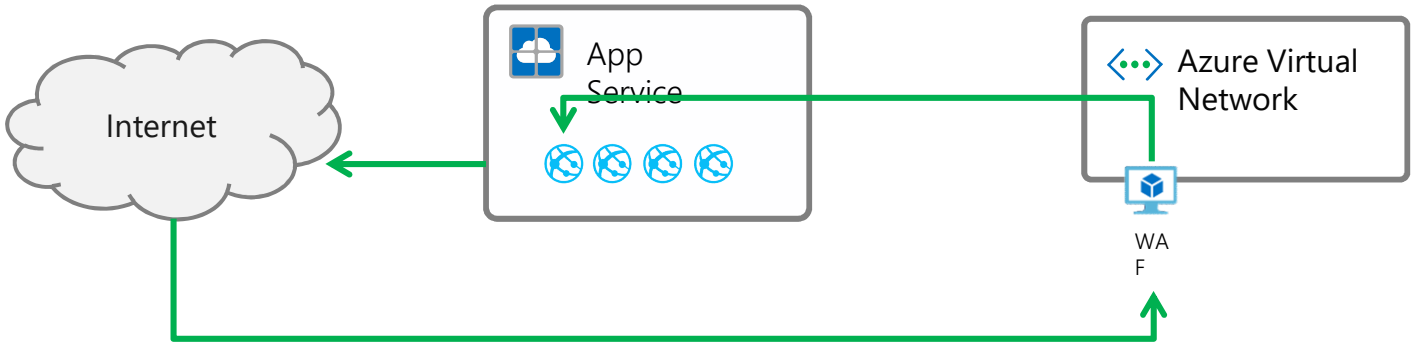


Multi home style integration that enables the backend of your app to be directly in your VNet.

Outbound backend calls from your app can reach endpoints in your Azure Virtual Network, across ExpressRoute, or secured with Service Endpoints.

Service Endpoint Integration: public IP (In Preview)

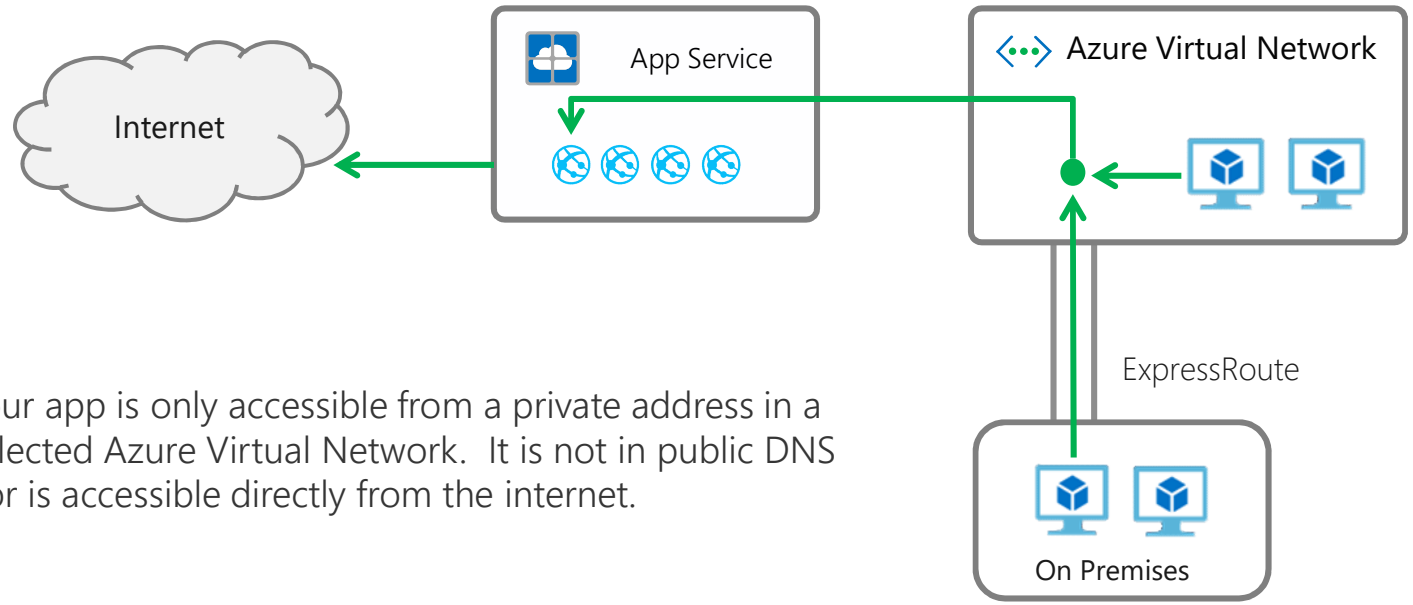
Scenario: Lock down access to your app to only coming from your VNets
Example: Restrict access to an app to only coming from a WAF in your VNet



Inbound calls to your app are restricted to only coming from a set of VNets/subnets. The endpoint is still a shared public IP address for App Service. The DNS name is public but the app is not accessible from the internet

Service Endpoint Integration: private IP

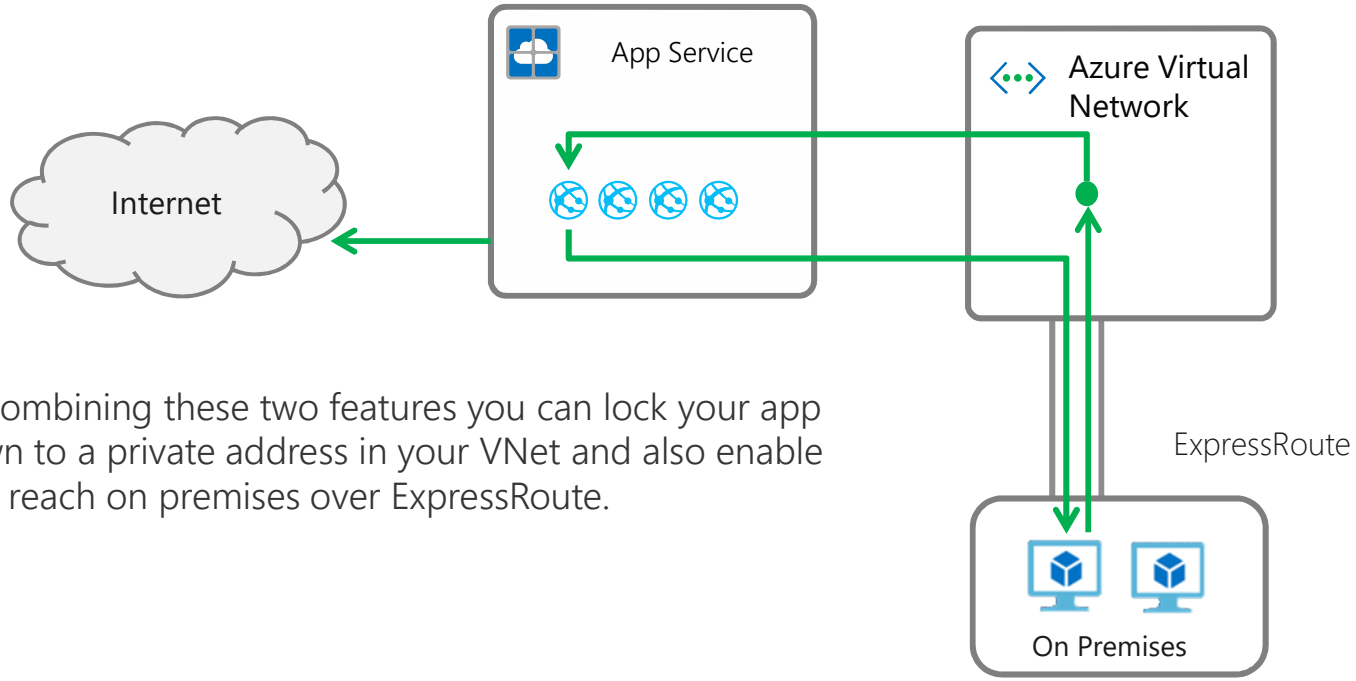
Scenario: Private IP address assignment to an app
Example: Line of business application hosting



Your app is only accessible from a private address in a selected Azure Virtual Network. It is not in public DNS nor is accessible directly from the internet.

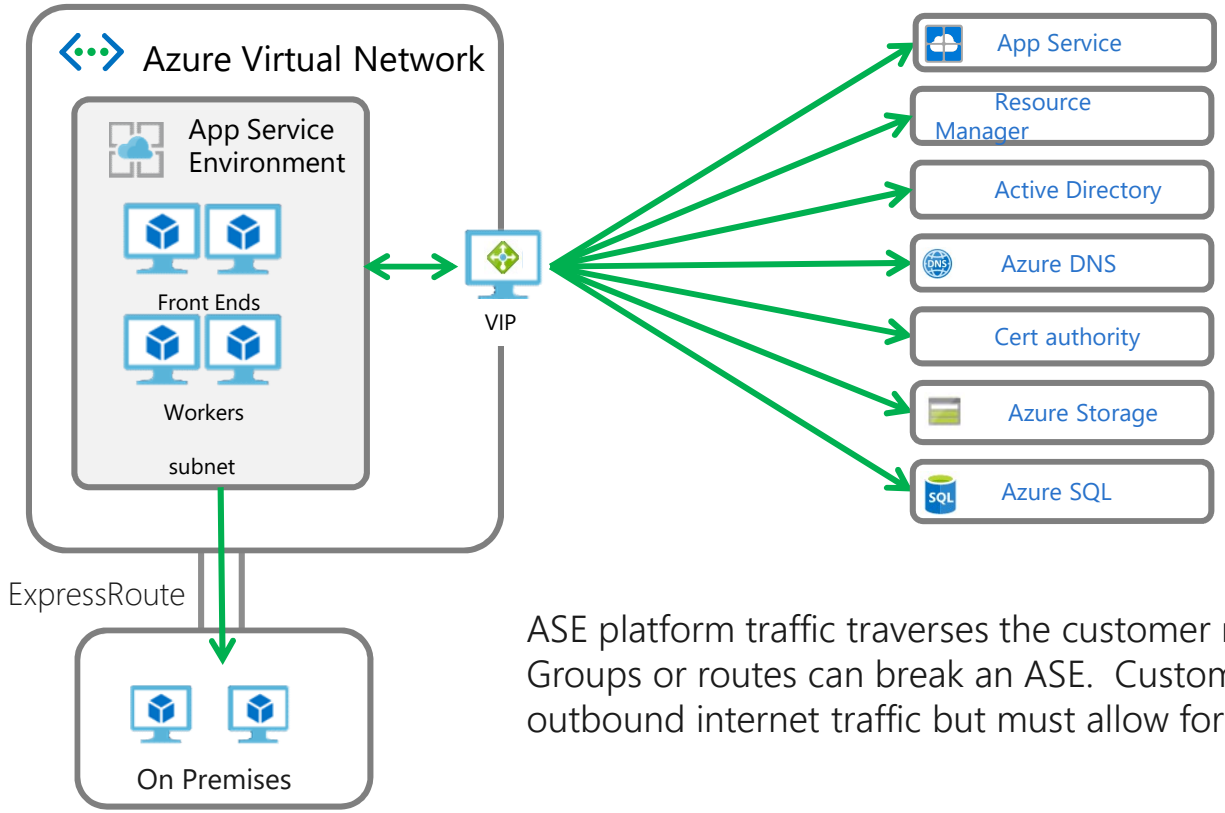
New VNet Integration + Service Endpoints: Private IP

Scenario: App network isolation without requiring an ASE



By combining these two features you can lock your app down to a private address in your VNet and also enable it to reach on premises over ExpressRoute.

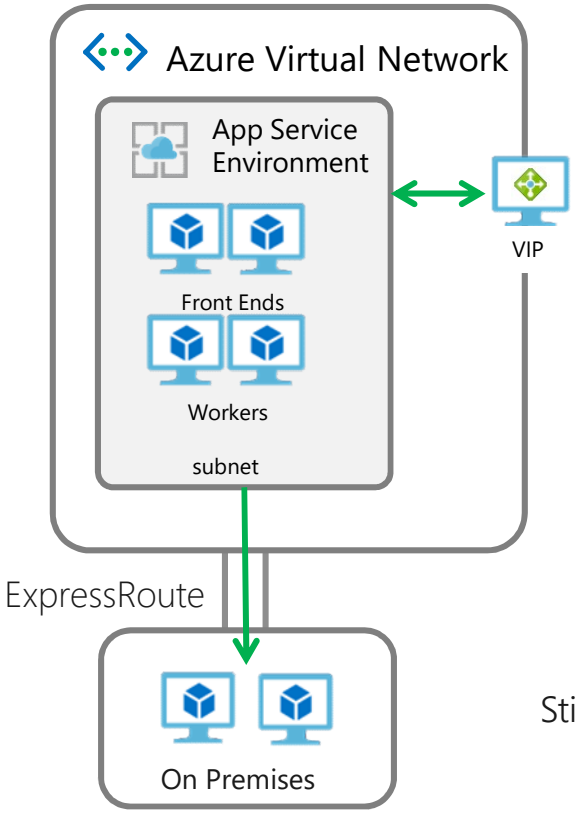
ASE today – complex network dependencies



ASE platform traffic traverses the customer network. Network Security Groups or routes can break an ASE. Customers cannot block all outbound internet traffic but must allow for dependency traffic.

Others tools

ASE tomorrow - simple and even more secure



Completely isolated ASE
No inbound or outbound management traffic travels on the customer VNet. Customers can completely lock down their system

Instant'ish scaling (<30 seconds)
The new system architecture enables rapid scaling for the ASE.

Still single tenant. Even more secure. Even more isolated.

Azure DevOps

Azure Boards

Deliver value to your users faster using proven agile tools to plan, track, and discuss work across your teams.

Azure Pipelines

Build, test, and deploy with CI/CD that works with any language, platform, and cloud. Connect to GitHub or any other Git provider and deploy continuously.

Azure Repos

Get unlimited, cloud-hosted private Git repos and collaborate to build better code with pull requests and advanced file management.

Azure Test Plans

Test and ship with confidence using manual and exploratory testing tools.

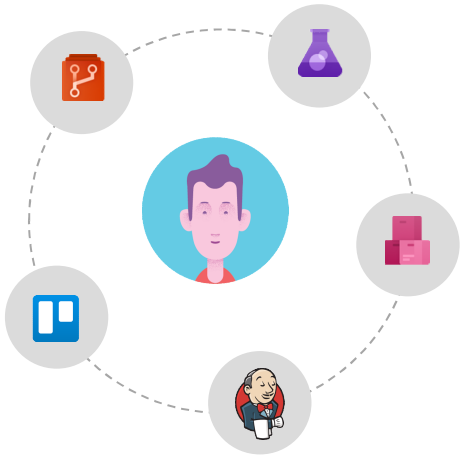
Azure Artifacts

Create, host, and share packages with your team, and add artifacts to your CI/CD pipelines with a single click.

https://azure.com/devops

Azure DevOps: Choose the tools and clouds you love

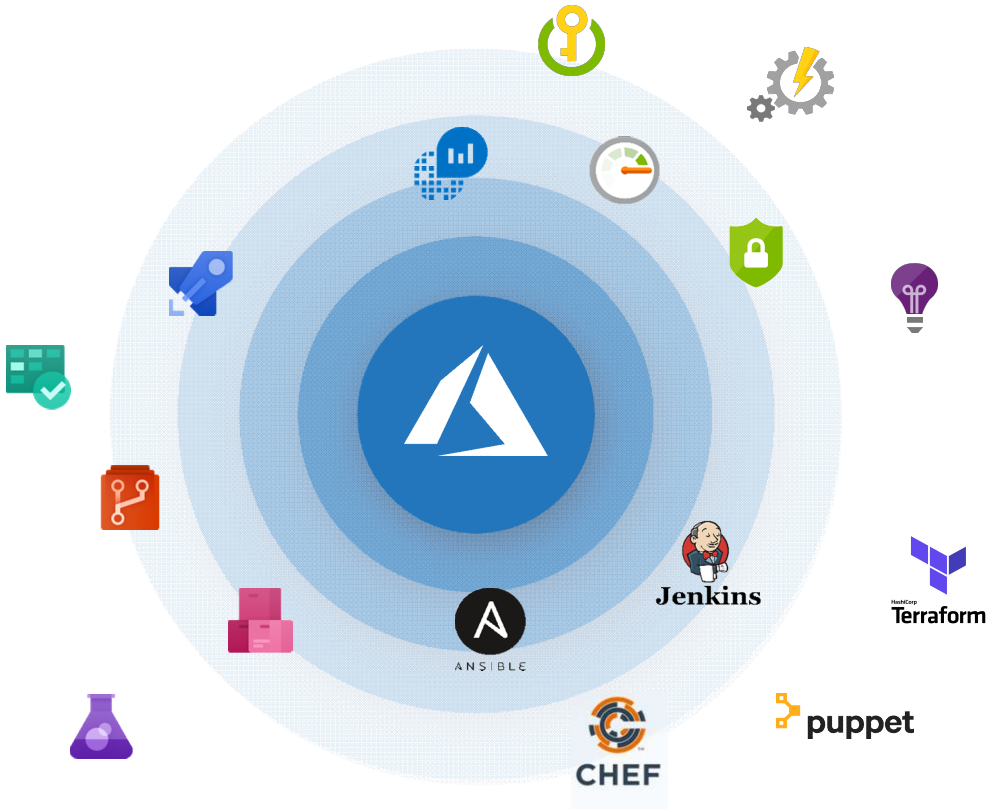
Azure DevOps lets developers choose the tools that are right for them



Mix and match to create workflows with tools from Microsoft, open source or your favorite 3rd party tools

Target any cloud, on-prem or both and deploy to the servers you need

Broadening the Azure Ecosystem

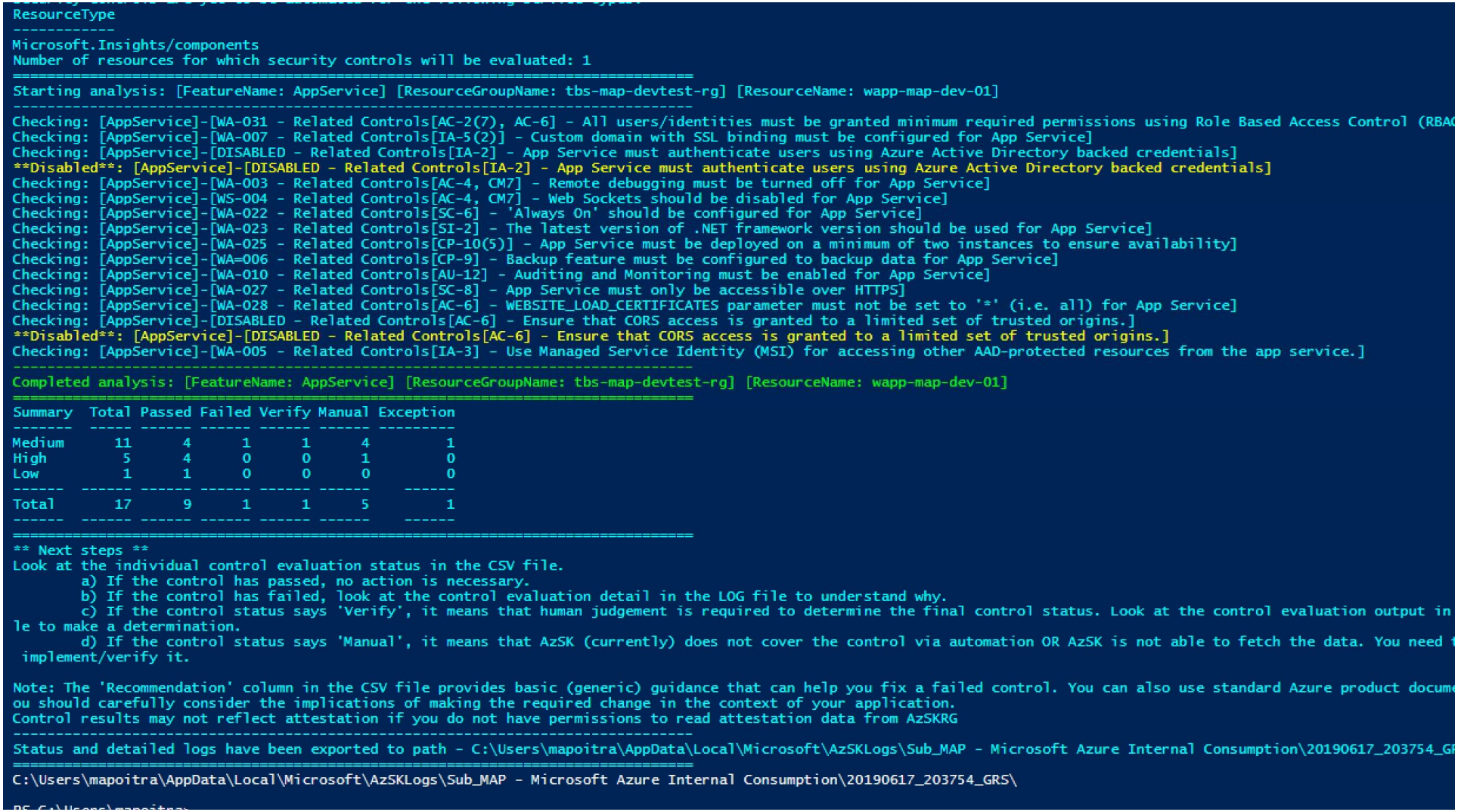


DevOps Kit For Azure

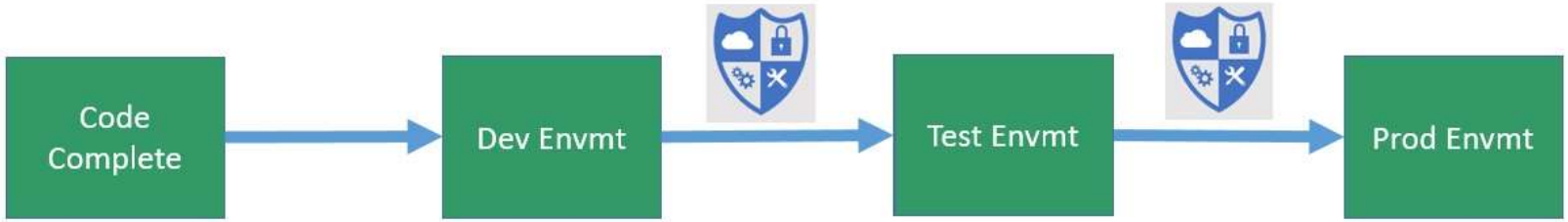
https://azsk.azurewebsites.net/index.html

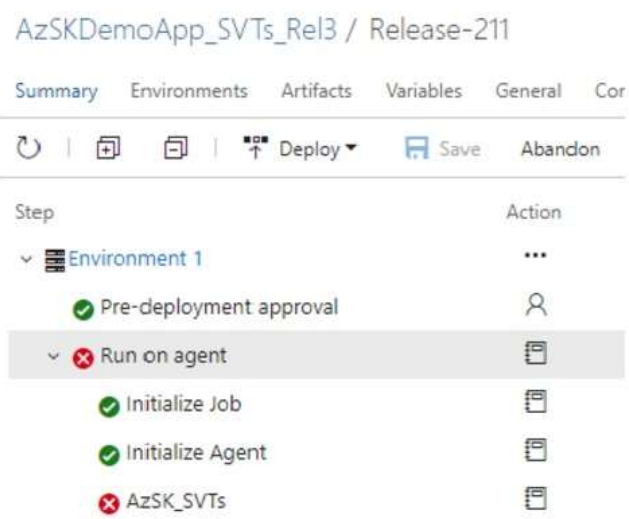
https://github.com/azsk/DevOpsKit

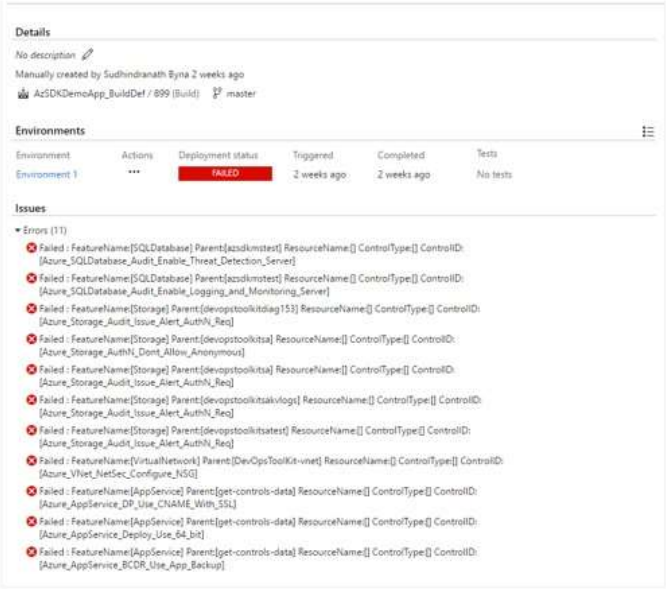
Customizable Security Test Coverage



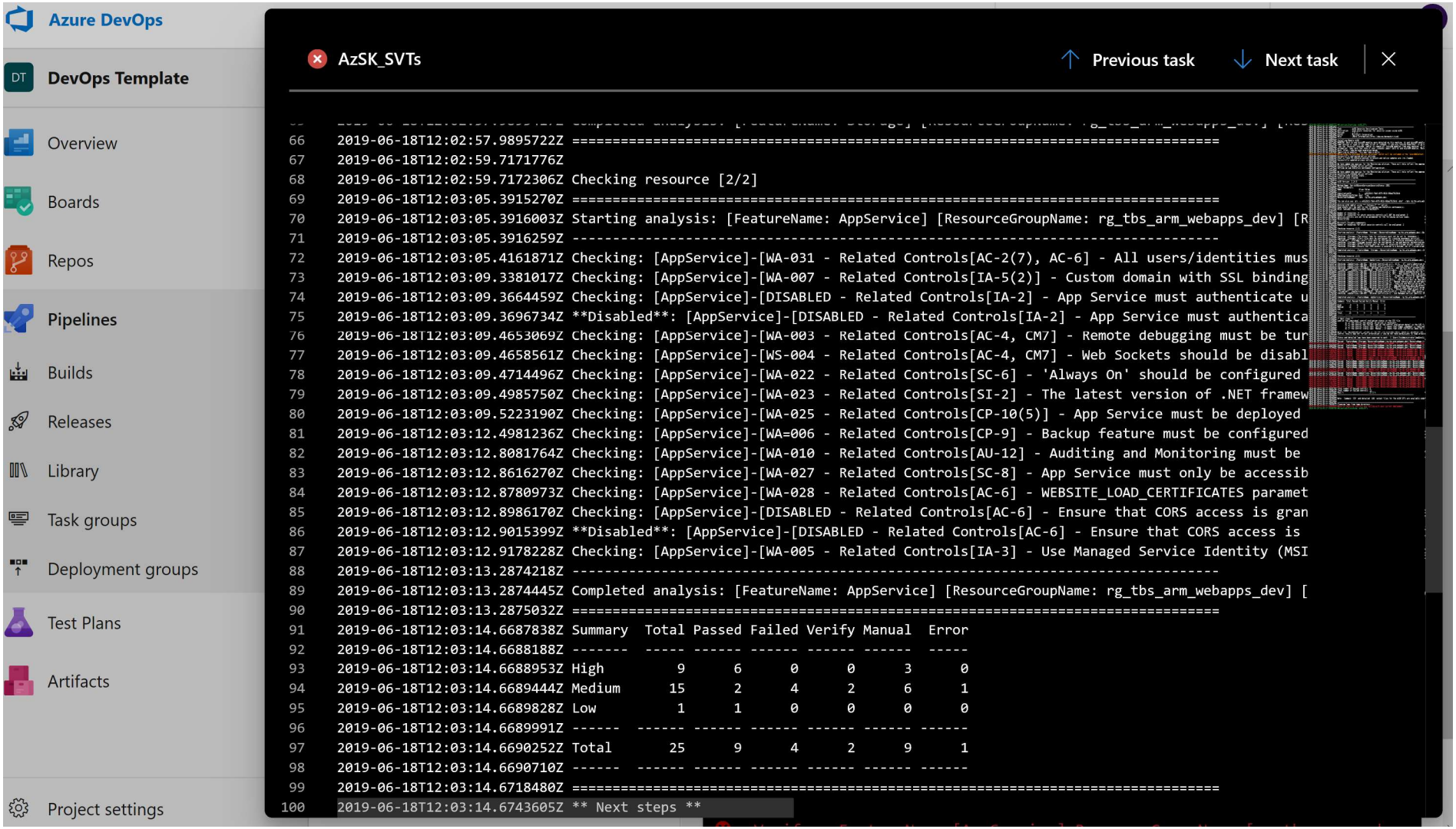
Check security in CICD pipelines





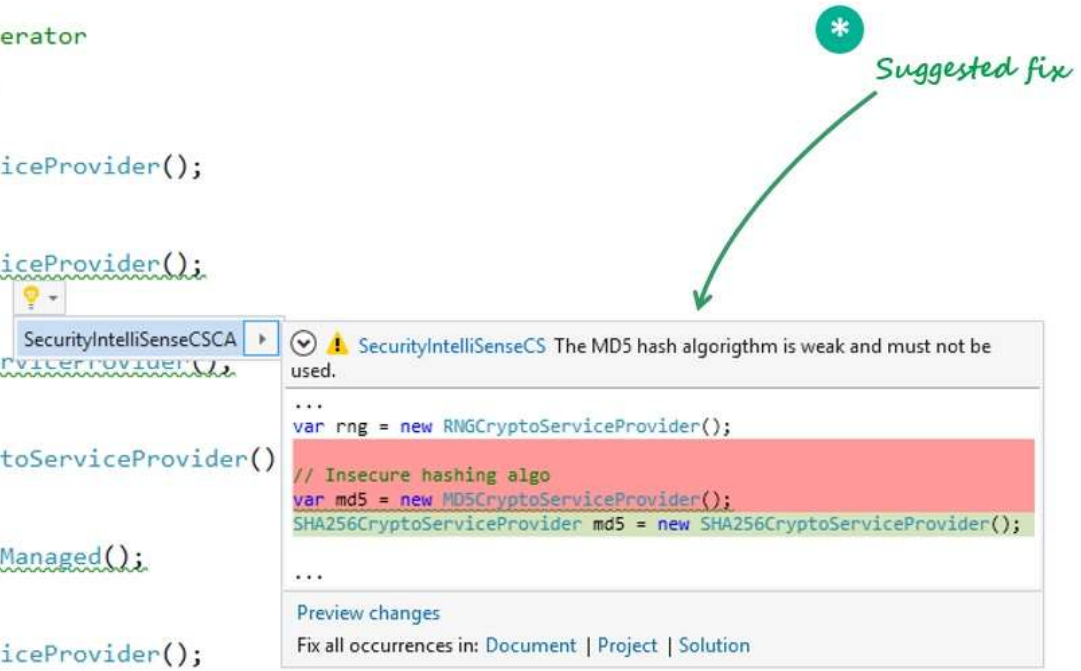


Integrate with CI/CD Pipelines



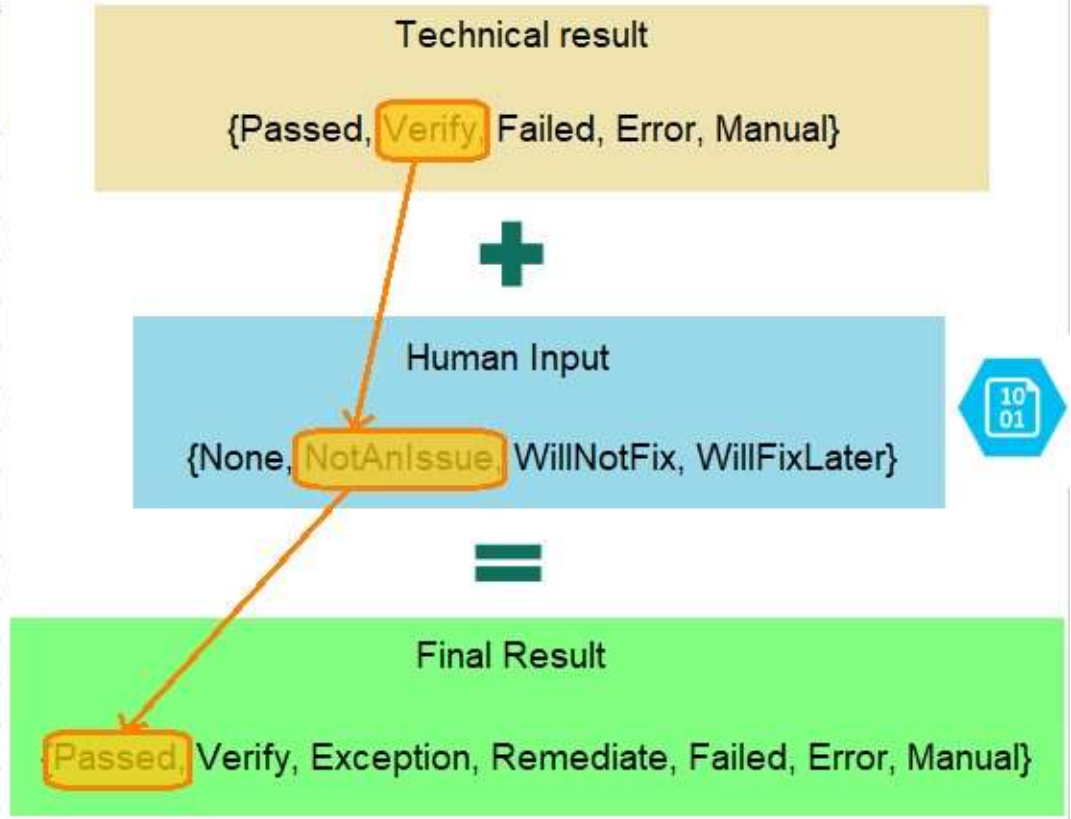
Write secure code with Security IntelliSense

```
public static void RandomData()
{
    // Insecure Random data generator
    var random = new Random();

    // Secure
    var rng = new RNGCryptoServiceProvider();

    // Insecure hashing algo
    var md5 = new MD5CryptoServiceProvider();

    // Insecure hashing algo
    var sha1 = new SHA1CryptoServiceProvider();

    // Secure
    var sha256 = new SHA256CryptoServiceProvider()

    //Insecure Encryption
    var rijndael = new RijndaelManaged();

    // Secure
    var aes = new AesCryptoServiceProvider();

    // Insecure AES config
    aes.KeySize = 128;
```



Control Attestation (overriding AzSK results)

Control Scan Result	Attestation Status	Effective Status
Passed	None	Passed
Verify	None	Verify
Verify	NotAnIssue	Passed
Verify	WillNotFix	Exception
Verify	WillFixLater	Remediate
Failed	None	Failed
Failed	NotAnIssue	Passed
Failed	WillNotFix	Exception
Failed	WillFixLater	Remediate
Error	None	Error
Error	NotAnIssue	Passed
Error	WillNotFix	Exception
Error	WillFixLater	Remediate
Manual	None	Manual
Manual	NotAnIssue	Passed
Manual	WillNotFix	Exception
Manual	WillFixLater	Remediate

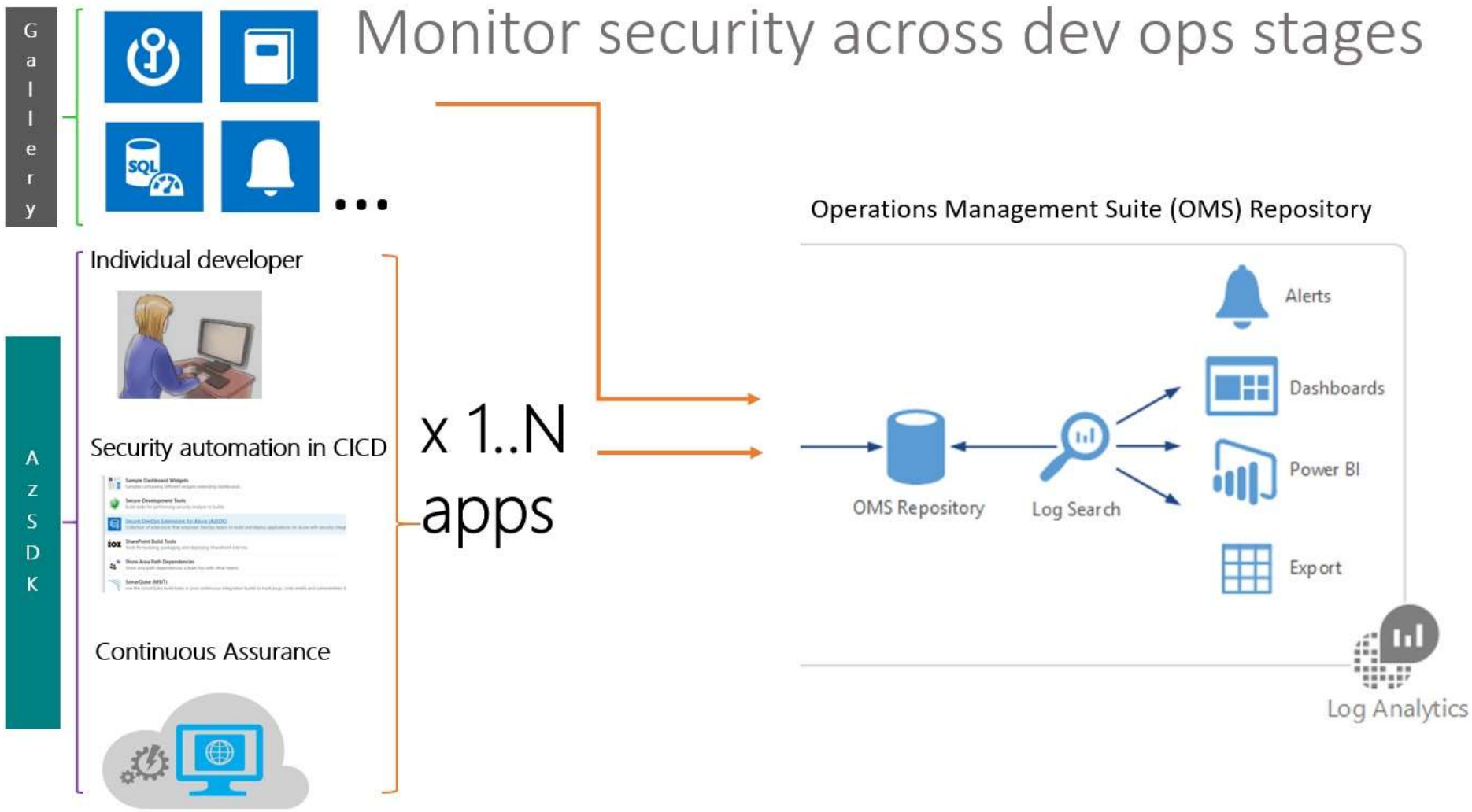


Track security drift in production

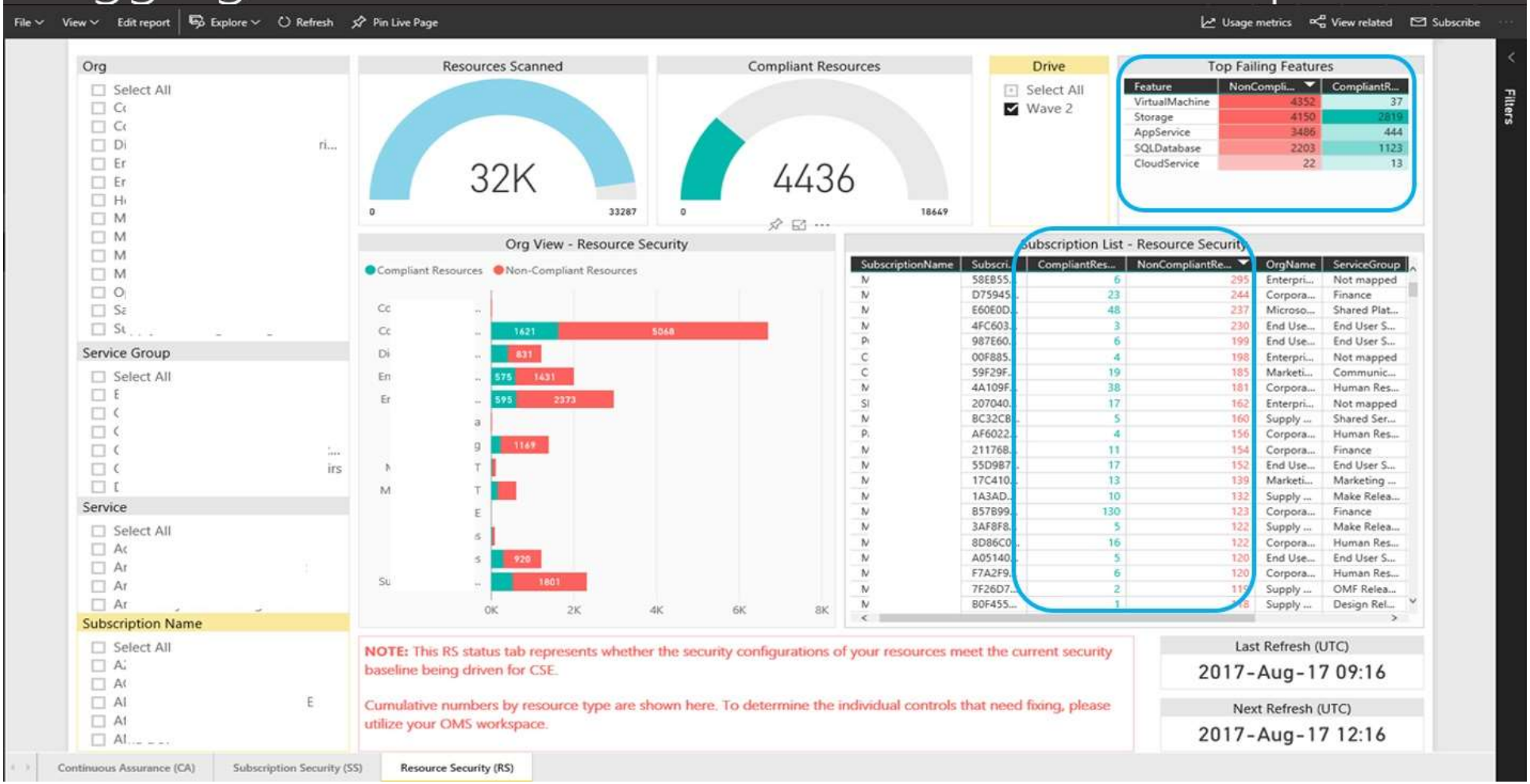
Azure Automation

Scan cloud resources in a scheduled fashion

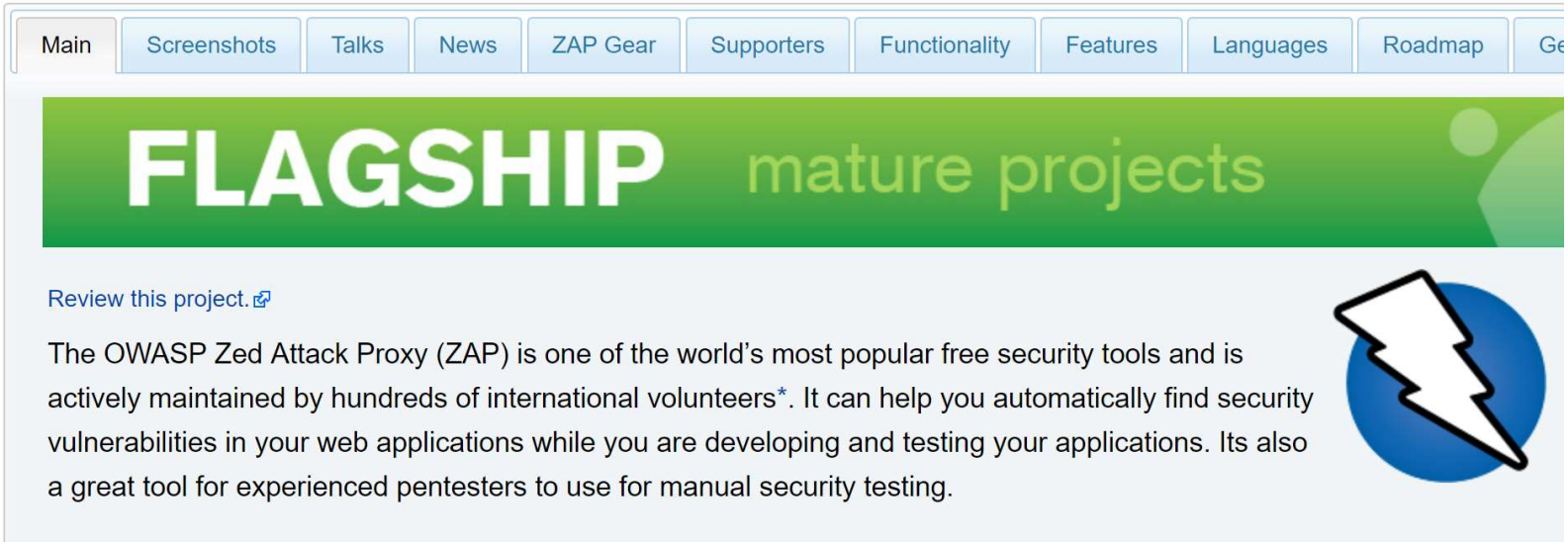
Monitor security across dev ops stages



Aggregate view of cloud risks across the enterprise



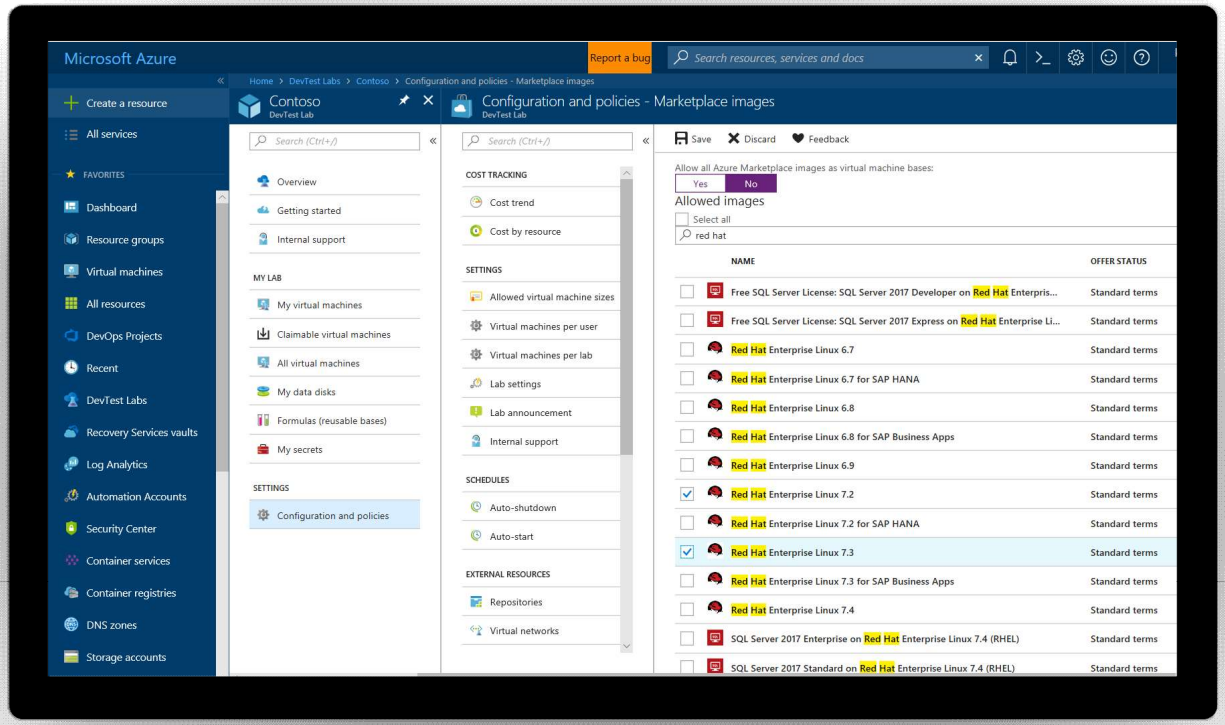
OWASP Zed Attack Proxy Project



Self-Service Dev/Test Environments

Azure Lab Services

- Simplify cloud environment management for developers and testers.
- Enforce policies and control costs with full visibility
- Use templates, custom images and formulas to reproduce environments.
- Orchestrate with Azure Pipelines or integrate using REST API



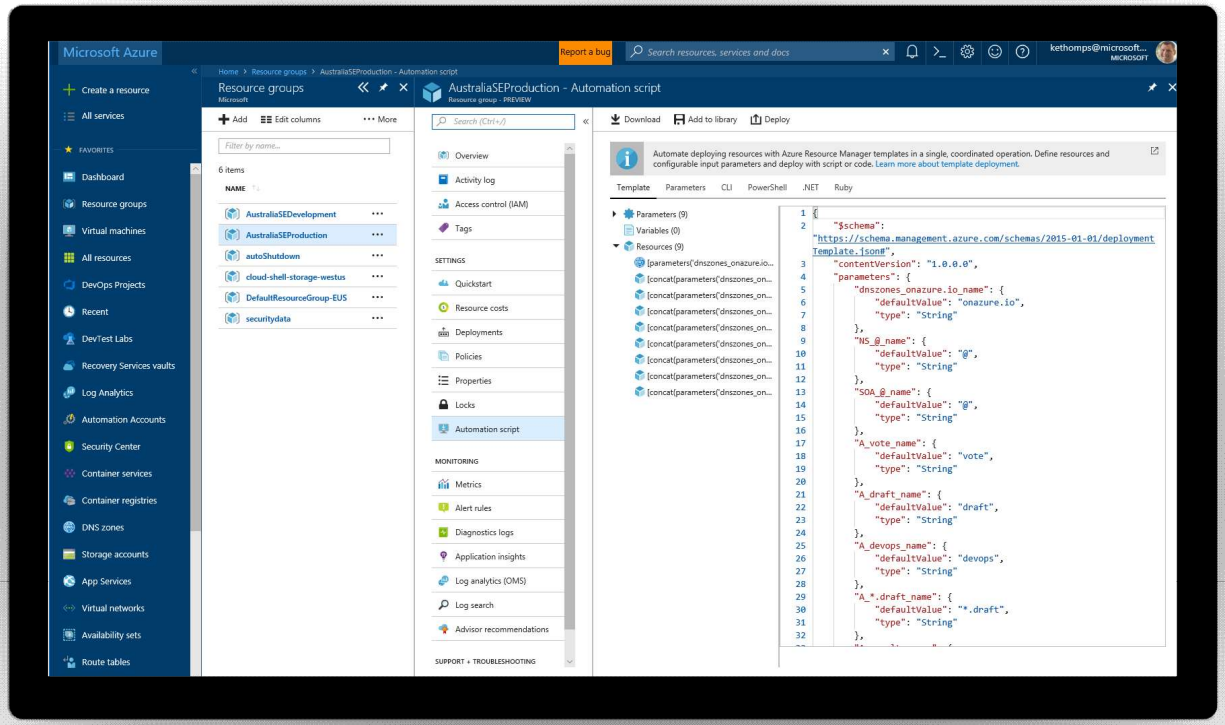
Infrastructure and Configuration as Code

Azure Resource Manager, Automation & 3rd Party Integrations

- Infrastructure as Code, built-in
- Azure Config & Automation
- Support for 3rd party and OSS tooling such as Terraform, Ansible, Chef, Puppet & SaltStack

TERRAFORM ANSIBLE CHEF

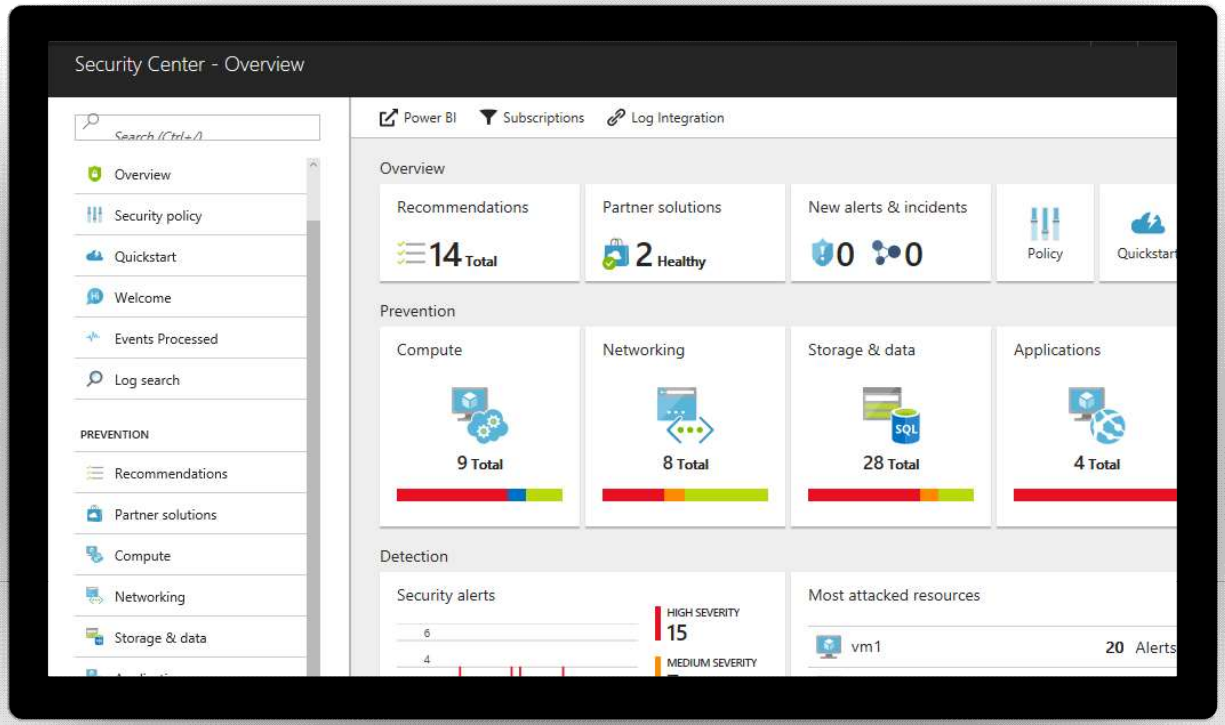
puppet SALTSTACK



Continuous Security

Azure Security Center

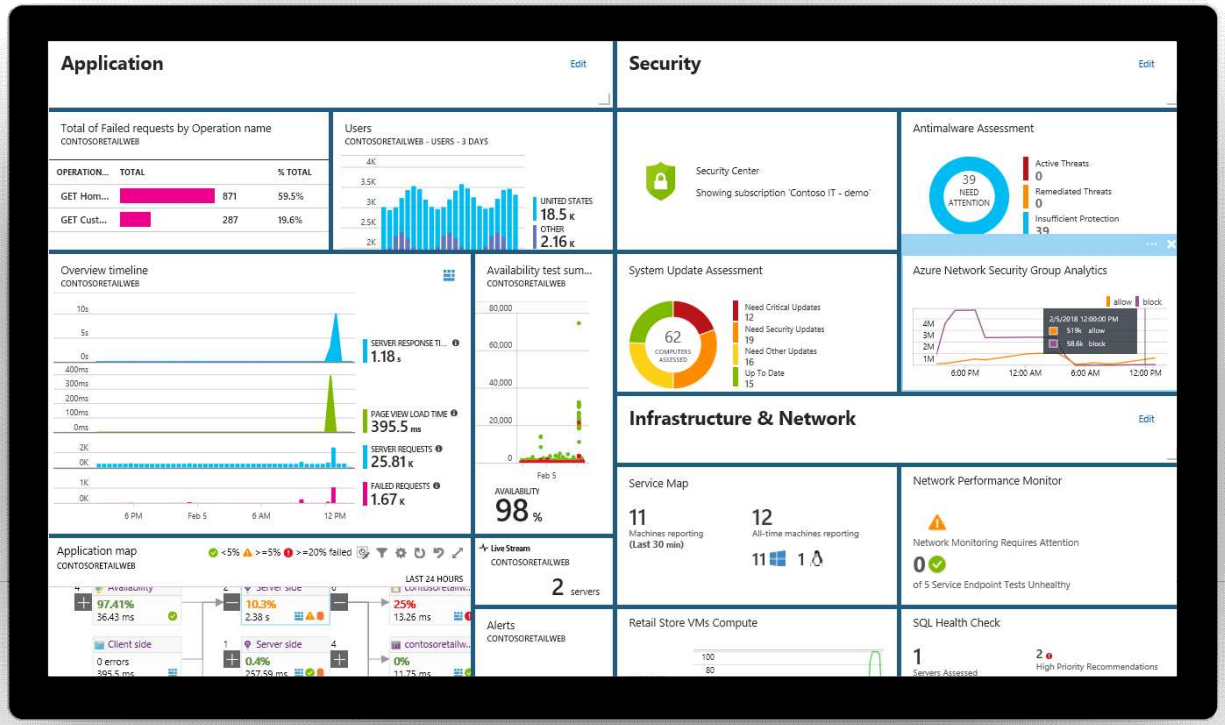
- Gain full visibility and control of your cloud security state
- Leverage ML to Proactively identify and mitigate risks to reduce exposure to attacks
- Quickly detect and respond to threats with advanced analytics



Smarter Insights, Faster

Azure Monitor, Application Insights & Log Analytics

- Pre-defined solutions with smart thresholds
- Visualize data in intuitive and customizable dashboards
- Separate the signal from the noise and accelerate root-cause analysis
- Integrate your existing processes & tools like Service Now



Demo

Appendix

App Services Networking Resources

Doc links

- IP Restrictions: https://docs.microsoft.com/azure/app-service/app-service-ip-restrictions
- Hybrid Connections: https://docs.microsoft.com/azure/app-service/app-service-hybrid-connections
- VNet Integration: https://docs.microsoft.com/azure/app-service/web-sites-integrate-with-vnet
- App Service Environment: https://docs.microsoft.com/azure/app-service/environment/intro

Next Steps

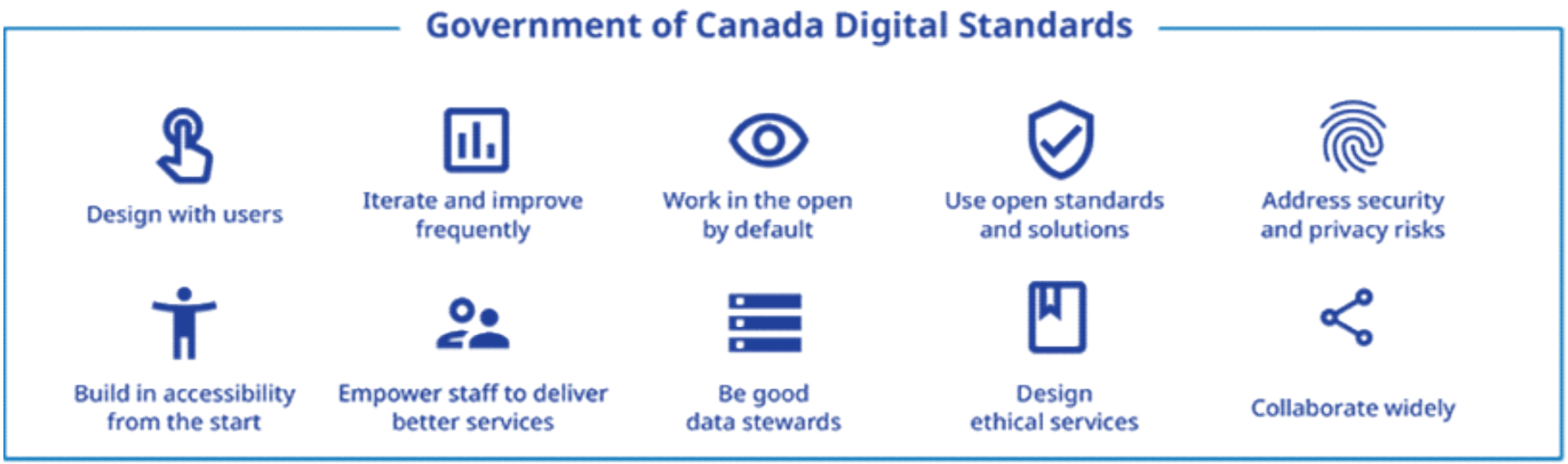
Questions?

Contact us:

GC Digital Direction

The digital government vision
The Government of Canada is an open and service-oriented organization that operates and delivers programs and services to people and businesses in simple, modern and effective ways that are optimized for digital and available anytime, anywhere and from any device.

Digitally, the Government of Canada must operate as one to benefit all Canadians.



https://www.canada.ca/en/government/system/digital-government/digital-operations-strategic-plan-2018-2022.html

References

TB Policies & Standards

- Policy on Management of Information Technology
- Policy on Government Security
- Direction for Electronic Data Residency, ITPIN No: 2017-02
- Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)

Guidance

- Government of Canada Security Control Profile for Cloud-Based GC IT Services
- Government of Canada Cloud Security Risk Management Approach and Procedures
- CSE ITSG-22 Baseline Security Requirements for Network Security Zones in the Government of Canada
- CSE ITSG-38 Network Security Zoning - Design Considerations for Placement of Services within Zones
- CSE ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems
- CSE ITSP.40.062 Guidance on Securely Configuring Network Protocols