Cloud Direct®

How to establish secure development environments in Azure

Sean O'Brien, Azure Lead, Cloud Direct

Cassandra Browning, Cloud Security Architect, Microsoft

10:00 – 11:00 AM

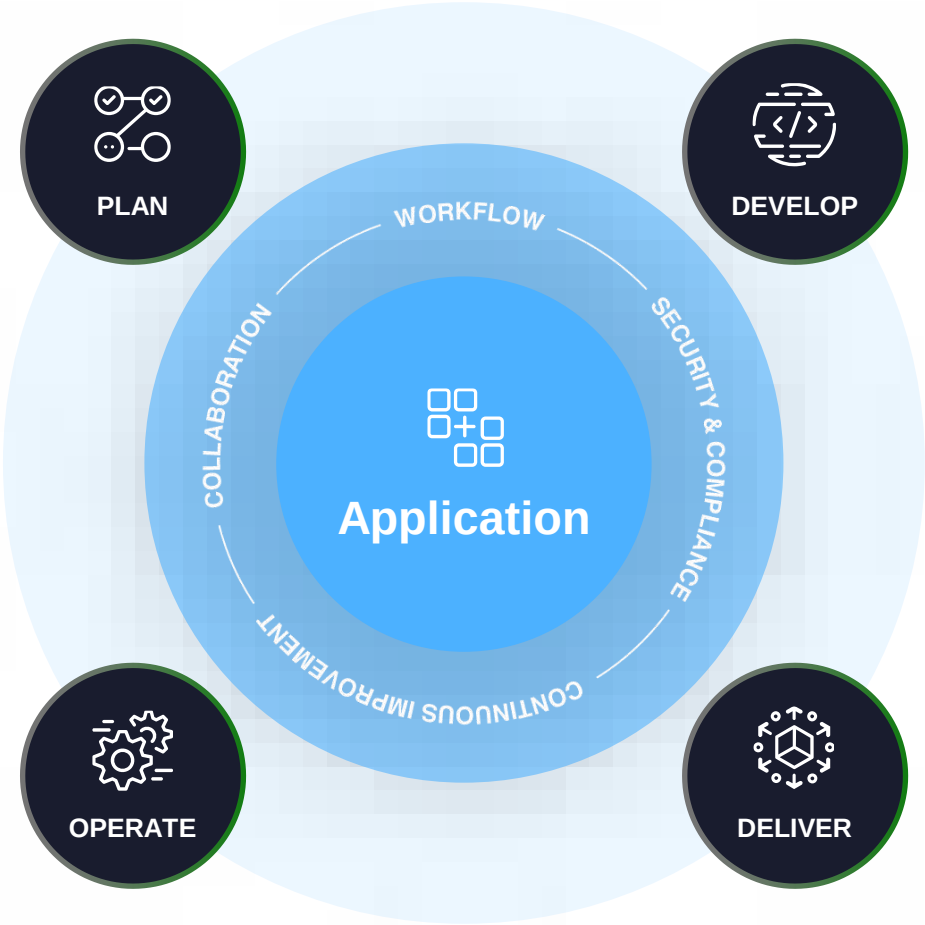
What do we mean by DevSecOps?

DevOps Definition (Development + Operations)

DevOps is the union of people, processes, and technology to deliver continuous value to users.

DevSecOps Definition (Development + Security + Operations)

DevSecOps is an evolution in the way development organizations approach security by introducing a security-first mindset culture and automating security into every phase of the software development lifecycle from design to delivery.



Securing Software Development

Key requirements for success

Developers

- Maximize developer velocity
- Eliminate developer complexity
- Empower developers to contribute

CISOs

- Advanced Forensics / Detection Tools
- Partner with developer teams
- Proactive Hunting

Shared accountability

Secure the development environment

Embed security in the developer workflow

Secure cloud-based developer machines

Browser sandboxing

- For code browsing, limit scope for non-trusted repositories to a browser sandbox.

Environment Isolation

- Build non-trusted repositories in an isolated environment not on a local developer machine.

Identity and Access Management

- Cloned repositories should implement least privileged access principles.
- Developer user accounts (arguably all user accounts) should be protected by MFA.

Secret Management

- Secrets used in development should not be re-used

Prevent these types of attacks:

- Ability to execute malicious code on a developer machine
- Compromised developer machines acting as "jump-box" to further systems

Secure the DevOps Pipelines

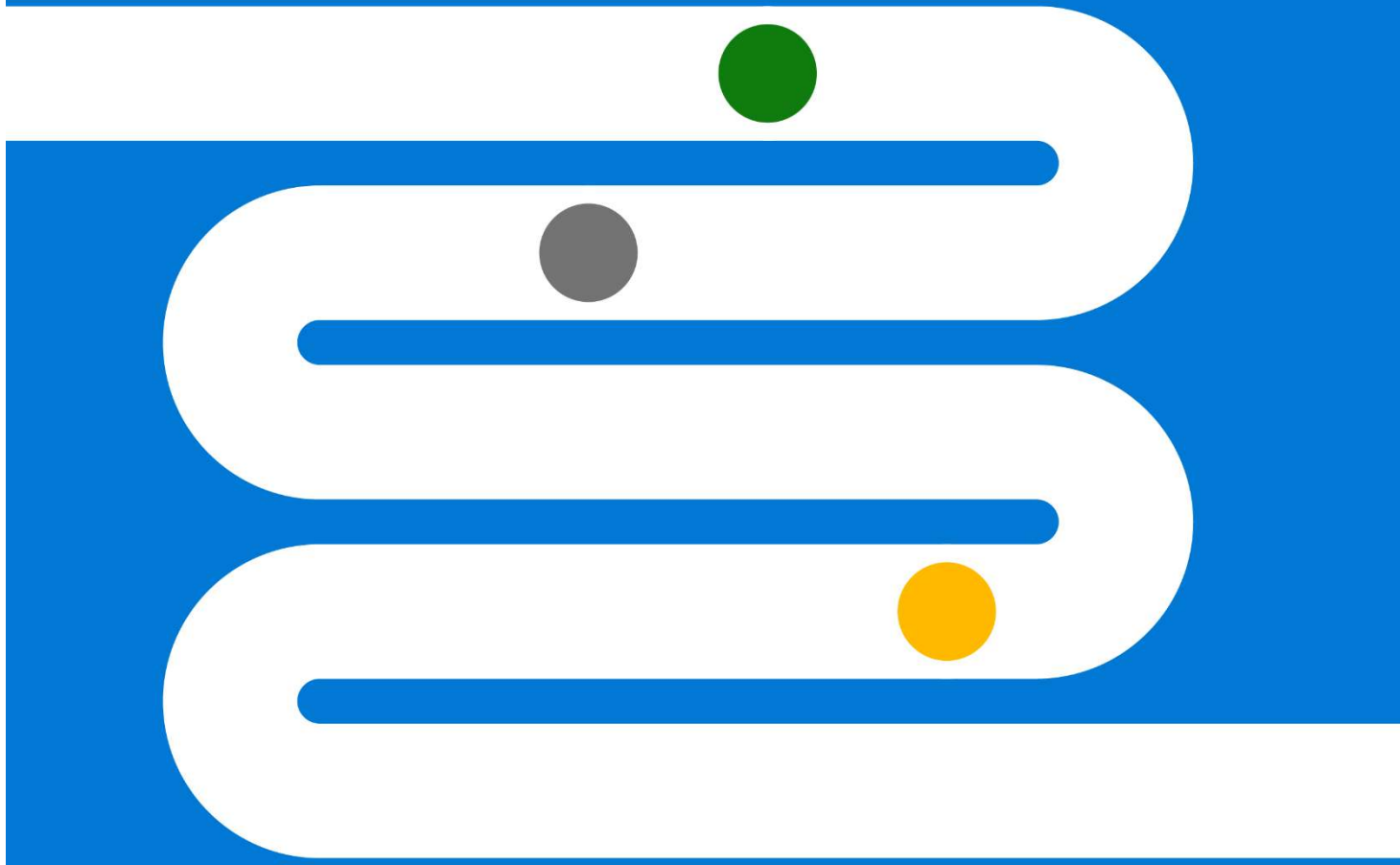
Adopt a centrally governed and secure engineering system

Only allow trusted, approved and authorized DevOps pipelines and actors the ability to enforce supply chain controls.

Control deployment from non-trusted pipelines by denying production certs

Prevent these types of attacks:

- Build tampering
- Unauthorized access to package repository and production infrastructure



Ensure developer velocity, securely

Secure the DevOps Pipelines (cont.)

Be able to produce verifiable and reproducible builds

Compilers

Sign properly with validated signatures

Builds

Produce verifiable build manifests—describing sources, cryptographic hashes of binaries/artifacts and full build parameters

Build Machines & infrastructure

Make highly restricted with least privileged access applied and with ephemeral build agents

DevOps services

Build and release infra use isolated managed identities and sensitive tenant profiles for isolation

Compilers & user processes

Execute in isolation or locked down environments

Software on build machines

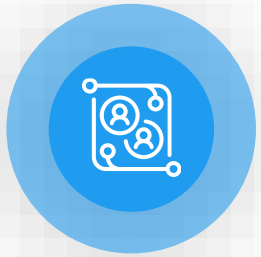
Sign properly with validated signatures

Prevent these types of attacks:

- Compromised compilers and build machines
- Compromised dependencies

Harden access to codebases

Ensure all codebases must have a maintainer



Follow least privileged access - grant access to developers to codebases by organization (no global access)

Limit elevated privileges. Do so only when absolutely necessary and implement a finite duration on higher access levels

Prevent these types of attacks:

- Source code exfiltration on developer machines
- Source code tampering or injection of malicious code

Harden pipeline access

Ensure code-to-cloud pipeline is secure

Create organization device policies – AAD + Device policies - to secure development machines

Make sure all operations adhere to least privileged principles

Regularly scan for identity access management to ensure least-privileged access management policies

Use multi-factor authentication and dual key/JIT approval for privileged operations and human-induced pushes

Enable endpoint protection for all workstations and allow only registered devices

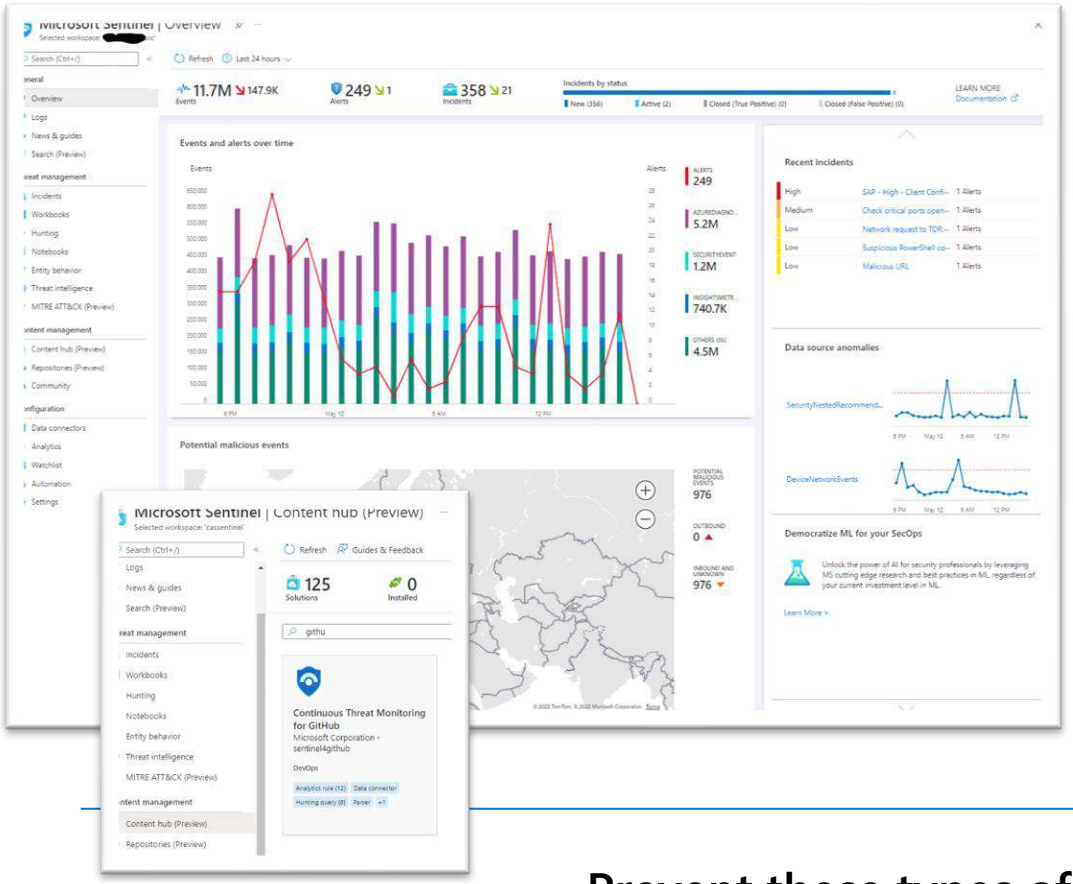
Inject identity early into the automation pipeline

Prevent these types of attacks:

- Compromised credentials
- Malicious insiders

Monitor the developer cloud

Detect and respond to suspicious activities



Monitor for anomalous activities to identify and detect that which may represent nefarious intent from mass repo cloning, downloading, or deletion

Regularly scan for identity access management to ensure least-privileged access management policies

Enable alerting and routing for security policies across DevOps pipelines

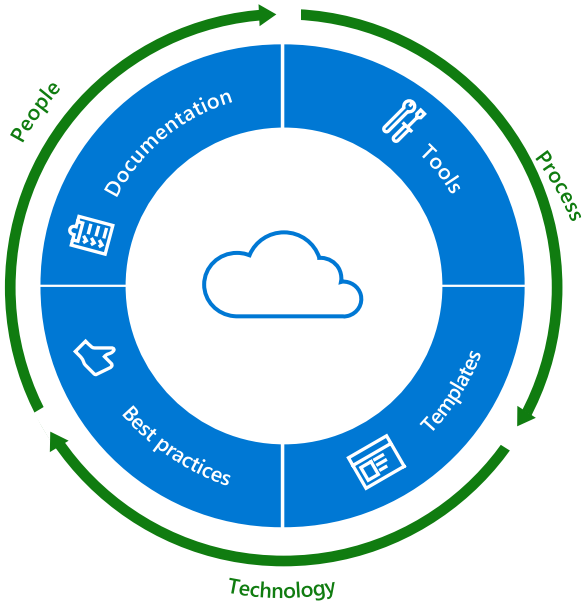
Automate notifications to developers of leaked tokens, secrets, or credentials

1. https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/microsoft-sentinel-continuous-threat-monitoring-for-github-new/ba-p/3343209
2. https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/monitoring-the-software-supply-chain-with-azure-sentinel/ba-p/2176463

Prevent these types of attacks:

- Threat from within
- Escalation of brute force attack/intrusion access

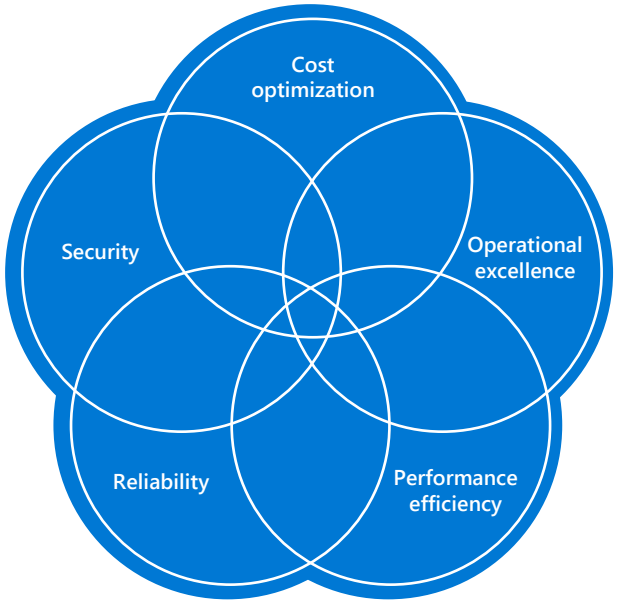
Microsoft resources, guidance, and best practices



Microsoft Cloud Adoption Framework for Azure

Actionable, efficient, and comprehensive Azure cloud guidance from Microsoft to accelerate your adoption journey.

Start learning: Security Methodology

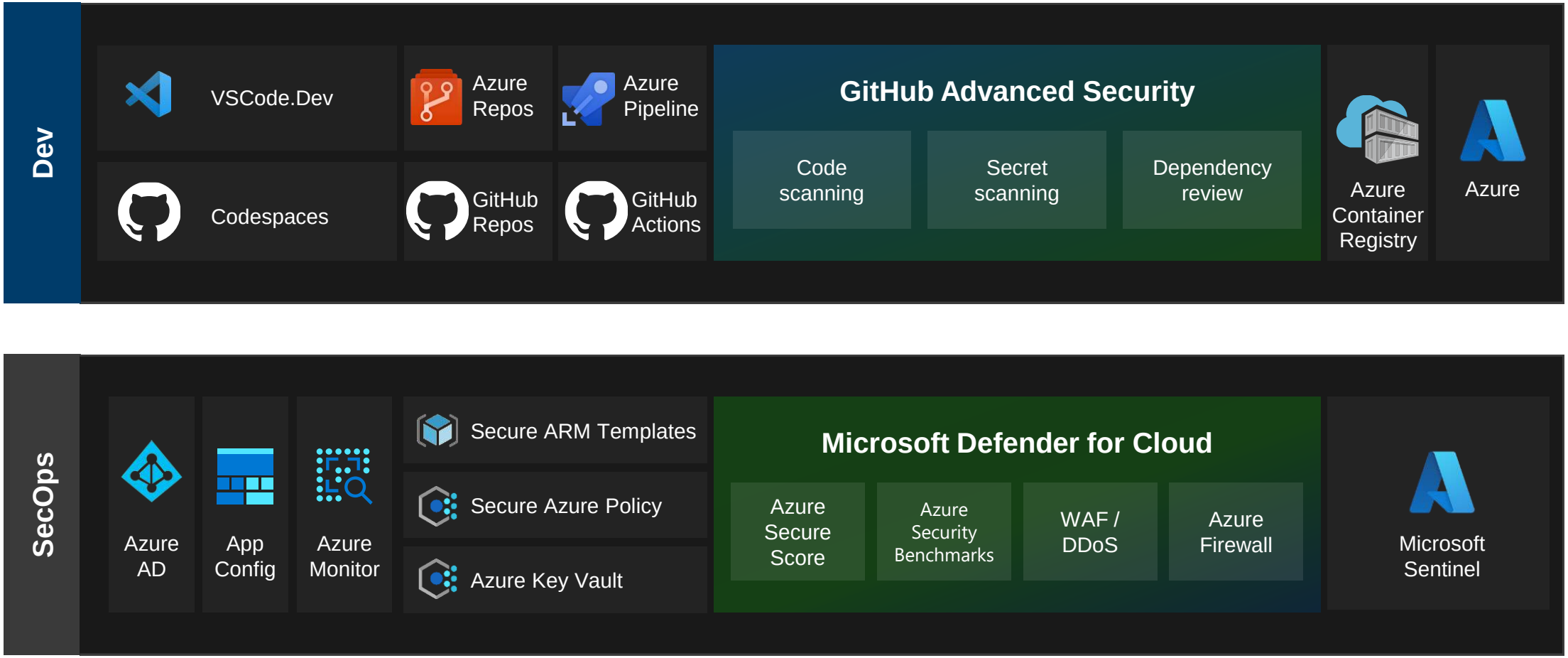


Microsoft Azure Well-Architected Framework

Architecture guidance and best practices created for architects, developers, and solution owners, to improve the quality of their workloads, based on five aligned and connected pillars

Start learning : Security Pillar

Develop apps securely with a unified solution from Microsoft



Where security fits in the development lifecycle

Pre-commit

- Threat modelling
- Secure coding standards
- Peer review

Commit (CI)

- Static code analysis
- Dependency management
- Credential scanning

Deploy (CD)

- Continuous monitoring
- Threat intelligence
- Blameless post-mortems

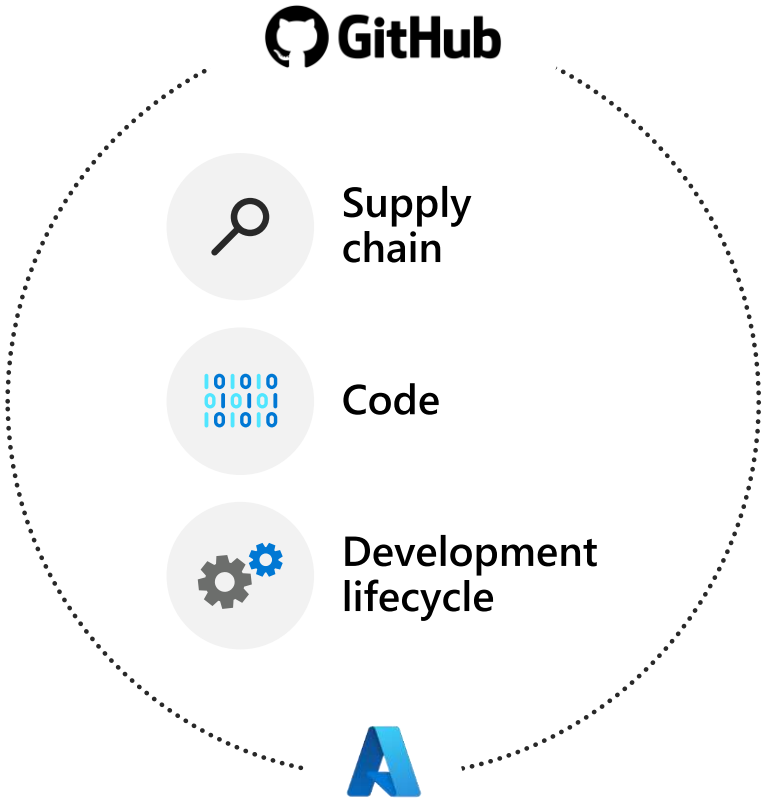
Deploy (CD)

- Infra as code (IaC) scanning
- Cloud configuration checks
- Security acceptance tests

Build secure apps from the start

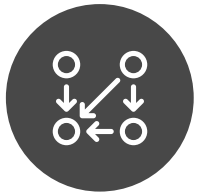
Implement integrated DevSecOps for secure development and deployment of applications

- Deploy secure code across clouds–Azure, AWS, Google Cloud, and others
- Helps reduce security effort, increase development speed, and improve application security
- Focus on actionable and high priority security issues within the developer workflow
- Have peace of mind with enforced security and compliance policies
- Provide central visibility to security admins through Microsoft Defender for Cloud integration



Shift-left with secure DevOps

Github Advanced Security



Dependency scanning

- Alerts and security updates for new vulnerabilities
- Integrated review when introducing new dependencies

Code scanning

- Extensible framework for code scanning
- Integrated within the developer workflow
- Backed by industry-leading CodeQL engine

Secret scanning

- Scanning for leaked secrets in public and private repos
- Partnership with 40+ providers

1. https://docs.github.com/github/getting-started-with-github/about-github-advanced-security
2. https://owasp.org/www-community/Source_Code_Analysis_Tools

Microsoft Defender For Cloud

Cloud-native protection across clouds and hybrid environments

Harden and manage your Security Posture

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

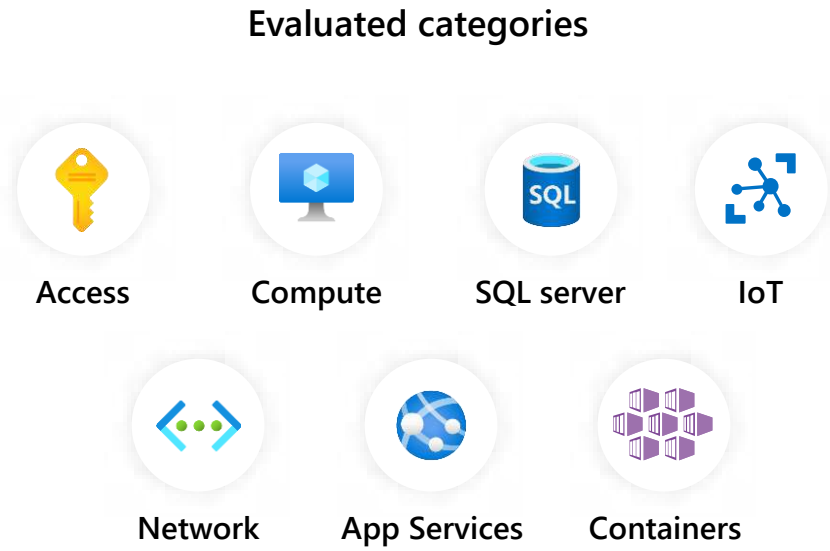
Amazon Web Services

Google Cloud Platform

Hybrid cloud

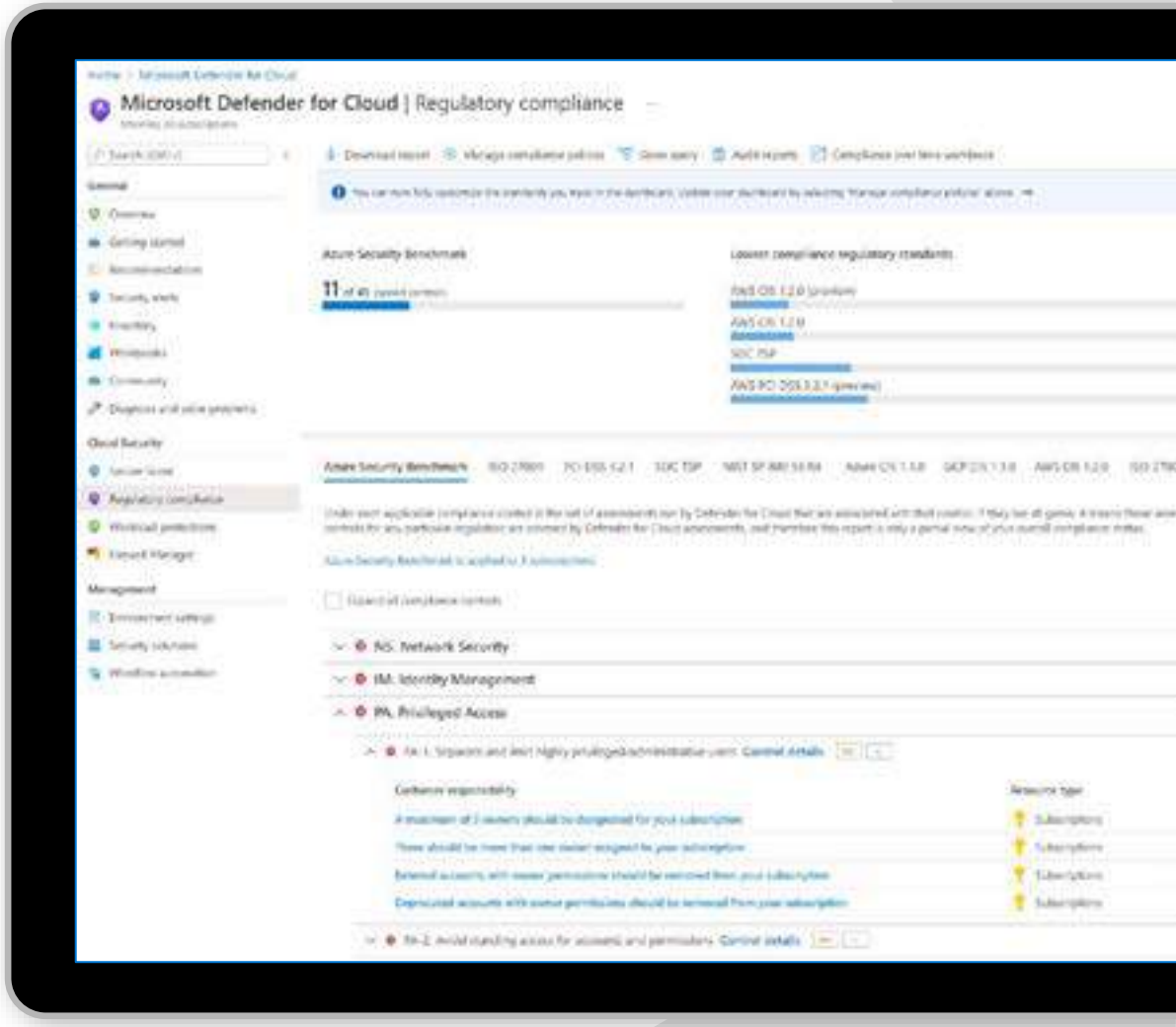
Secure Score

- Assess and implement best practices for security and compliance
- Cover all critical cloud resources across network, access, compute, databases, your service layer and more
- 450+out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements
- Use “Quick fix” to remediate with a single click or enforce policies to avoid configuration drifts
- Improve and track your secure score and overall security posture over time



Compliance assessment and management

- Assess and manage your compliance status with a continuous assessment of your cloud resources
- Use industry standards, regulatory compliance frameworks, and vendor provided benchmarks to implement security and compliance best practices
- Create custom recommendations to meet unique organizational needs



<u>Support for:</u>

- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices

Full-stack coverage with dedicated detections

Compute

- Any server
- Azure VMSS
- App Services
- Azure K8s

Service Layer

- Azure DNS
- Key Vault
- Network Layer V1
- Resource Manager

Databases and Storage

- Blob storage
- File storage
- Maria DB
- Cosmos DB
- Azure SQL
- MySQL
- Postgres SQL

AWS workloads

- Amazon EKS
- Amazon EC2

GCP workloads

- GKE clusters
- Google Compute

Microsoft Defender for Containers

Kubernetes security by Microsoft Defender for Cloud

Advanced Threat Detection

- Deterministic, AI, and anomaly-based detection
- Kubernetes runtime context
- Fileless attack detection

Vulnerability Assessment

- Visibility of running images with vulnerabilities
- Continuous scan for running images

Hardening and Kubernetes Policy

- Follow CIS benchmark
- Admission control policy- Mandate/audit security best practices on Kubernetes workloads

Multi-cloud support

- Azure Kubernetes Service
- Kubernetes on-prem and on IaaS
- Amazon EKS

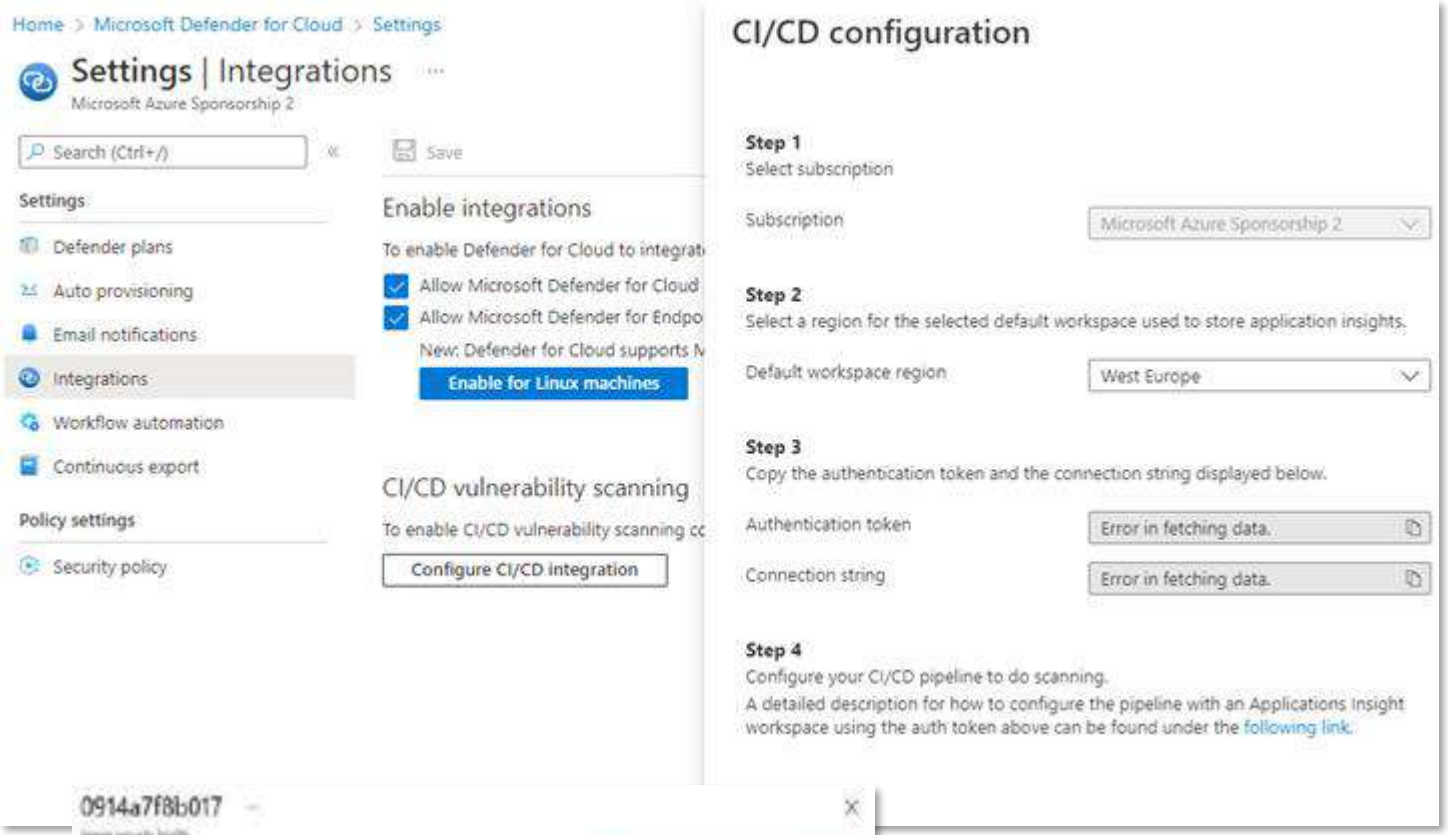
Kubernetes-native deployment

- Frictionless at scale provisioning
- Visibility and management capabilities via Kubernetes tooling

- One Defender plan for container security across the software supply chain
- Merging Defender for Kubernetes and Defender for Container registries which are now considered deprecated
- Removing dependency in the Servers plan and in the Log Analytics agent.

GitHub integration with Microsoft Defender for Containers

- Embed vulnerability scanning
- Give visibility to build and registry container scan results
- Provide traceability



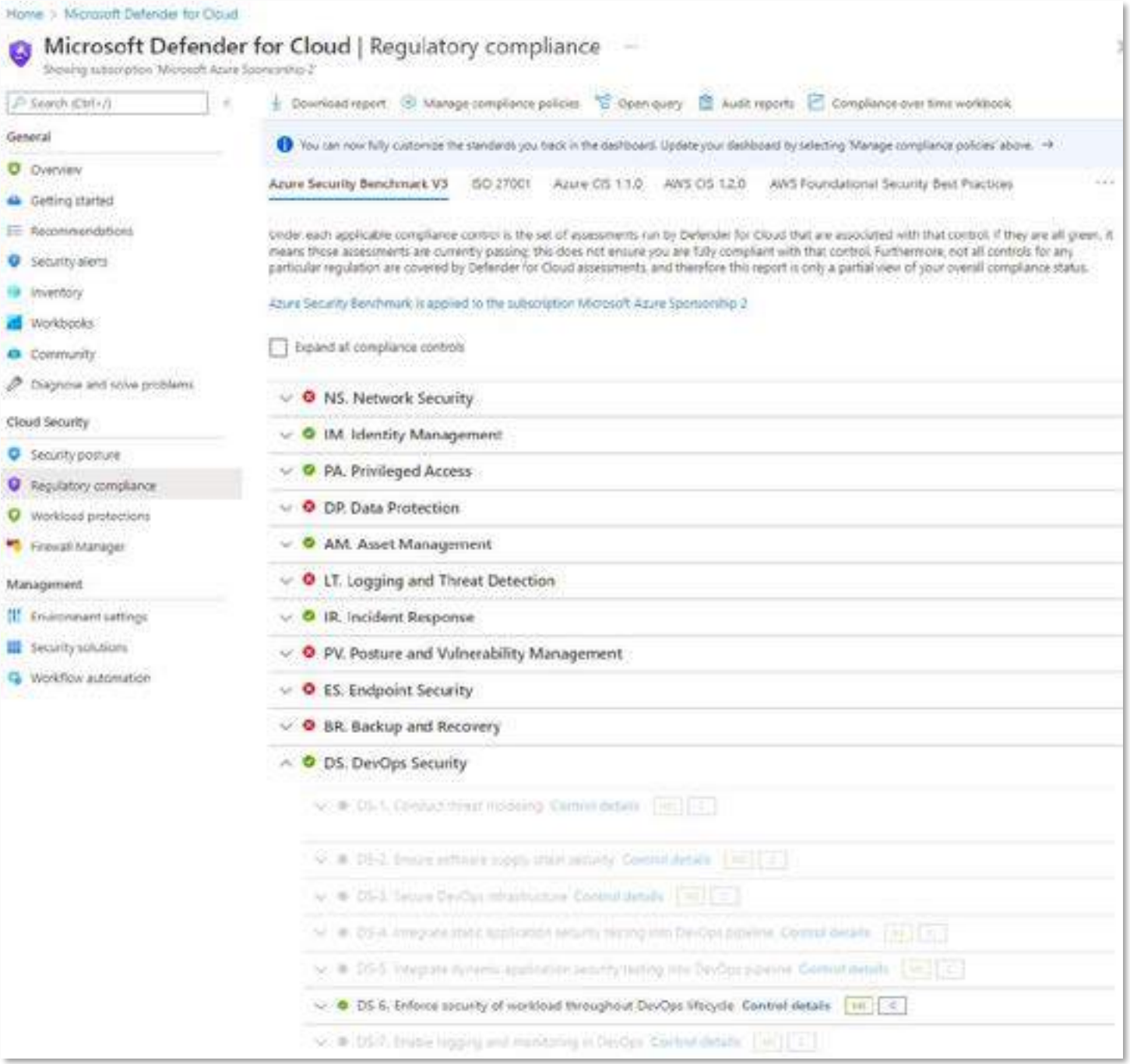
Need technical guidance?
[Container security with Microsoft Defender for Cloud | Microsoft Docs]

Azure Security Benchmark v3

DevOps Security Controls

Now in GA

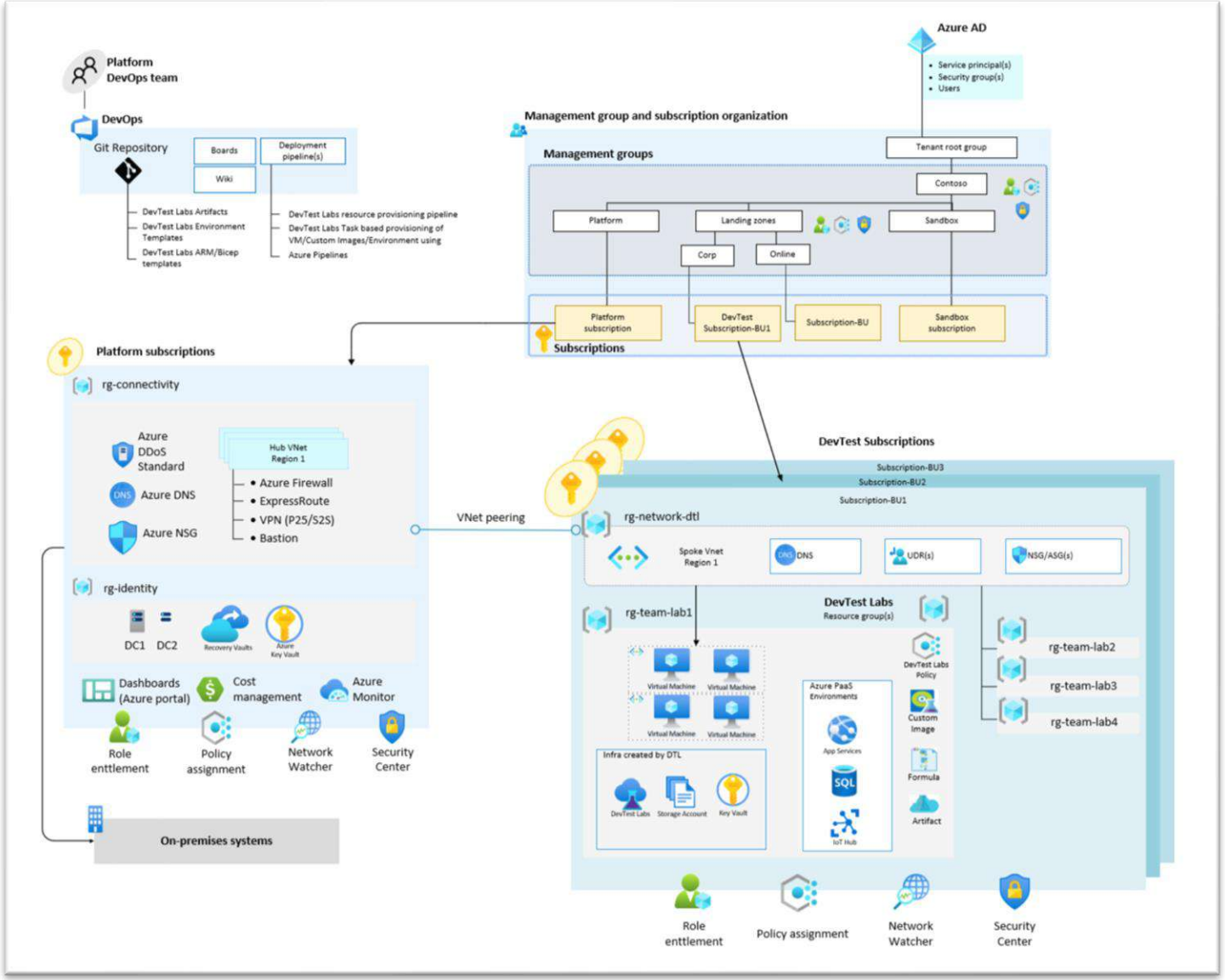
- Provides concrete guidance to secure your deployment pipelines based on industry standards (CIS/NIST/PCI)
- Enables monitoring of DevOps security guidance in Microsoft Defender for Cloud
- Helps meet compliance requirements for your DevOps environment



Azure Architecture Center

Example Azure architectures to help you visualize and understand

- Many example architectures have diagrams along with detailed explanations
- Cover considerations such as security, availability, devops
- Can often deploy the architecture from a github repository to test
- Example shown here is a dev test reference architecture in A ze



[Azure DevTest Labs reference architecture for enterprises]

[Security architecture design - Azure Architecture Center | Microsoft Docs]

[DevTest Labs | Microsoft Azure]

Key actions:

Turn on Azure Secure Score

Gain insight into the security state of your cloud workloads simply by enabling Defender for Cloud

Turn on Microsoft Defender for all cloud workloads

Protect your workloads with built-in threat protection

Turn on WAF and DDoS Protection for every website

Protect your web applications from malicious attacks

Turn on Azure Firewall for every subscription

Protect your Azure virtual network resources

Follow DevSecOps practices

Secure your environments and embed security into your development workflow

Review your application workloads, or work with a partner who has deep expertise in the area - Azure Well-Architected Review - Assessments | Microsoft Docs.

Helpful Links

General Guidance

- Cloud Adoption Framework (CAF) Security Methodology – https://aka.ms/cafsecure
- Azure Well-Architected Framework (WAF) – Security Pillar overview – http://aka.ms/wafsecurity
- Microsoft's Cybersecurity Reference Architecture (MCRA) – Technical Architecture – https://aka.ms/mcra
- Microsoft Azure Architecture Center – https://aka.ms/architecture
- https://docs.microsoft.com/en-us/azure/devtest-labs/devtest-lab-overview

Workload security controls

- Azure Firewall – https://aka.ms/azurefirewall
- Azure DDoS – https://aka.ms/azureddos
- Azure Front Door – https://aka.ms/azurefrontdoor
- Web Application Firewall – https://aka.ms/webapplicationfirewall
- Azure Private Link – https://aka.ms/privatelink
- Microsoft Defender for Cloud – https://aka.ms/asc

Application Security

- GitHub Advanced Security – https://github.com/advanced-security/
- Read our e-book - 6 tips for integrating security into your DevOps practices
- The Open Web Application Security Project (OWASP) – https://owasp.org/
- Microsoft DevSecOps - https://aka.ms/DevSecOpsSolution
- https://owasp.org/www-community/Source_Code_Analysis_Tools

How do I start ?

Security Maturity and Zero Trust

- CSAT (Cybersecurity Assessment) – Funded assessment to help you understand current maturity
- Cloud Direct Zero Trust Assessment – Maturity of security controls aligned to Zero Trust Pillars

DevOps and SDLC (Software Development Lifecycle)

- Cloud Direct DevOps Assessment – Understanding you toolchain to identify efficiencies and best practice.
- Developer Velocity Assessments – are you empowering your developers?

Cloud Direct®

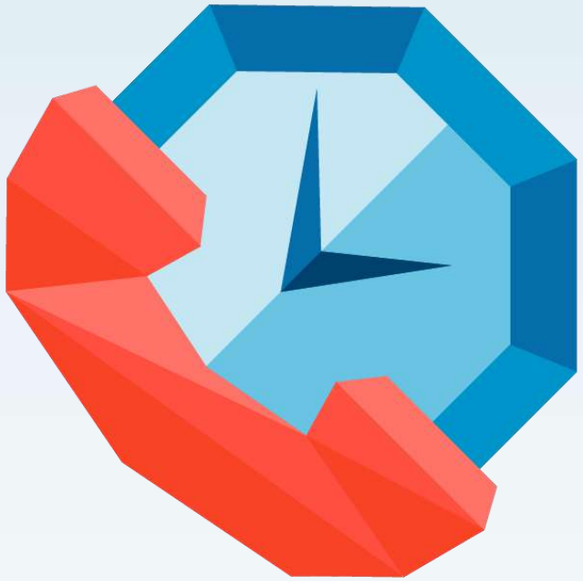
Get in touch

0800 0315 966

sales@clouddirect.net

clouddirect.net

linkedin.com/company/clouddirect



Cloud Direct®