

# Como proteger o seu código usando o Microsoft Defender for DevOps

Valéria Baptista  
valeriaz@microsoft.com



# Who I am?

- Ciências da Computação
- MBA em Cloud Computing
- Pós Docência para Ensino Superior
- Professora na XP Educação
- MCT Microsoft
- Fundadora da comunidade técnica Canal da Cloud.
- Palestrante, entusiasta Cloud e mentora de carreira.



---

# Agenda

- 
- Introductions
  - Why Azure Defender for DevOps
  - Defender for DevOps Architecture
  - Q&A

# Customer challenges

## Fragmented visibility

**Over 54%** of enterprises do not integrate security in DevOps pipelines <sup>1</sup>

**More than half** of enterprises are concerned over rogue applications and compute instances <sup>2</sup>

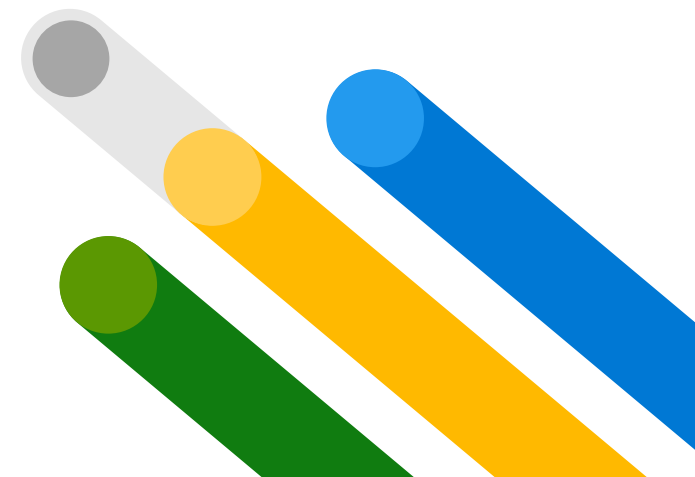
## Lack of insights

**Over 34%** of enterprises lack developer buy-in due to inadequate automation and prioritization <sup>3</sup>

## Pervasive silos

**Over 50%** of enterprises indicate DevOps and security silos as the biggest challenge to implement DevSecOps <sup>4</sup>

1. Microsoft Enterprise DevOps Report  
2. SANS 2022 Cloud Security Survey  
3. Rethinking the Sec in DevSecOps: Security as Code A SANS Survey  
4. Rethinking the Sec in DevSecOps: Security as Code A SANS Survey



# Microsoft's cloud-native application protection platform

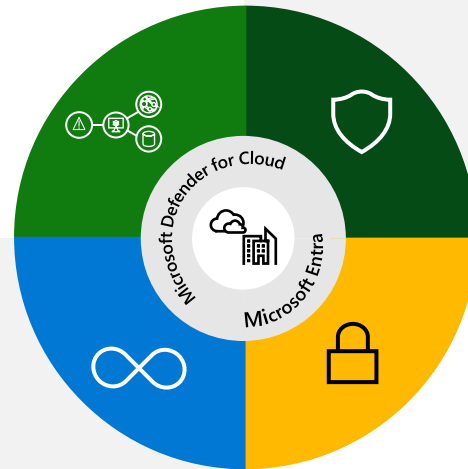


## Cloud security posture management

Full visibility and contextual insights to identify and remediate your most critical risk

## DevSecOps

Unify your DevOps security management across multi-pipelines



## Cloud workload protection

Detect and respond to modern threats across your cloud workloads in runtime

## Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM



Microsoft Purview  
(Data protection, governance and compliance)



Microsoft Defender External  
Attack Surface Management  
(EASM)



Azure Network Security



Microsoft Sentinel  
(SIEM)

# How we're different



## Multi-cloud and hybrid support

- » Streamlined auto-provisioning for new resources
- » Multicloud security benchmark for compliance
- » Multicloud agentless vulnerability scanning
- » Built in with Azure with no deployment required and the broadest protection coverage



## Contextual code to cloud security

- » Integrated view across clouds to manage security posture, assess risk, and take required actions
- » Prioritized recommendations with attack path, reducing noise by up to 99%
- » Track and manage your security posture state over time



## Full-lifecycle protection

- » Manage security of cloud-native applications with a single platform
- » Minimize vulnerabilities from making it to production with code scanning and IaC scanning
- » Reduce time to remediate with integrated workflows into developer environments



## Advanced Threat Protection

- » Workload-specific signals and threat alerts
- » CWPP with dedicated workload protection for Azure storage and databases
- » Deterministic, AI, and anomaly-based detection mechanisms
- » Leverages the power of Microsoft Threat Intelligence with 43 trillion signals daily



Cloud Security

# Code to cloud

# Empower security teams with unified DevOps security management across multipipeline and multicloud environments



Unify visibility into  
DevOps security posture



Strengthen cloud  
resource configurations



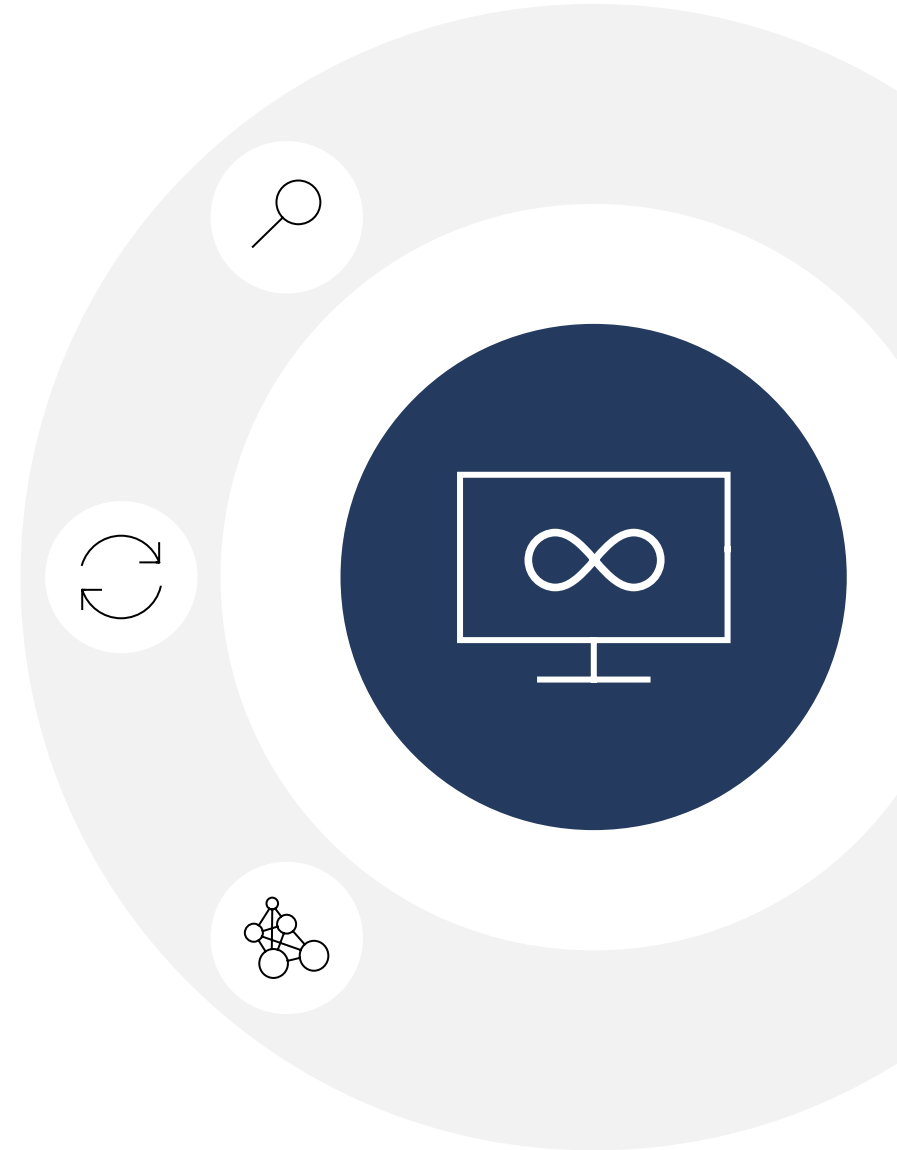
Automate with integrated  
security intelligence



# Unify visibility into DevOps security posture

Shifting cloud security left,  
bridging SecOps and DevOps

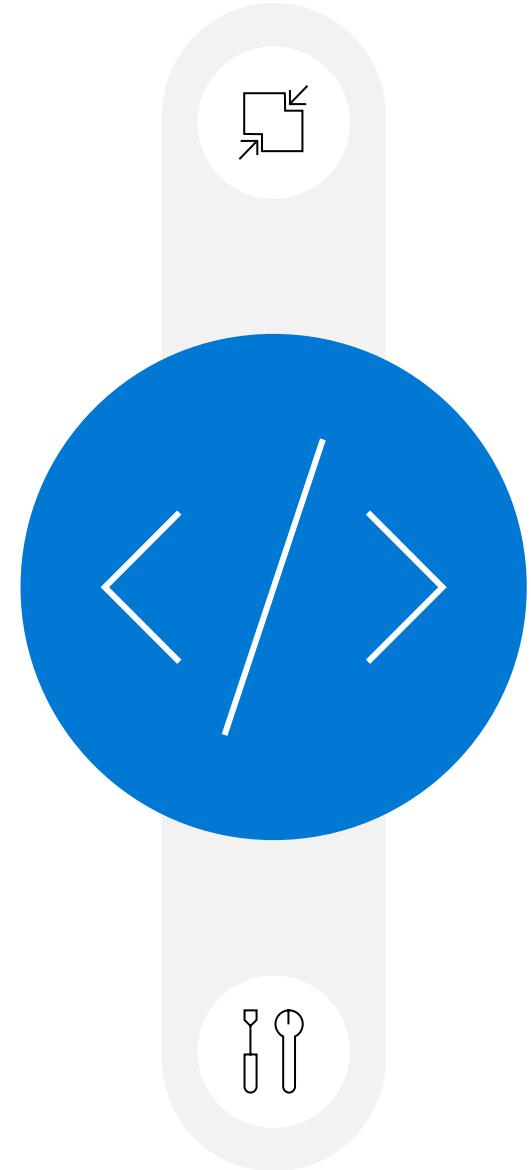
- » Automated discovery
- » Continuous assessment
- » Security insights



# Strengthen cloud resource configurations in code

Prevent security issues from reaching production

- » Discover Infrastructure-as-Code misconfigurations
- » Secure Containers and Code
- » Multi-Cloud Support



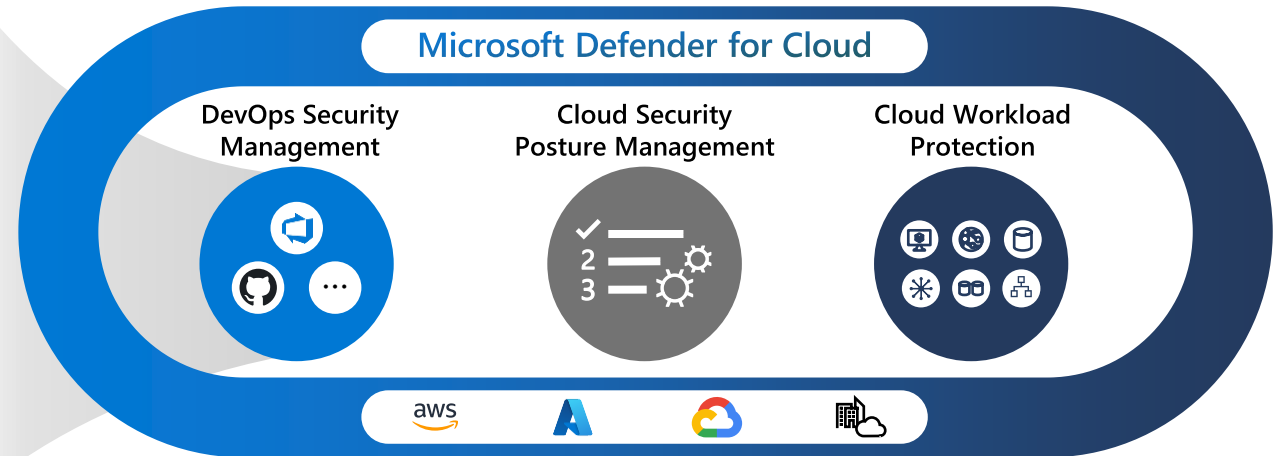
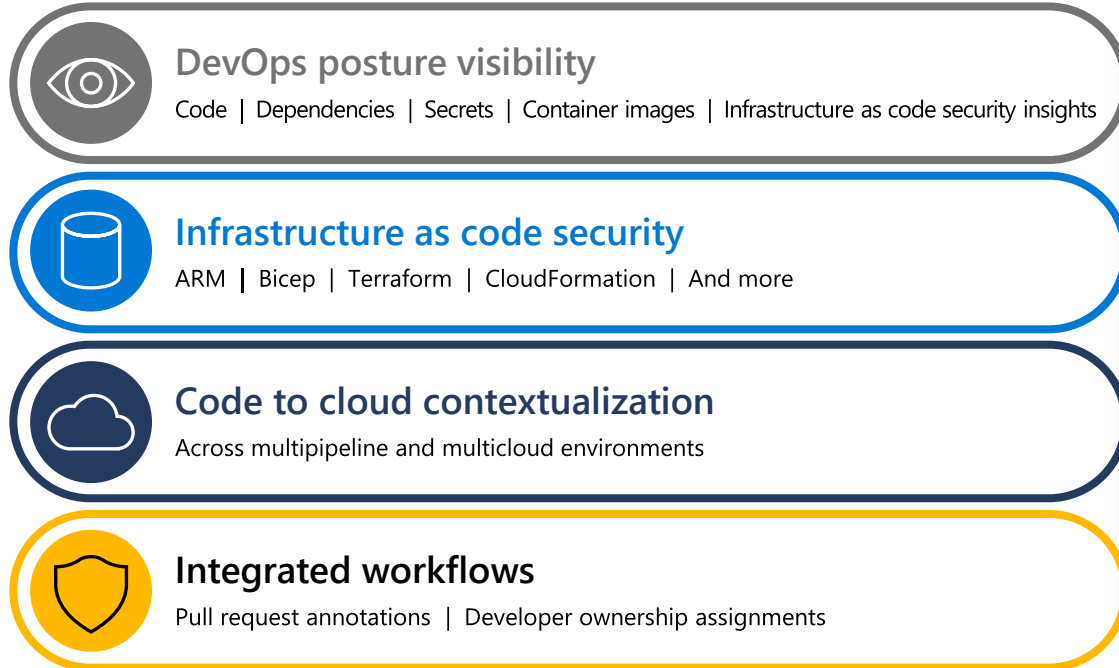
# Automate with integrated security intelligence

Simplify to remediate faster,  
do more with less!

- » Code to cloud contextualization
- » Prioritize critical security issues
- » Drive remediation in code







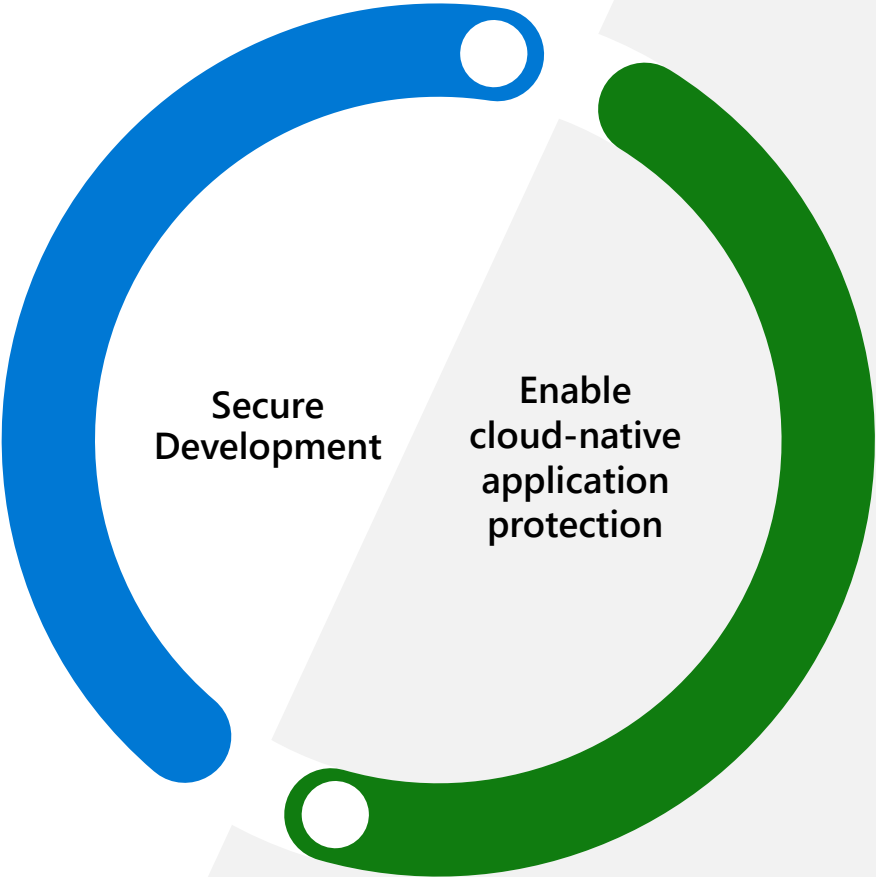
# Defender for DevOps Architecture



# Better Together





GitHub Advanced Security on  
GitHub and Azure DevOps  
Developer first. Community driven

-  Code security
-  Dependencies security
-  Embedded secrets protection
-  Developer code remediation



## Defender for DevOps

Unify multi-pipeline DevOps security

- Multi-pipeline DevOps security management** 
- Infrastructure-as-Code security** 
- Code to cloud contextualization** 
- Automated workflows** 

# Unify visibility into DevOps security posture

## » Automated discovery

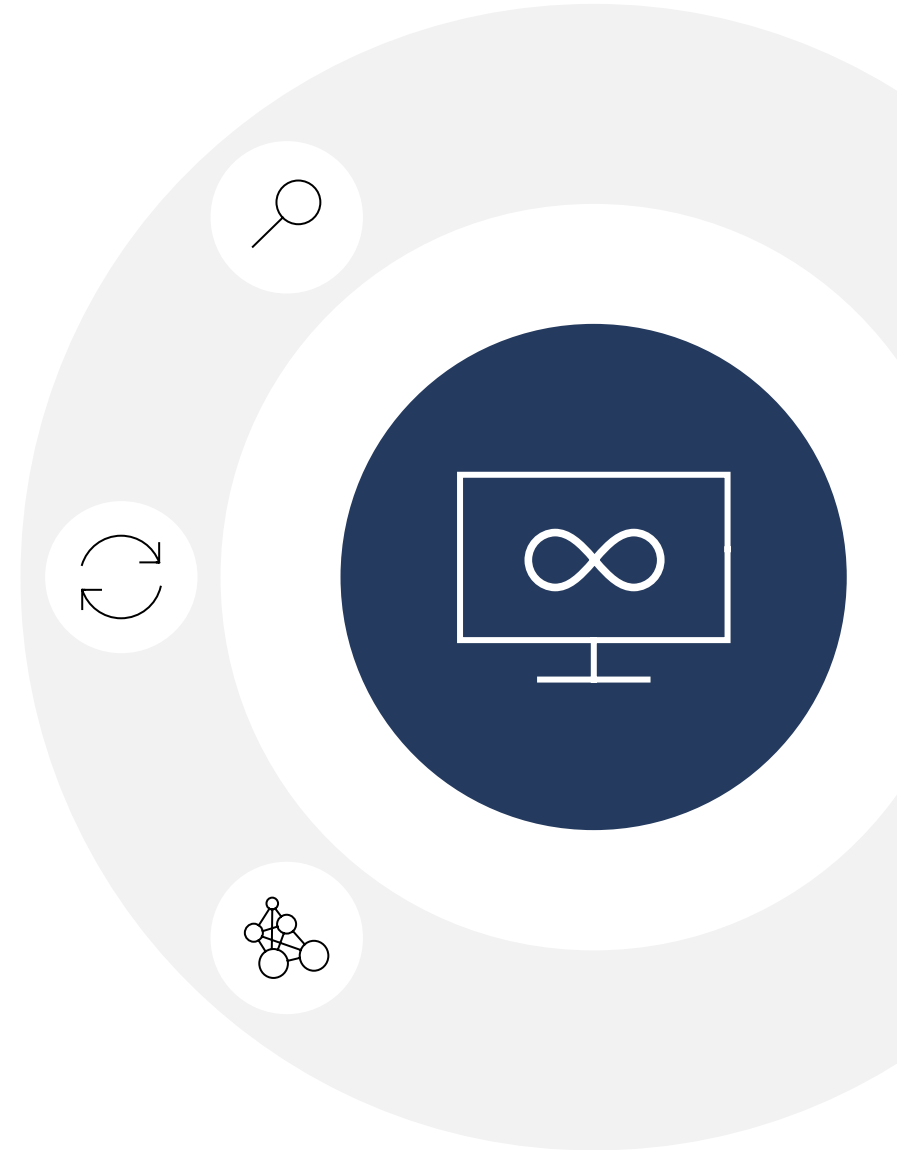
- Full DevOps inventory
- Multipipeline (GitHub, Azure DevOps)

## » Continuous assessment

- DevOps environment hardening
- Continuum between developers and SecOps
- DevOps compliance

## » Security insights

- Single console to manage DevOps security
- Custom workbooks



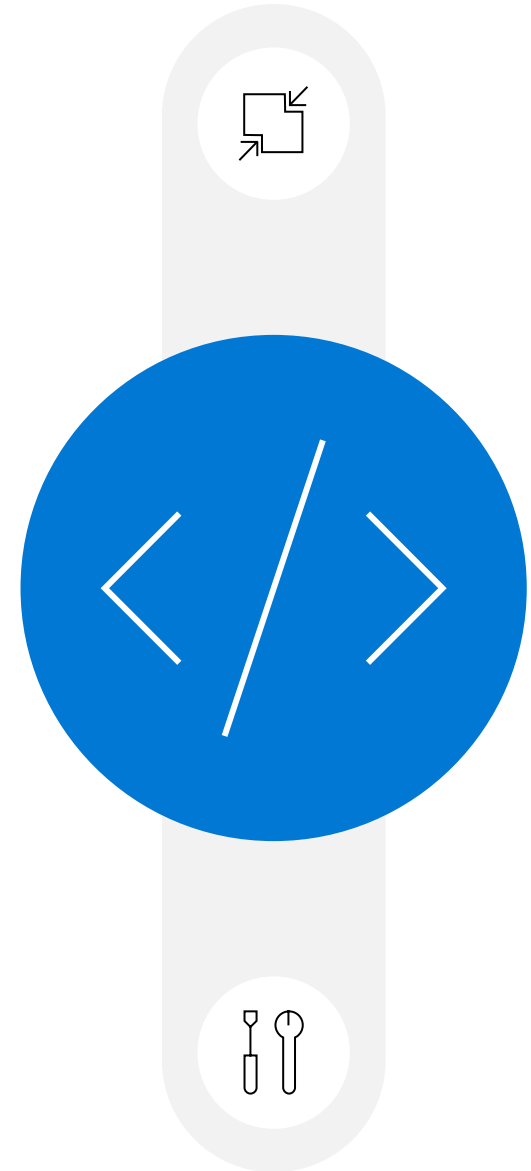
# Strengthen cloud resource configurations in code

## » Discover Infrastructure-as-Code misconfigurations

- Apply Azure Security Benchmark checks to Infrastructure-as-Code templates
- Discover security issues in Infrastructure-as-Code templates
- Empower developers with clear remediation guidance
- Identify security issues to the line of code for quick fixes

## » Multi-Cloud Support

- Support ARM, Bicep, Helm, CloudFormation, Terraform templates



# Automate with integrated security intelligence

## » Code to cloud contextualization

- Enrich cloud security graph with application code insights

## » Prioritize critical security issues in code

- OSS Vulnerabilities
- Exposed credentials

## » Drive remediation in code

- Custom workflows for developer ownership assignments (Logic App)
- SecOps initiated Pull Request annotations





# Unify visibility into DevOps security posture



## » Automated discovery

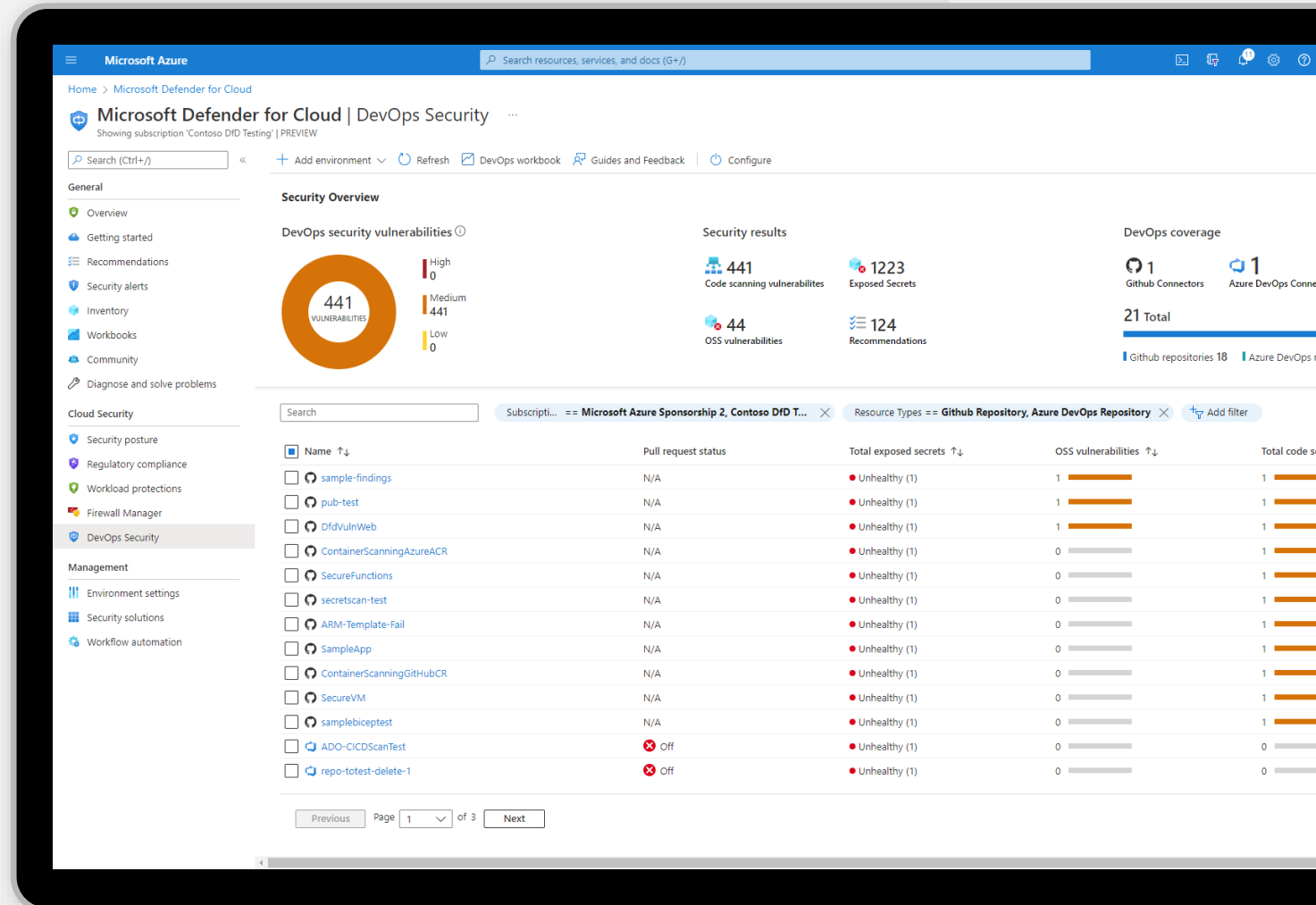
- Full DevOps inventory
- Multi-pipeline (GitHub, Azure DevOps)

## » Continuous assessment

- DevOps environment hardening
- Create a continuum between developers and SecOps
- DevOps compliance

## » Security insights

- Single console to manage DevOps security
- Custom workbooks



# Strengthen cloud resource configurations in code



## » Discover Infrastructure-as-Code misconfigurations

- Apply Azure Security Benchmark checks to Infrastructure-as-Code templates
- Identify security issues to the line of code for quick fixes
- Empower developers with clear remediation guidance

## » Multi-Cloud Support

- Support ARM, Bicep, Helm, CloudFormation, Terraform templates

The screenshot displays the Microsoft Azure (Preview) portal interface. At the top, there's a navigation bar with the Microsoft Azure (Preview) logo, a 'Report a bug' button, and a search bar. Below the navigation bar, the page title is 'Code repositories should have infrastructure as code scanning findings resolved'. The page content is organized into sections: 'Severity' (Medium), 'Freshness interval' (30 Min), and 'Tactics and techniques' (Initial Access +1). The 'Description' section explains that Defender for DevOps has found infrastructure as code security configuration issues in repositories. The 'Remediation steps' section is currently expanded, showing a table of findings. The table has columns for ID, Security check, Category, Applies to, and Severity. The findings are listed as follows:

ID	Security check	Category	Applies to	Severity
fed0cc5f-7e87-fdbe-2f4a-130656da8397	SQL servers with auditing to storage account destination sh...	Infrastructure as Code	8 of 57 resources	Medium
4d51611b-9af6-dfde-095a-aec22e861a5	Managed identity should be used in your API App.	Infrastructure as Code	8 of 57 resources	Medium
c0faa81b-66f2-442e-ea50-8aea3ff7910f	FTPS only should be required in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
0717f465-6b08-c906-5d2f-b5d0ccf25a17	Web Application should only be accessible over HTTPS.	Infrastructure as Code	8 of 57 resources	Medium
c2e82186-a886-c27b-f7be-c04fc65680f4	Latest TLS version should be used in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
9fba18b6-dafd-7e9d-45b9-f230e6b0d735	Managed identity should be used in your Web App.	Infrastructure as Code	8 of 57 resources	Medium
79071d15-d0cf-4fb9-641b-a6dd8a542138	Diagnostic logs in App Services should be enabled.	Infrastructure as Code	8 of 57 resources	Medium
c25f476b-a403-1520-1e5b-1cbd813fc9dc	FTPS only should be required in your Function App.	Infrastructure as Code	8 of 57 resources	Medium
43356200-4594-ba54-b3ba-7cfe315358e9	Function App should only be accessible over HTTPS.	Infrastructure as Code	8 of 57 resources	Medium
eeefd957-fef7-ec76-4f23-0fb764736462	Latest TLS version should be used in your Function App.	Infrastructure as Code	8 of 57 resources	Medium

At the bottom of the page, there are buttons for 'Trigger logic app', 'Assign owner', and 'Change owner and set ETA'. A feedback section asks 'Was this recommendation useful?' with 'Yes' and 'No' radio buttons.

# Automate with integrated security intelligence



## » Code to cloud contextualization

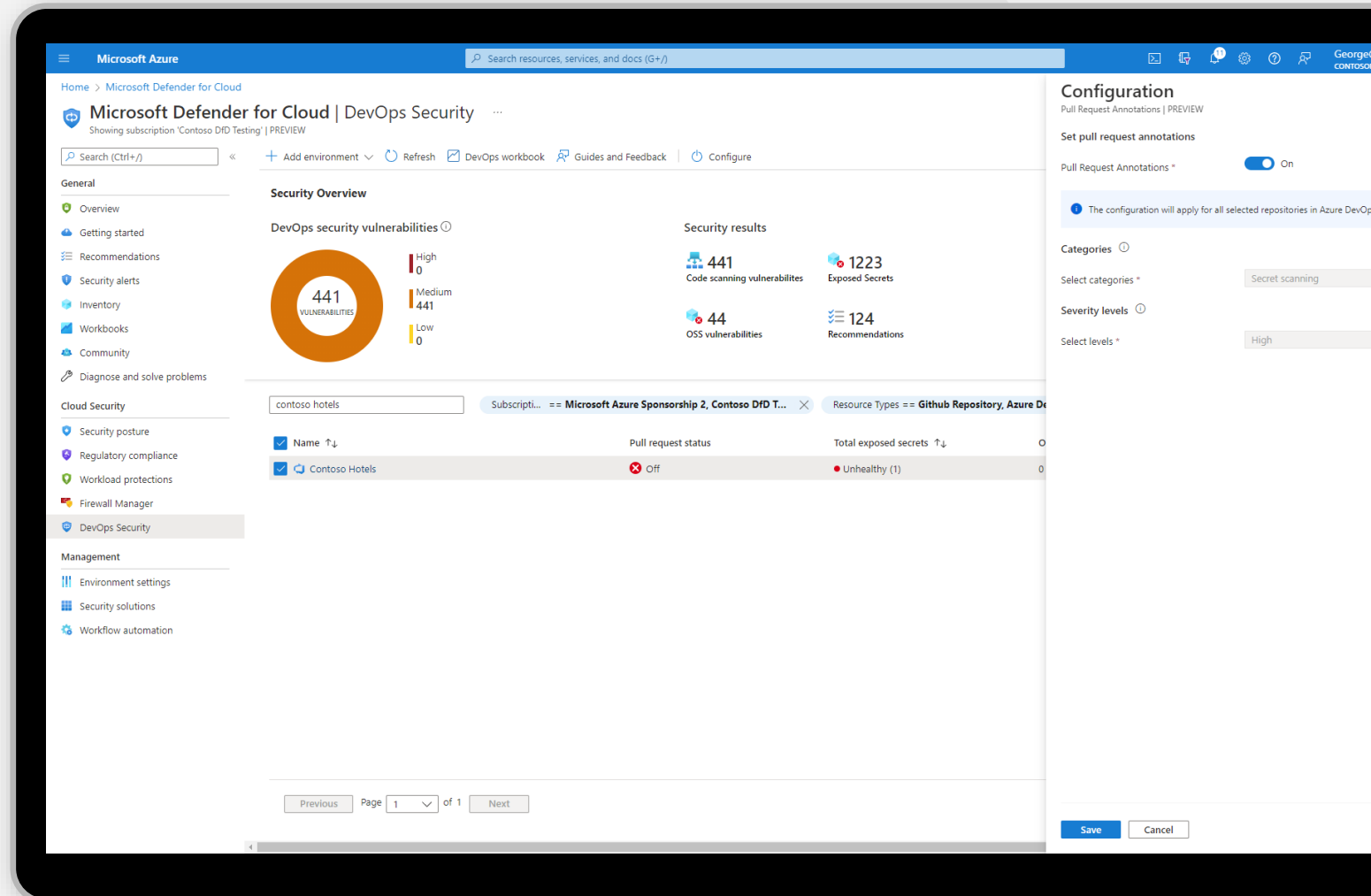
- Enrich cloud security graph with application code insights

## » Prioritize critical security issues in code

- OSS Vulnerabilities
- Exposed credentials

## » Drive remediation in code

- Custom workflows for developer ownership assignments
- SecOps initiated Pull Request annotations





# DEMO

Unify visibility into DevOps security posture



Thank You!

