

Defender for DevOps –

Unify security management for DevOps

Lukasz Szankowski
Security CSA



Microsoft's cloud-native application protection platform (CNAPP)

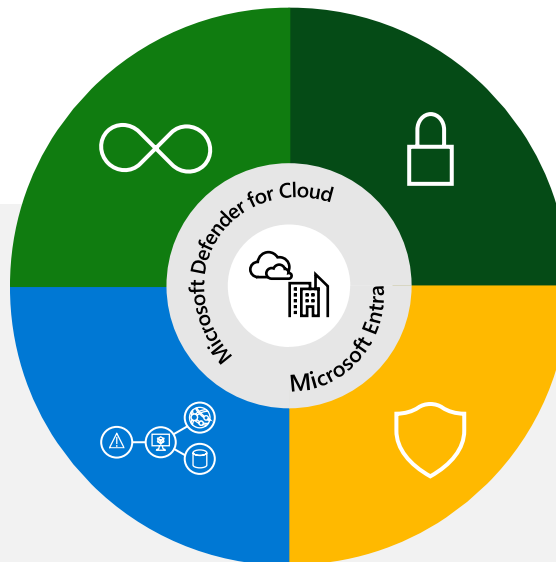


DevSecOps

Unify your DevOps security management across multi-pipelines

Cloud security posture management

Visibility and contextual insights to identify and help remediate your most critical risk



Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM

Cloud workload protection

Help detect and respond to modern threats across your cloud workloads in runtime

Integrated to protect across your cloud infrastructure

Microsoft Purview
(Data Security)

Microsoft Defender External
Attack Surface Management
(EASM)

Azure Network Security

Microsoft Sentinel
(SIEM)

Customer challenges

Fragmented visibility

Over 54% of enterprises do not integrate security in DevOps pipelines ¹

More than half of enterprises are concerned over rogue applications and compute instances ²

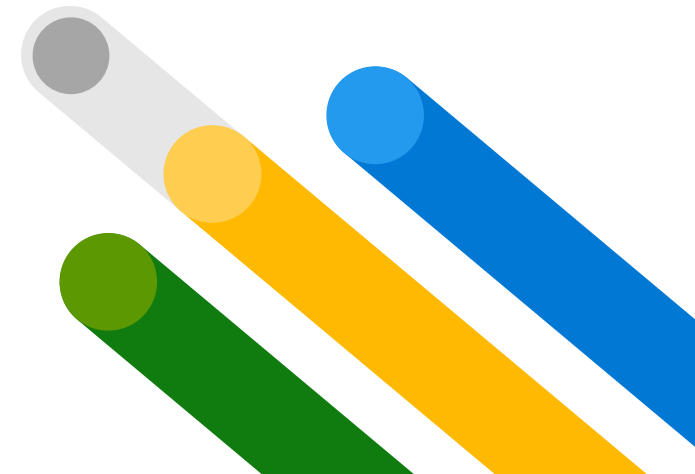
Lack of insights

Over 34% of enterprises lack developer buy-in due to inadequate automation and prioritization ³

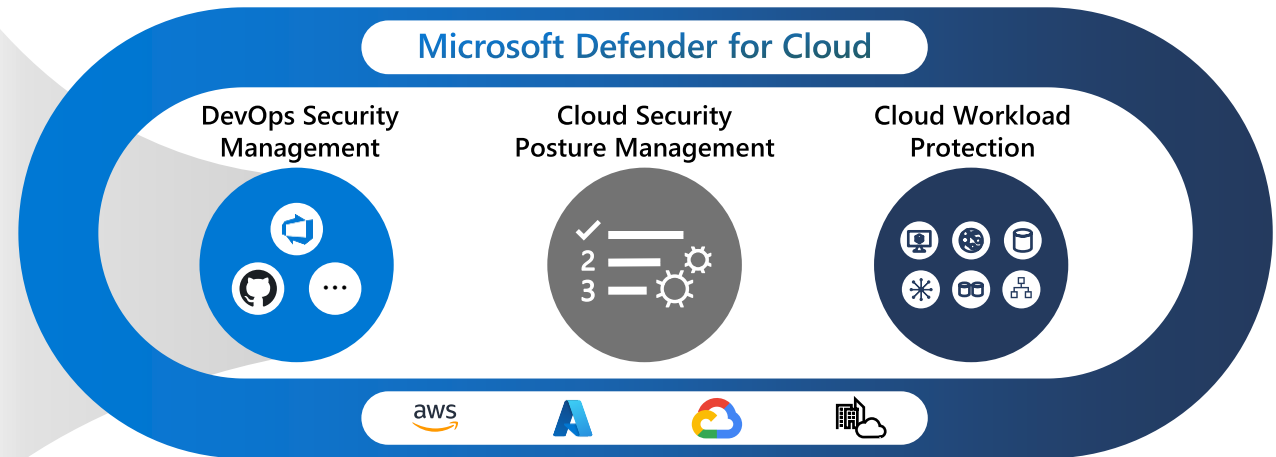
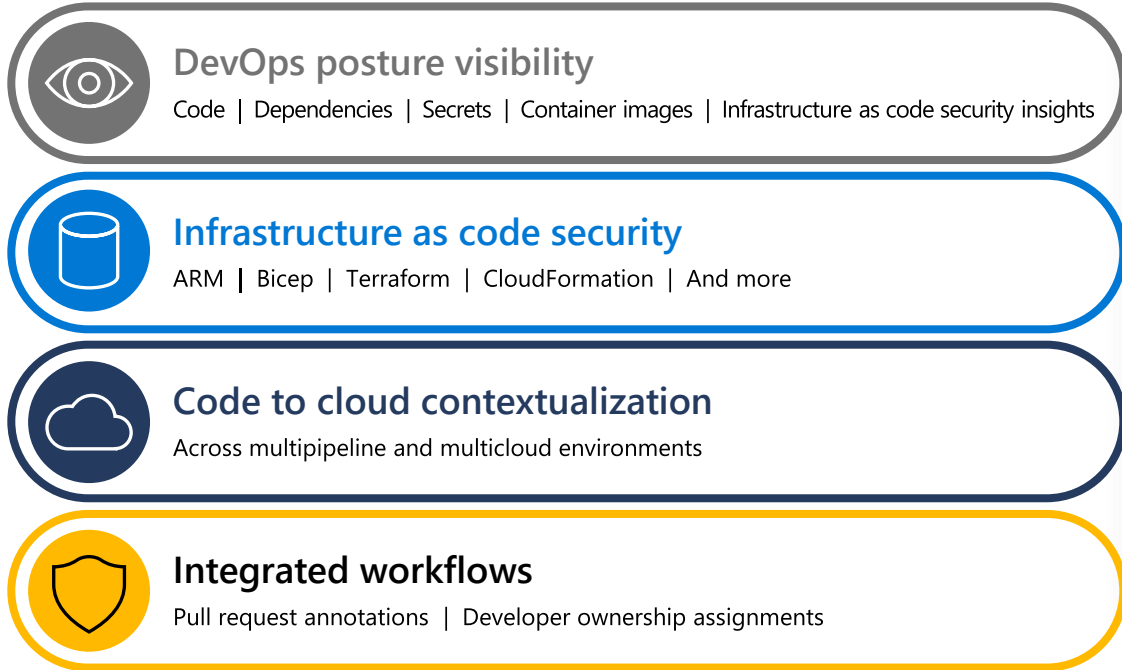
Pervasive silos

Over 50% of enterprises indicate DevOps and security silos as the biggest challenge to implement DevSecOps ⁴

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



Defender for DevOps architecture



Unify visibility into DevOps security posture



» Automated discovery

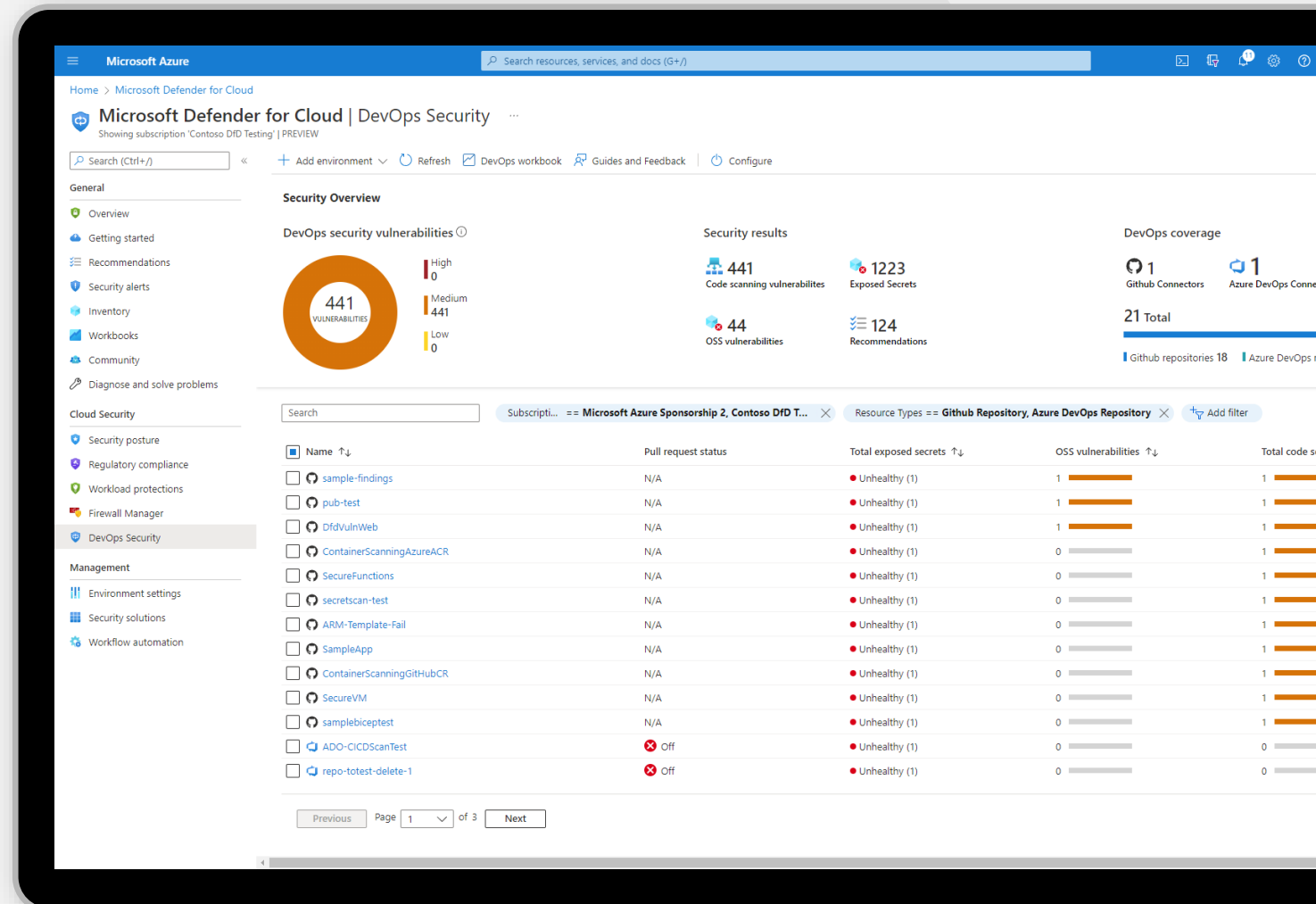
- Full DevOps inventory
- Multi-pipeline (GitHub, Azure DevOps)

» 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) interface, specifically the Microsoft Defender for Cloud Recommendations page. The main heading is "Code repositories should have infrastructure as code scanning findings resolved". The severity is "Medium", the freshness interval is "30 Min", and there are "Initial Access +1" tactics and techniques. The description states: "Defender for DevOps has found infrastructure as code security configuration issues in repositories. The issues shown below have been detected in template files. To improve the security posture of the related cloud resources, it is highly recommended to remediate these issues." The remediation steps and affected resources sections are collapsed. The security checks section is expanded, showing a table of findings.

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-aeec22e861a5	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
79071df5-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-7cfe315359e9	Function App should only be accessible over HTTPS.	Infrastructure as Code	8 of 57 resources	Medium
eeefd957-fef7-ec76-f23-0fb764736462	Latest TLS version should be used in your Function App.	Infrastructure as Code	8 of 57 resources	Medium

At the bottom of the findings table, there are buttons for "Trigger logic app", "Assign owner", and "Change owner and set ETA". Below the table, there is a feedback question: "Was this recommendation useful?" with radio buttons for "Yes" and "No".

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

Microsoft Azure

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | DevOps Security

Showing subscription: 'Contoso DFD Testing' | PREVIEW

Search (Ctrl+F) Add environment Refresh DevOps workbook Guides and Feedback Configure

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security

Management

- Environment settings
- Security solutions
- Workflow automation

Security Overview

DevOps security vulnerabilities

441 VULNERABILITIES

High 0
Medium 441
Low 0

Security results

441 Code scanning vulnerabilities
1223 Exposed Secrets
44 OSS vulnerabilities
124 Recommendations

contoso hotels Subscripti... == Microsoft Azure Sponsorship 2, Contoso DFD T... Resource Types == Github Repository, Azure D...

Name	Pull request status	Total exposed secrets
Contoso Hotels	Off	Unhealthy (1)

Previous Page 1 of 1 Next

Save Cancel

Demo



Thank you

