Defender for DevOps –

Unify security management for DevOps

Lukasz Szankowski
Security CSA

Microsoft Security

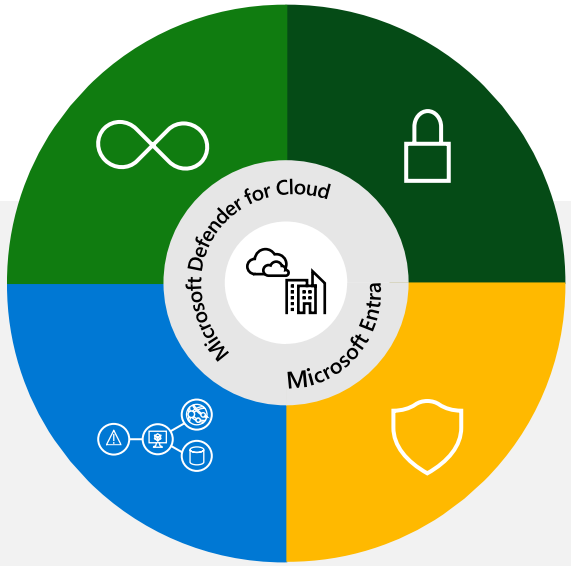
Microsoft's cloud-native application protection platform (CNAPP)

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)

Microsoft Security

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

DevOps posture visibility

Code | Dependencies | Secrets | Container images | Infrastructure as code security insights

Infrastructure as code security

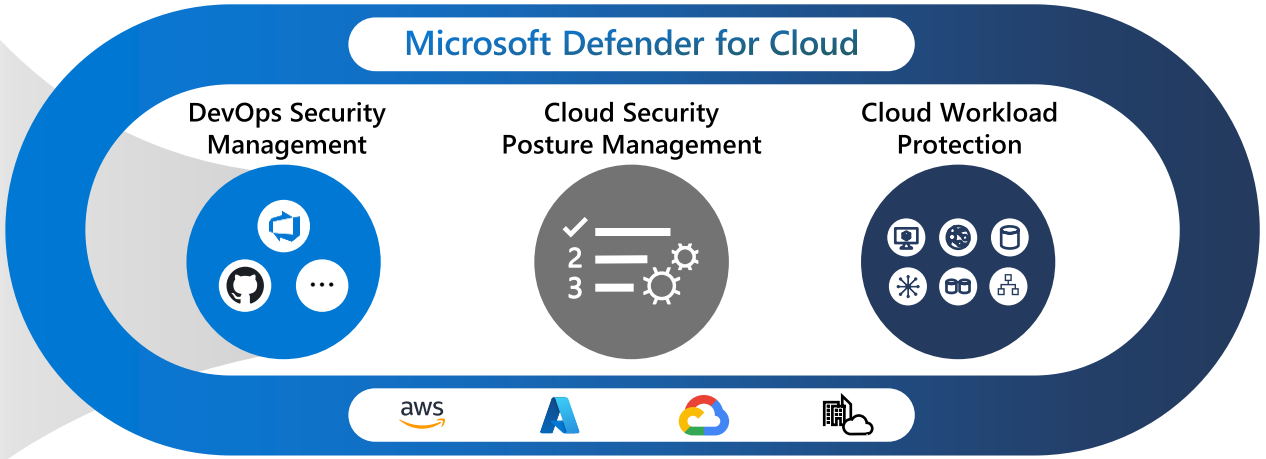
ARM | Bicep | Terraform | CloudFormation | And more

Code to cloud contextualization

Across multipipeline and multicloud environments

Integrated workflows

Pull request annotations | Developer ownership assignments



Microsoft Security

Unify visibility into DevOps security posture

Automated discovery

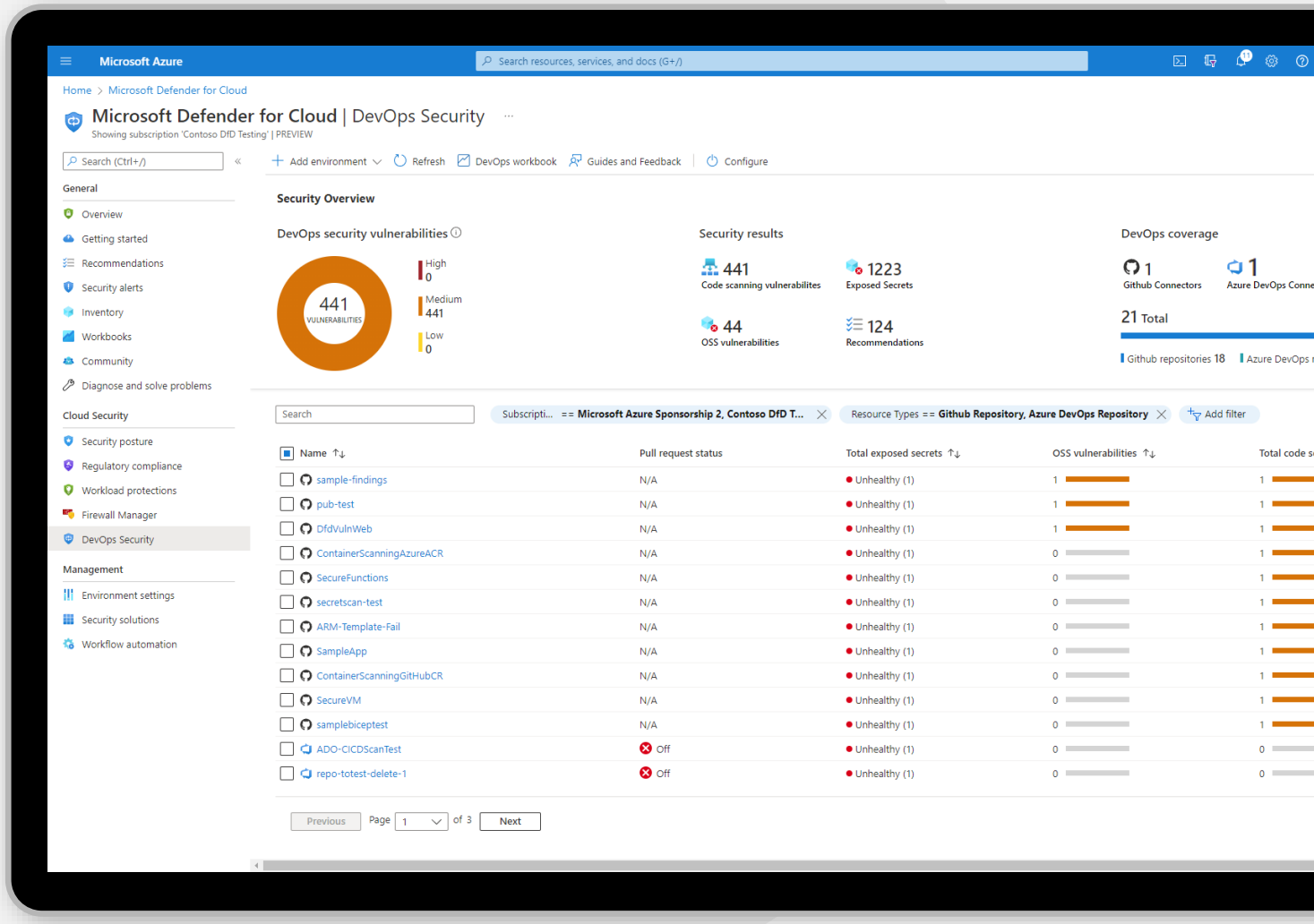
- Full DevOps inventory
- Multi-pipeline (GitHub, Azure DevOps)

Continuous assessment

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

Security insights

- Single console to manage DevOps security
- Custom workbooks



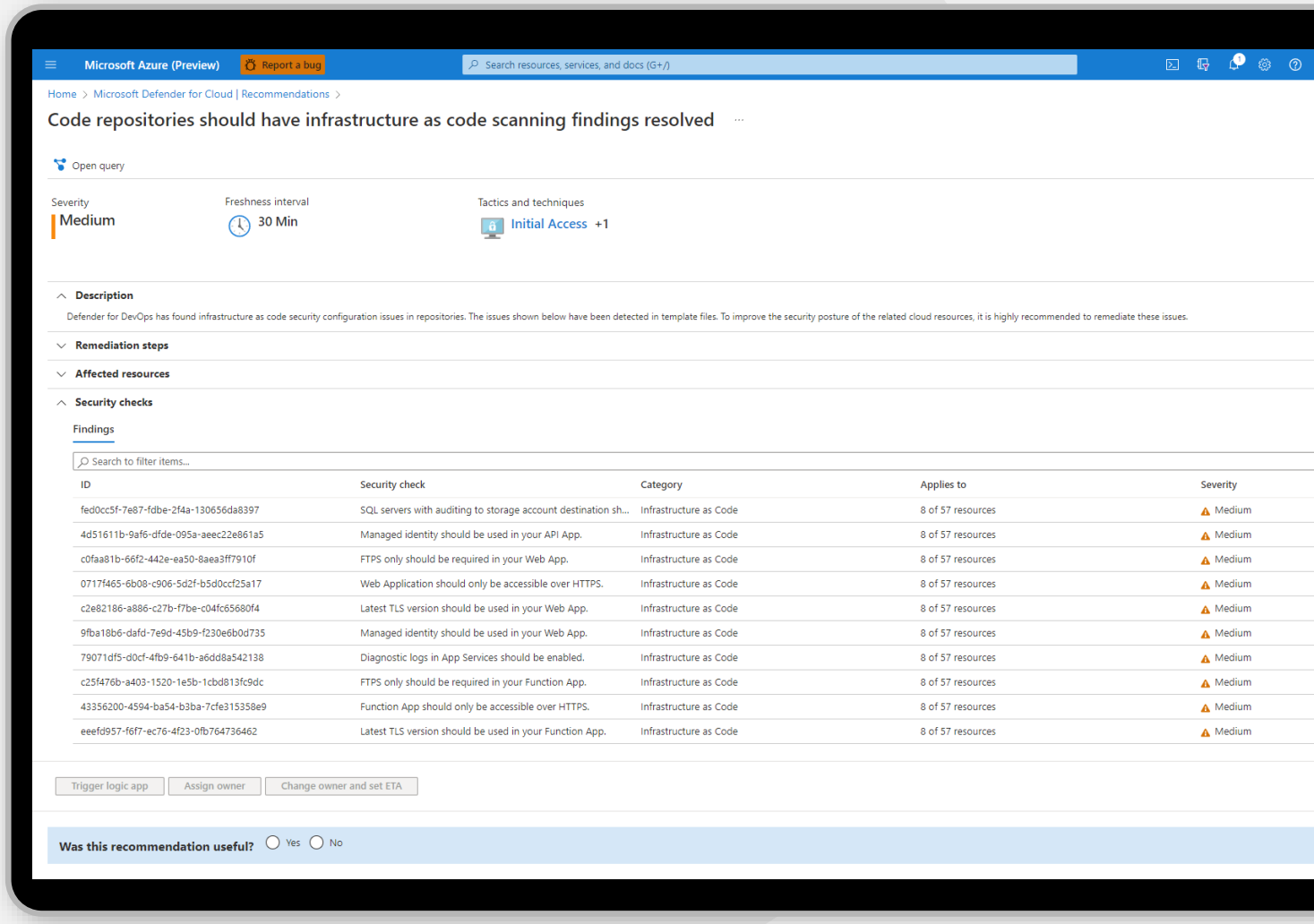
Strengthen cloud resource configurations in code

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



Automate with integrated security intelligence

Code to cloud contextualization

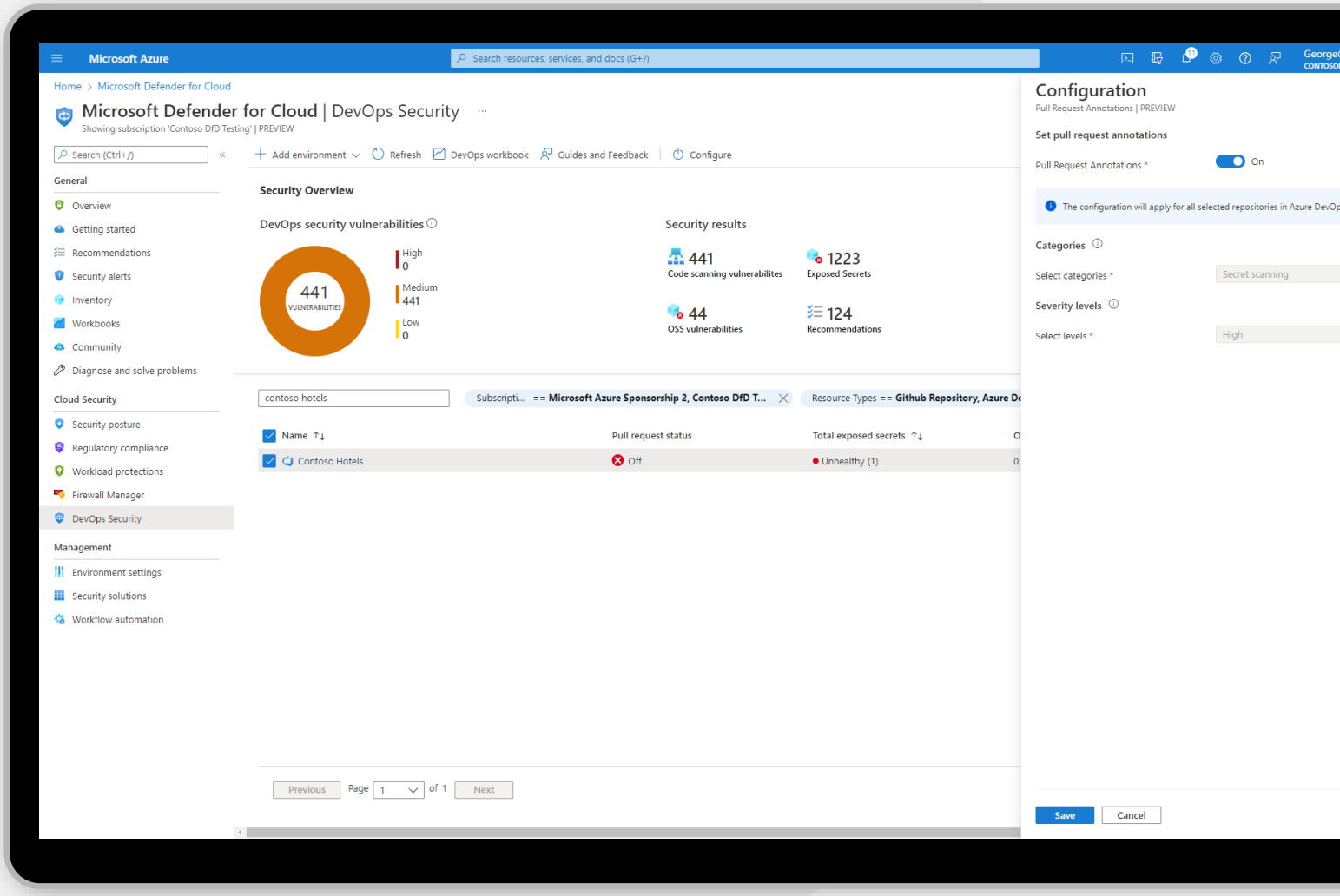
- Enrich cloud security graph with application code insights

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

Thank you