Security Management Capabilities in Microsoft Azure

Vlad Catrinescu

Microsoft MVP | Independent Consultant

@vladcatrinescu | VladTalksTech.com | YouTube.com/@VladTalksTech

Overview

Introduction to DevSecOps, CSPM, and CWPP

Protecting cloud-based applications with Microsoft Defender for Cloud

Introduction to DevSecOps, CSPM, and CWPP

DevSecOps

DevSecOps (short for development, security, and operations) is a development practice that integrates security initiatives at every stage of the software development lifecycle to deliver robust and secure applications. DevSecOps infuses security into the continuous integration and continuous delivery (CI/CD) pipeline, allowing development teams to address some of today's most pressing security challenges at DevOps speed.

https://www.vmware.com/ca/topics/glossary/content/devsecops.html

Cloud Workload Protection Platform

A cloud workload protection platform (CWPP) is a security tool that detects and removes threats inside cloud software. A CWPP is like an automobile mechanic who identifies flaws and breakdowns inside a car's engine before they cause further damage — only it inspects the interior of cloud services, not cars. CWPPs automatically monitor a wide range of workloads, including physical on-premise servers, virtual machines, and serverless functions.

https://www.cloudflare.com/learning/cloud/what-is-cwpp/

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) is a market segment for IT security tools that are designed to identify misconfiguration issues and compliance risks in the cloud. An important purpose of CSPM programming is to continuously monitor cloud infrastructure for gaps in security policy enforcement.

https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM

Cloud Security Posture Management

Misconfigurations of a cloud environment are the most common mistake in the cloud

- Can lead to a data breach

CSPM tools can reduce cloud-based security incidents due to a misconfiguration by 80%

- According to Gartner

Combination of Tools and Services

Zero Trust-based access control

Real-time risk scoring

Threat and vulnerability management

Discovering sharing risks

Technical policies

Threat modeling

Protecting Cloud-based Applications with Microsoft Defender for Cloud

Microsoft Defender for Cloud

Microsoft Defender for Cloud is a cloud-native application protection platform that is made up of security measures and practices that are designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

DevSecOps

A development security operations solution that unifies security management at the code level across multicloud and multiple-pipeline environments

CSPM

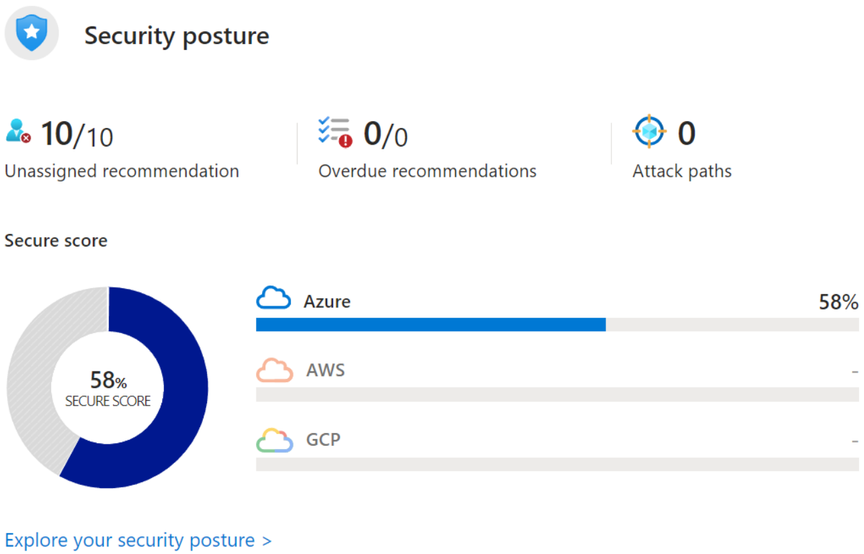
A cloud security posture management solution that surfaces actions that you can take to prevent breaches

CWPP

A cloud workload protection platform with specific protections for servers, containers, storage, databases, and other workloads

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Secure Score



Microsoft Defender for cloud aggregates your security posture in a single score

Provides concrete actions to increase your security

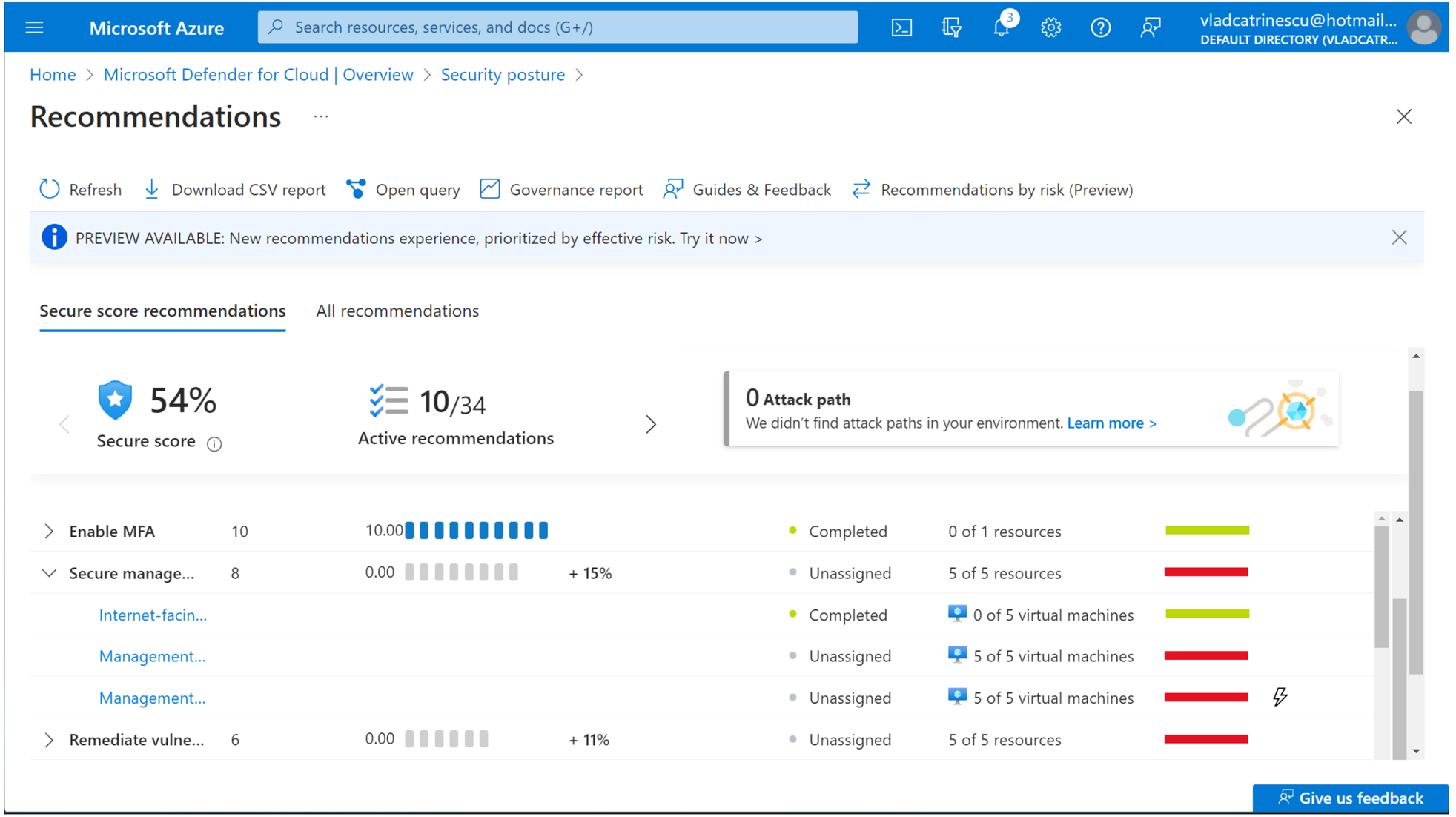
- Bigger the security impact – more points it's worth

Secure score is continuously updated

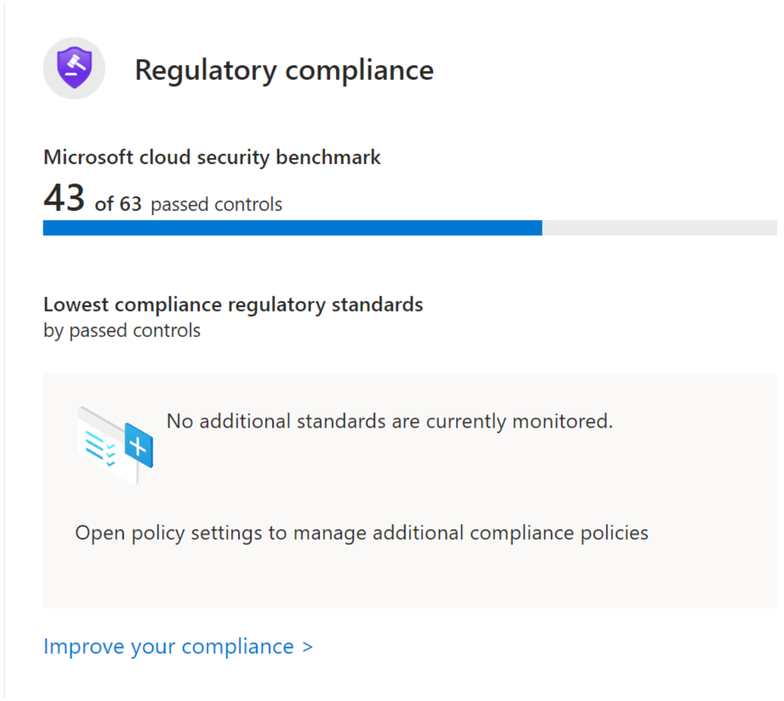
- Depending on resources added to your subscriptions

Evaluates Azure, AWS, and GCP resources

Hardening Recommendations



Regulatory Compliance



Single consolidated view of Microsoft security recommendations

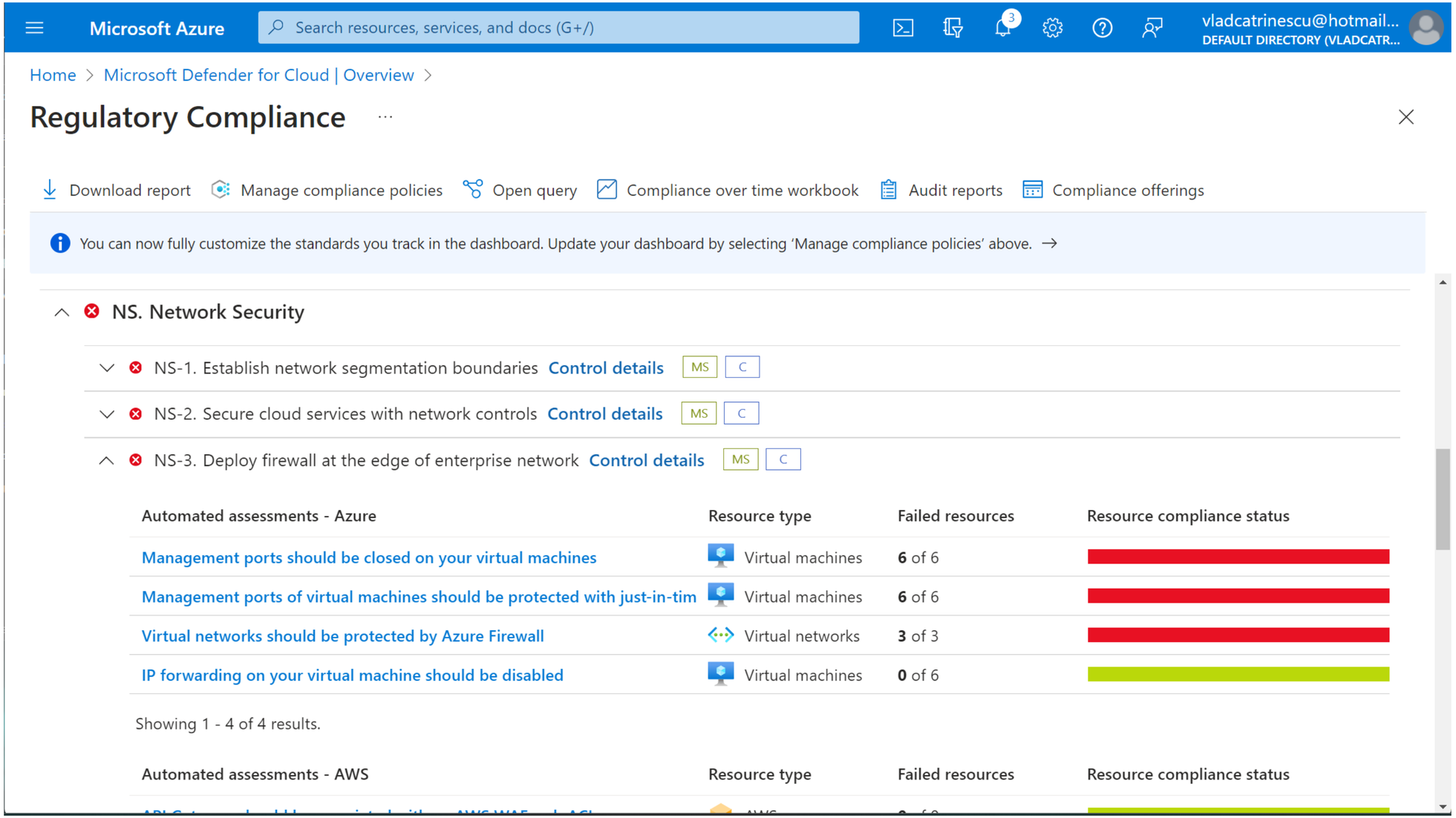
Can help meet regulatory standards such as

- NIST SP-800
- HIPAA
- ISO 27001

Default to the Microsoft cloud security benchmark (MCSB)

- Microsoft authored set of guidelines with controls from
  - Center for Internet Security (CIS)
  - National Institute of Standards and Technology (NIST)

Regulatory Compliance



Key Information

Control domain	High-level description of a feature or activity that needs to be addressed and isn't specific to a technology or implementation
Mapping to industry frameworks	Mapping to CIS, NIST, or Payment Card Industry Data Security Standards (PCI DSS) frameworks
Recommendation	Each control area has multiple recommendations on how to secure your cloud resources. Ex: Establish network segmentation boundaries
Azure Guidance	Technical instructions on how to implement the recommendation in Azure
AWS | GCP Guidance	Microsoft also provides instructions for AWS and Google Cloud Platform

Control Domains

Recommendation

Mapping to industry frameworks

Azure Guidance

Filter by title

- Microsoft cloud security benchmark
- Introduction
- MCSB Controls (v1)
  - Overview of MCSB controls
  - **Network security**
  - Identity management
  - Privileged Access
  - Data protection
  - Asset management
  - Logging and threat detection
  - Incident response
  - Posture and vulnerability management
  - Endpoint security

Download PDF

NS-7: Simplify network security configuration

Expand table

CIS Controls v8 ID(s)	NIST SP 800-53 r4 ID(s)	PCI-DSS ID(s) v3.2.1
4.4, 4.8	AC-4, SC-2, SC-7	1.1, 1.2, 1.3

Security principle: When managing a complex network environment, use tools to simplify, centralize and enhance network security management.

Azure guidance: Use the following features to simplify the implementation and management of the virtual network, NSG rules, and Azure Firewall rules:

- Use Azure Virtual Network Manager to group, configure, deploy, and manage virtual networks and NSG rules across regions and subscriptions.
- Use Microsoft Defender for Cloud Adaptive Network Hardening to recommend NSG hardening rules that further limit ports,

Certification

Microsoft Certified: Azure Network Engineer Associate - Certifications

As a candidate for this certification, you should have subject matter expertise in planning, implementin...

Documentation

Microsoft cloud security benchmark - Data protection

Microsoft cloud security benchmark - Data protection

Microsoft cloud security benchmark - Identity Management

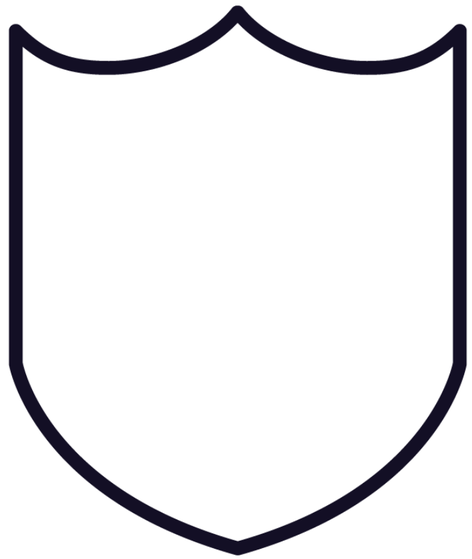
Microsoft cloud security benchmark - Identity Management

Microsoft cloud security benchmark - Backup and recovery

Microsoft cloud security benchmark -Backup and recovery

Show 5 more

Microsoft Defender for Cloud Plans: CWPP



Microsoft Defender plans

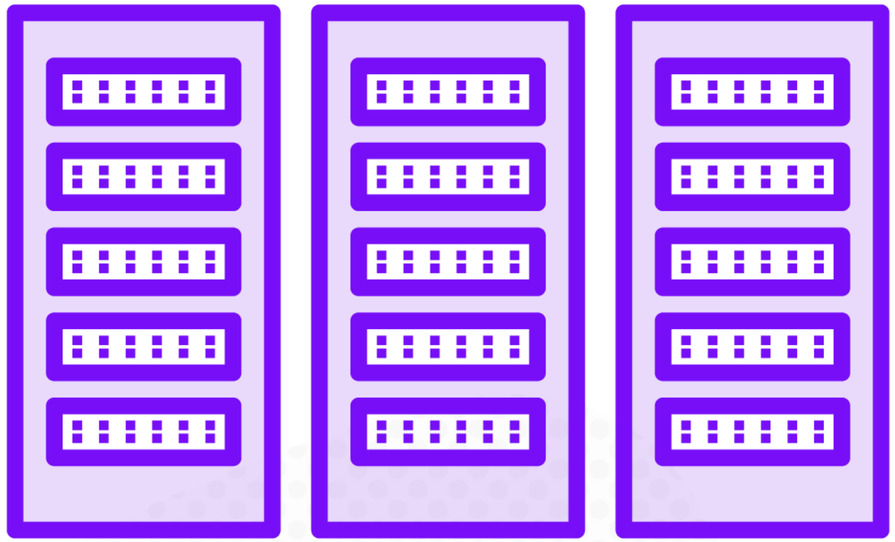
- Microsoft Defender for servers
- Microsoft Defender for App Service
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Kubernetes
- Microsoft Defender for container registries
- Microsoft Defender for Key Vault
- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS

Hybrid Cloud Protection

Microsoft Defender can also protect

- Virtual machines in other clouds (AWS/GCP)
- Non-Azure/On-premises servers

Enabled by Azure Arc



Microsoft Defender Security Alerts

Microsoft Defender can generate alerts when it detects a threat in your environment

Alerts can trigger workflows in Azure Logic Apps

Alerts can be exported to a SIEM service such as Microsoft Sentinel

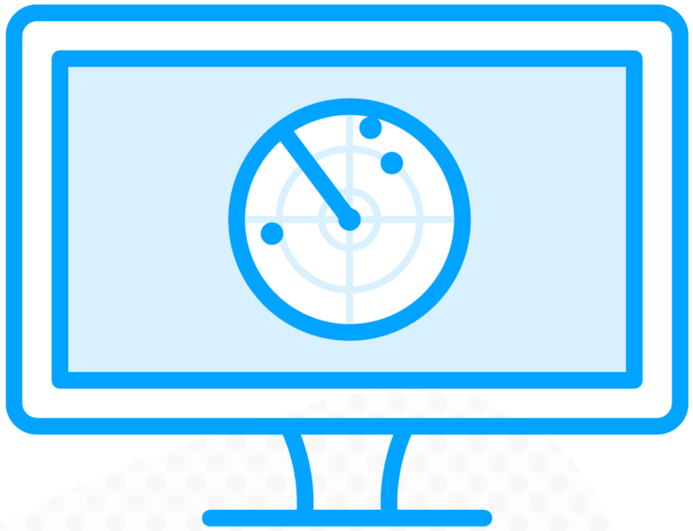
- More on that in the next module!

Vulnerability Assessment and Management

Includes vulnerability scanning for VMs/ containers

Powered by Qualys

Findings are reported in Defender for Cloud

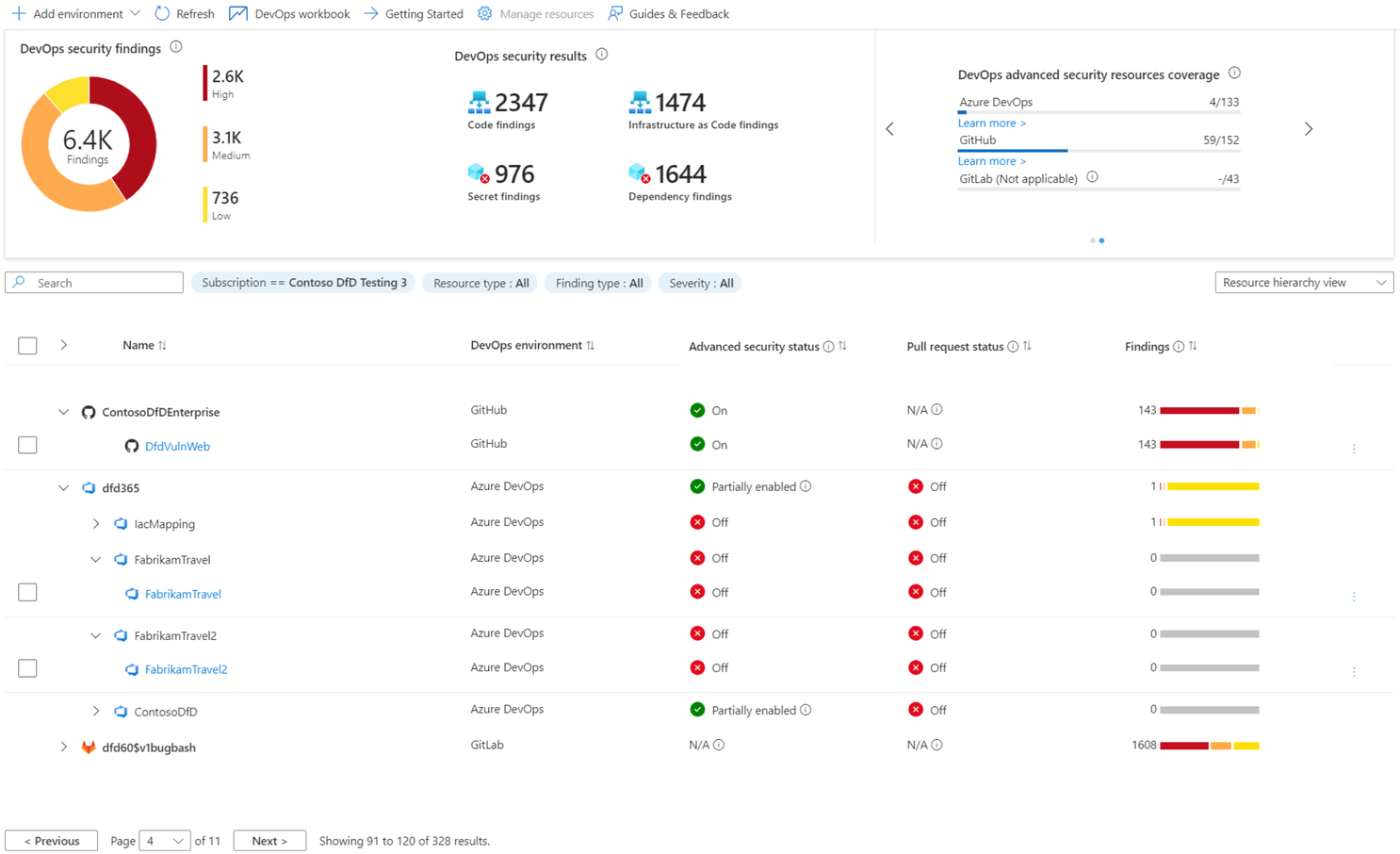


DevOps Security Management

Unified visibility into DevOps security posture

Strengthen cloud resource configurations throughout the development lifecycle

Prioritize remediation of critical issues in code



Demo

Exploring Microsoft Defender for Cloud

Module Conclusion

Introduction to DevSecOps, CSPM, and CWPP

- Development, security, and operations
- Cloud Workload Protection Platform
- Cloud Security Posture Management

Microsoft Defender for Cloud

- Secure score
- Regulatory Compliance
- Microsoft Defender for Cloud Plans
- DevOps Security Management

Up Next:

Threat Detection and Mitigation with Microsoft Sentinel