



November 13-15, Oslo Spektrum

Craig Forshaw

Mastering regulatory compliance with Defender for Cloud

Who am I

- Senior Architect, Atea
- Microsoft MVP, Security & Azure IaC
- Organiser, Microsoft Security User Group
<https://www.meetup.com/Microsoft-Security-User-Group/>
- Blog medium.com/@craig4shaw
- LinkedIn <https://no.linkedin.com/in/craig4shaw>



What we will talk about

- Cloud compliance challenges
- Defender for cloud regulatory compliance
- Compliance in code
- Governance rules
- Headaches





Contoso application 1

Contoso application 2

Contoso application 3

Contoso application 4

Contoso application 5

Contoso application 6

Contoso application 7

Contoso application 8

Contoso application 9

Contoso application 10

Contoso application 2



DASHBOARD

VIRTUAL MACHINES

INSTANCES

LINKED RESOURCES

NAME	↓	TYPE	STATUS	SUBSCRIPTION	LOCATION	🔍
VM-0-12-11-1		Virtual machine	Stopped	auxTU1Subscription431	Windows Azure Preview	
VM-0-12-11-2	→	Virtual machine	Stopped	auxTU1Subscription431	Windows Azure Preview	
VM-0-12-11-3		Virtual machine	Online	auxTU1Subscription431	Northwest US	
VM-0-12-11-4		Virtual machine	Online	auxTU1Subscription431	Northwest US	
VM-0-12-11-5		Virtual machine	Online	auxTU1Subscription431	Northwest US	
VM-0-12-11-6		Virtual machine	Online	auxTU1Subscription431	Northwest US	
VM-0-12-11-7		Virtual machine	Created	auxTU1Subscription431	Windows Azure Preview	
VM-0-12-11-8		Virtual machine	Online	auxTU1Subscription431	Northwest US	
VM-0-12-11-9		Mobile Service	Unhealthy	auxTU1Subscription431	-	



NEW



ADD



MANAGE



DELETE



POWER SHELL



1



1



1



1



1



?

Data breaches are increasing

Threat Actors

- Hackers
- Insiders
- Criminal gangs
- Nation-state threat actors

Identity Theft Resource Center Sees Third-Most Data Breach Victims in a Quarter in Q2 2024

Date: 07/17/2024

[Identity Theft Resource Center Sees Third-Most Data Breach Victims in a Quarter in Q2 2024 - ITRC](#)

Understanding cloud compliance challenges

- Complex regulatory landscape
- Cloud is dynamic and security is infinite
- Shared responsibility model
- Configuration monitoring
- Incident response

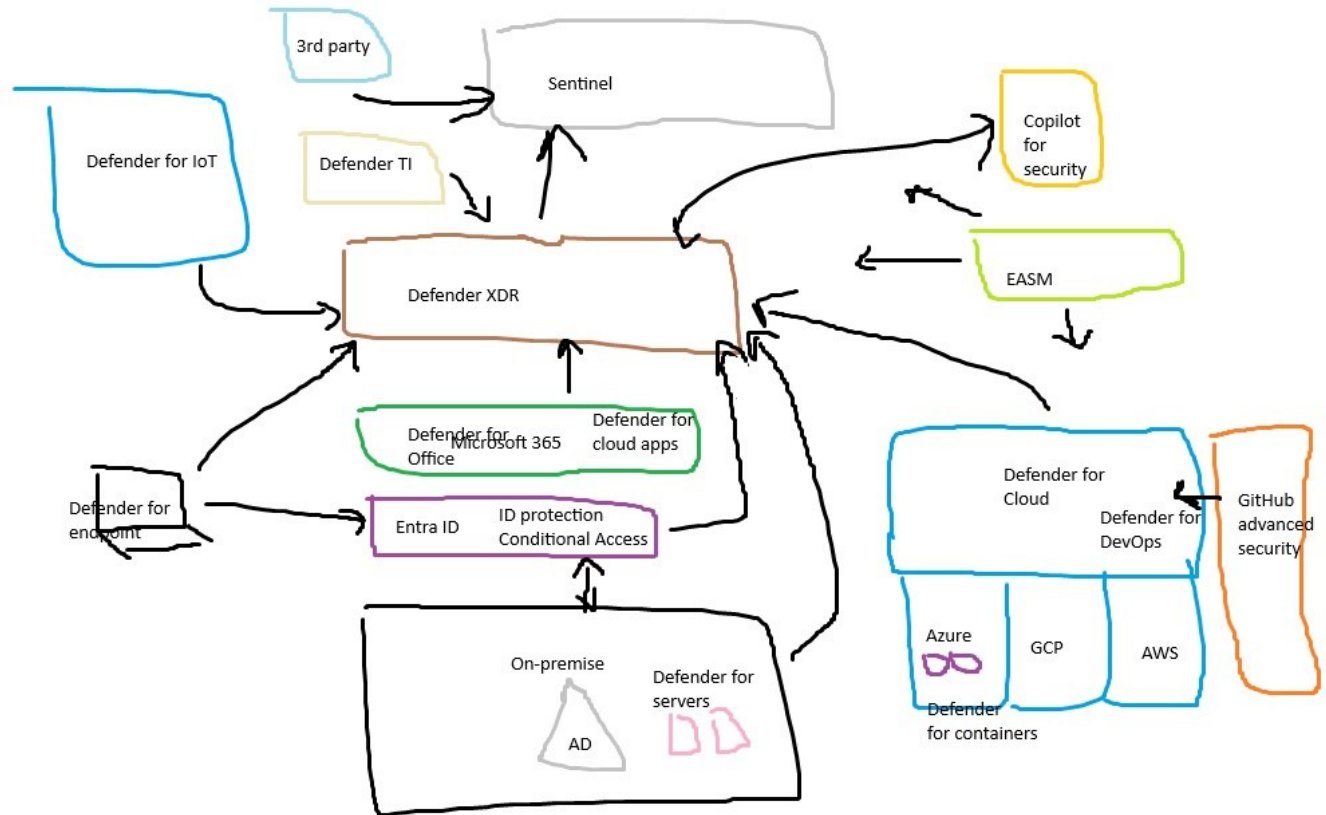
Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and directory infrastructure	Shared	Shared	Customer	Customer
	Applications	Shared	Shared	Customer	Customer
	Network controls	Shared	Shared	Customer	Customer
	Operating system	Microsoft	Microsoft	Customer	Customer
	Physical hosts	Microsoft	Microsoft	Customer	Customer
Responsibility transfers to cloud provider	Physical network	Microsoft	Microsoft	Customer	Customer
	Physical datacenter	Microsoft	Microsoft	Customer	Customer

Legend: Microsoft (Light Blue), Customer (Dark Blue), Shared (Diagonal Split)

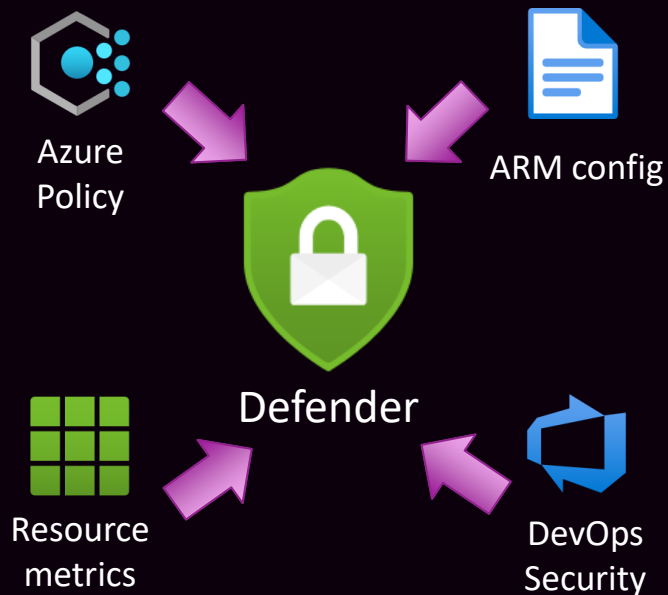
Defender for cloud regulatory compliance



Defender XDR



Defender for cloud



- Cloud native application protection platform (CNAPP)
- Cloud security posture management
- Cloud workload protection
- Multi-cloud compliance monitoring
- DevSecOps

Defender plan features

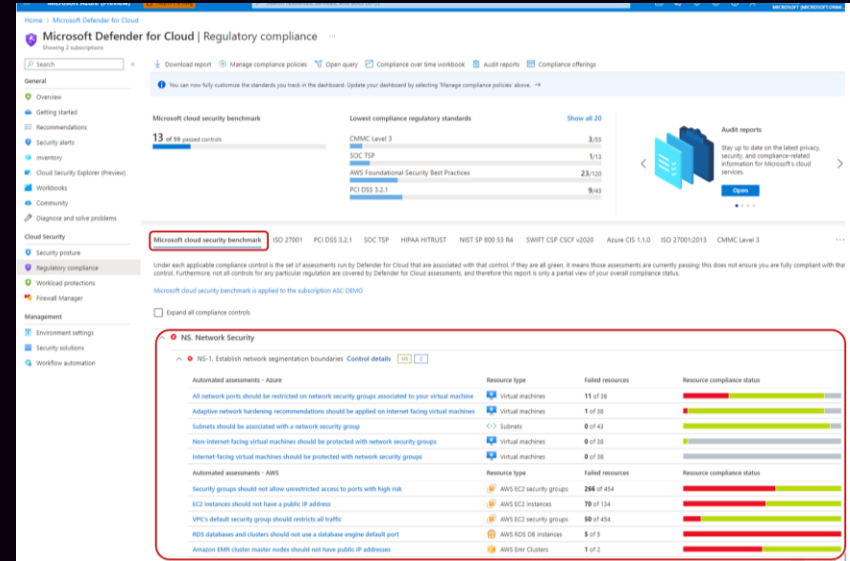
- Foundational CSPM (*Free*)
 - Security recommendations
 - Asset
 - Secure score
 - Data export
 - Workflow automation
 - Microsoft Cloud Security Benchmark (MCSB)

- Defender CSPM (*PAYG*)

AI security posture management	-	✓	Azure, AWS
Agentless VM vulnerability scanning	-	✓	Azure, AWS, GCP
Agentless VM secrets scanning	-	✓	Azure, AWS, GCP
Attack path analysis	-	✓	Azure, AWS, GCP
Risk prioritization	-	✓	Azure, AWS, GCP
Risk hunting with security explorer	-	✓	Azure, AWS, GCP
Code-to-cloud mapping for containers	-	✓	GitHub, Azure DevOps
Code-to-cloud mapping for IaC	-	✓	Azure DevOps
PR annotations	-	✓	GitHub, Azure DevOps
Internet exposure analysis	-	✓	Azure, AWS, GCP
External attack surface management	-	✓	Azure, AWS, GCP
Permissions Management (CIEM)	-	✓	Azure, AWS, GCP
Regulatory compliance assessments	-	✓	Azure, AWS, GCP
ServiceNow Integration	-	✓	Azure, AWS, GCP
Critical assets protection	-	✓	Azure, AWS, GCP
Governance to drive remediation at-scale	-	✓	Azure, AWS, GCP
Data security posture management (DSPM), Sensitive data scanning	-	✓	Azure, AWS, GCP ¹
Agentless discovery for Kubernetes	-	✓	Azure, AWS, GCP
Custom Recommendations	-	✓	Azure, AWS, GCP
Agentless code-to-cloud containers vulnerability assessment	-	✓	Azure, AWS, GCP

Regulatory compliance dashboard

- Best practice recommendations
- MCSB is *enabled* by default
- Lots more standards available
- Can create custom standards & recommendations
 - Custom standard – Subscription owner
 - Customer recommendation – Security admin
- Exempt resources



MCSB controls

- Network
- Identity management
- Privileged access
- Data protection
- Asset management
- Logging and threat detection
- Incident response
- Posture and vulnerability management
- Endpoint security
- Backup and recovery
- DevOps Security
- Governance and strategy

Demo



Microsoft Defender for Cloud | Regulatory compliance

Showing 2 subscriptions

Search

Download report Manage compliance standards Open query Compliance over time workbook Audit reports Compliance offerings

Favorites

Regulatory compliance

Recommendations

DevOps security

Environment settings

Security posture

General

Overview

Getting started

Recommendations

Attack path analysis

Security alerts

Inventory

Cloud Security Explorer

Workbooks

Community

Diagnose and solve problems

Cloud Security

Security posture

Regulatory compliance

Workload protections

Data security

Firewall Manager

DevOps security

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance standards' above. →

Microsoft cloud security benchmark

36 of 63 controls passed

Lowest compliance standards

Azure CSPM (Preview)

Show all 2

0/1

Cloud compliance data now integrated in Microsoft Purview Compliance Manager



Defender for Cloud compliance data now seamlessly integrates into Microsoft Purview Compliance Manager, allowing you to centrally assess and manage compliance across your organization's entire digital estate. [Learn more>](#)

Open

Microsoft cloud security benchmark

Azure CSPM (Preview)

Corporate Platform Engineering Standards

GCP CSPM (Preview)

GCP Default

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [licensing terms](#).

Corporate Platform Engineering Standards is applied to the subscription demo-sub

☐ Expand all compliance controls

1. Corporate Platform Engineering Standards

Automated assessments

Resource type

Failed resources

Resource compliance status

Set Terraform state storage account as DoNotDelete

Custom

Storage accounts

1 of 1

Showing 1 - 1 of 1 results.

Set Terraform state storage account as DoNotDelete

Corporate Platform Engineering Standards

 Exempt  Open query

Severity

Medium

Freshness interval

 30 Min

^Description


^Remediation steps

Manual remediation:
Turn on the DoNotDelete setting on the Terraform storage account

^Affected resources

Unhealthy resources (1)Healthy resources (0)Not applicable resources (0)

Search azure resources

<input type="checkbox"/>	Name	↑↓	Subscription	Owner	↑↓	Due date	Status	↑↓	Last change date	↑↓	Ticket ID	↑↓	Risk level	Risk factors	Attack paths	
<input type="checkbox"/>	 nic2024demottfstate		demo-sub						11/11/2024, 6:33:34 PM				Low		0	...

Compliance in code



Compliance challenges with DevOps Security in the cloud

- Configuration vulnerabilities
- Configuration drift
- Security control enforcement of code
- Validating compliance



Defender for Cloud DevOps controls

- MCSB Security control: DevOps Security
 - *DS-1: Conduct threat modeling**
 - DS-2: Ensure software supply chain security
 - DS-3: Secure DevOps infrastructure
 - DS-4: Integrate static application security testing into DevOps pipeline
 - *DS-5: Integrate dynamic application security testing into DevOps pipeline**
 - DS-6: Enforce security of workload throughout DevOps lifecycle
 - *DS-7: Enable logging and monitoring in DevOps**
- Defender for DevOps GitHub action
 - Antimalware
 - Bandit
 - BinSkim
 - Checkov
 - Eslint
 - Template Analyzer
 - Terrascan
 - Trivy

Governance rules



Governance rules in Defender for cloud

- Governance rules identify resources that require remediation according to specific recommendations or severities
- Define rules that assign an owner and a due date on a timeframe of 7, 14, 30, or 90 days
- Can apply a grace period so that the resources given a due date don't affect the secure score
- Owners emailed weekly




Demo

Headaches



- Synchronisation period varies based on resource type (30 mins > 48 hours)
- Exporting of information is basic
- Navigation and usability could be improved
- Recommendations not in the Microsoft ecosystem need exceptions – *3rd party firewall, Alternative PIM solution, for example*

Useful stuff

- [AzAdvertizer](#) – release / change tracking on Azure governance
- [Bicepgoat](#) – vulnerable code for testing
- [Recordings | Security Community Webinars | Microsoft Community Hub](#)
 - [Enhancing Cloud Security Posture with Defender CSPM](#)
- My Blog  medium.com/@craig4shaw

Thank you!