XV EDYCJA WDI WARSZAWSKIE DNI INFORMATYKI

Ochrona środowiska multicloud narzędziami Microsoft

Konrad Sagała

Cloud Security Architect, Alior Bank

ORGANIZATOR GŁÓWNY: ACADEMIC PARTNERS KOMITET ORGANIZACYJNY: kilkadziesiąt organizacji z sektora IT / data science (pełna lista na stronie wydarzenia)

Agenda

- Multi-cloud security
- Native support for AWS and GCP
- CSPM capabilities for AWS and GCP
- CWP(P) capabilities for AWS and GCP

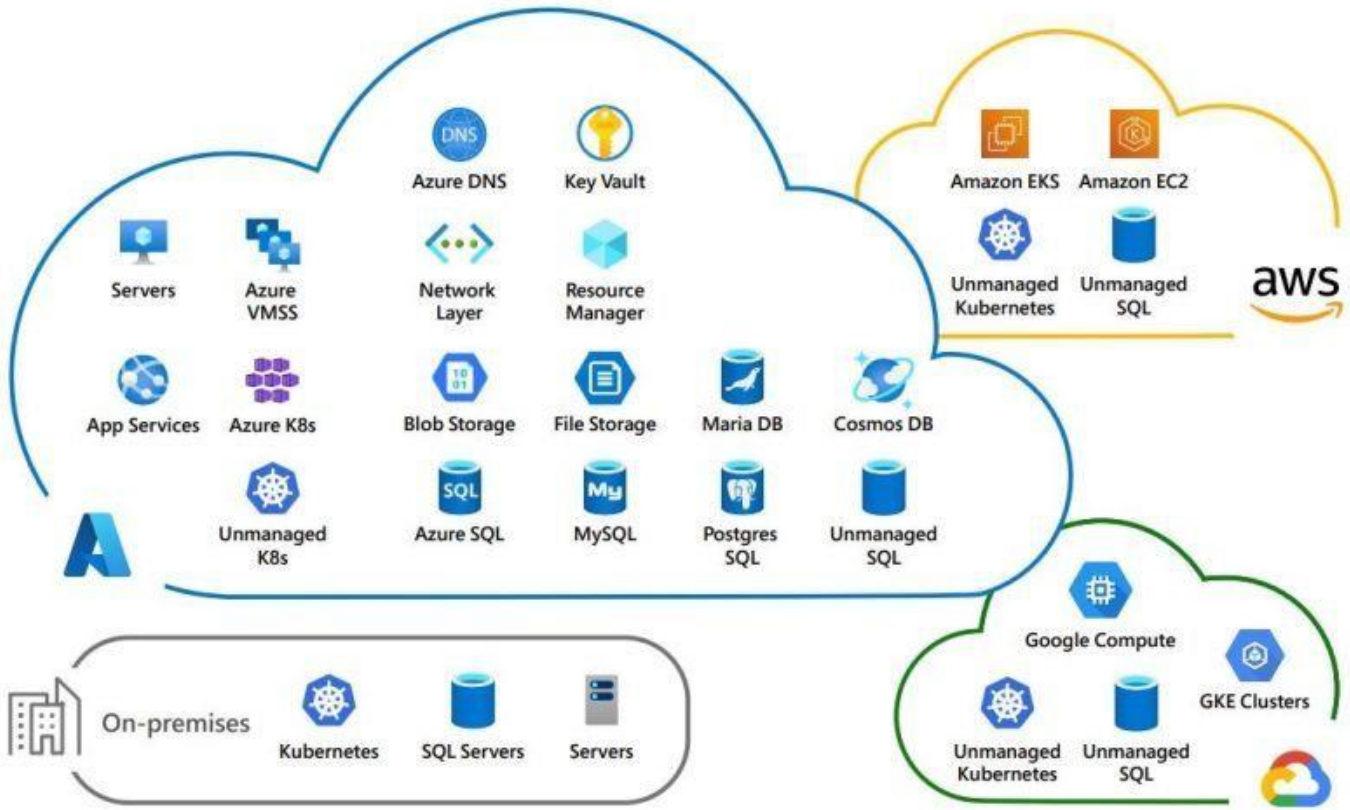
Cloud security challenges

- Visibility into security and compliance
- Increase in number and sophistication of attacks
- Complexity managing multi-cloud environment


Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

Microsoft Defender for Cloud

Secure your hybrid-cloud and multicloud workloads



Microsoft Defender for Cloud

Secure your critical cloud workloads running in AWS, Azure, and Google Cloud

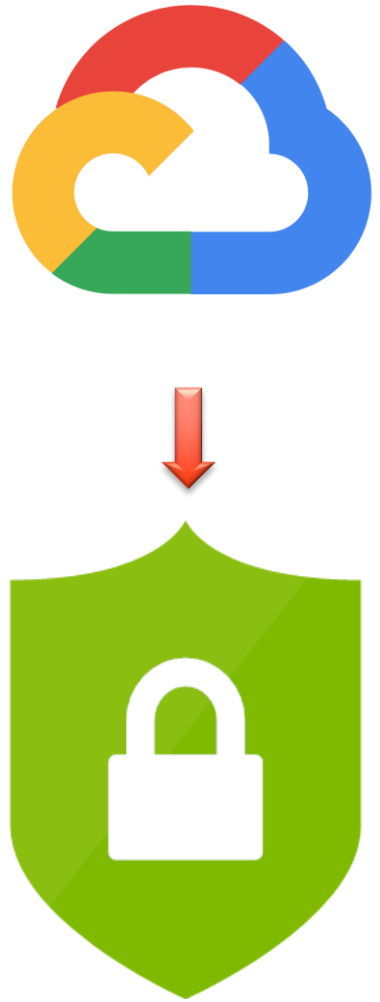
- Easy onboarding of AWS accounts and native support for Azure
- Get a bird's-eye view of your security posture and vulnerabilities across clouds with secure score
- Assess and implement best practices for compliance and security in the cloud
- Protect Amazon EKS and GKE clusters
- Protect GCP VM instances and AWS EC2 workloads
- Detect and block advanced malware and threats for Linux and Windows servers running in the cloud or on-premises

Connecting AWS accounts

- Easy, fast and granular onboarding
- Onboard single accounts or auto-provision the management account
- Defender plans are not dependent

Connecting GCP projects

- Connect GCP projects on the project level granular onboarding
- Run the provided script to GCP Cloud Shell
- Defender plans are not dependent



Onboarding demo

CSPM – security recommendations

- API based
- More than 160 out of the box recommendations for AWS
- More than 130 out of the box recommendations for AWS
- More than 30 resource types
- Regulatory compliance standards – CIS, PCI DSS, Best Practices

Compliance management

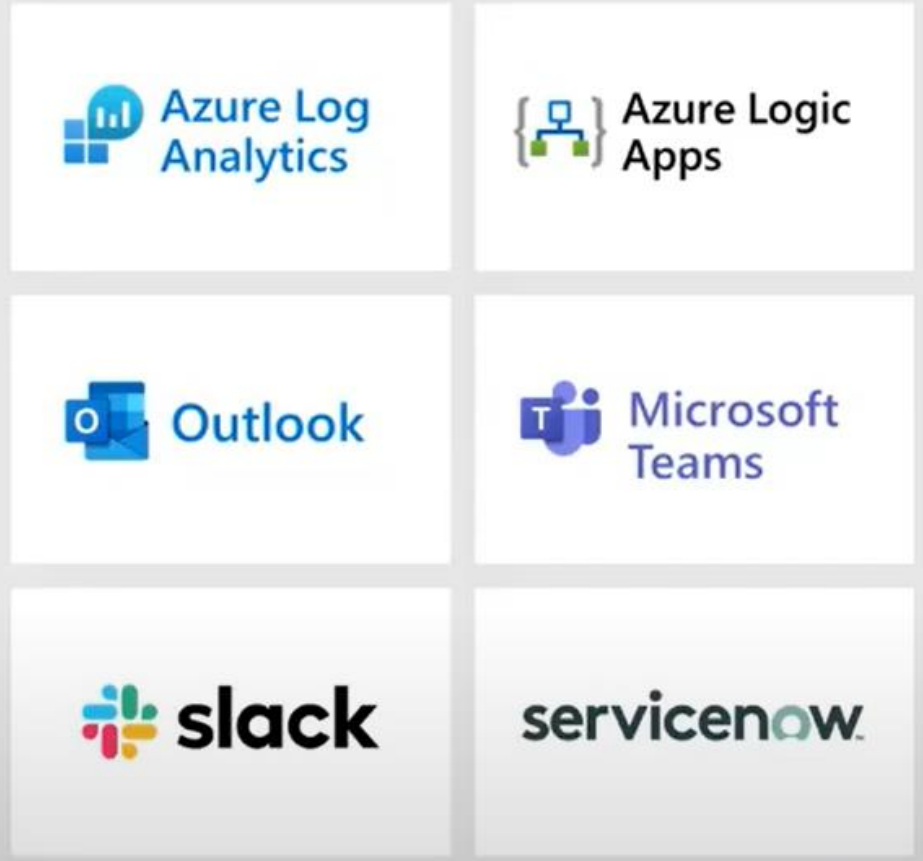
- Show compliance status, based on continuous assessments of Azure, AWS and GCP resources
- Monitor AWS and GCP resources
- Microsoft Cloud Security Benchmark monitoring enabled by default
- Mapped to the MITRE ATT&CK framework
- Support for common regulatory and compliance standards
- Reports of compliance status
- Custom recommendations possible

Inventory view

- Single view of all monitored resources
- Easy filtering, sorting and cross-referencing experience
- Continue exploration in Azure Resource Graph & export to CSV
- Management of resources

Automate response

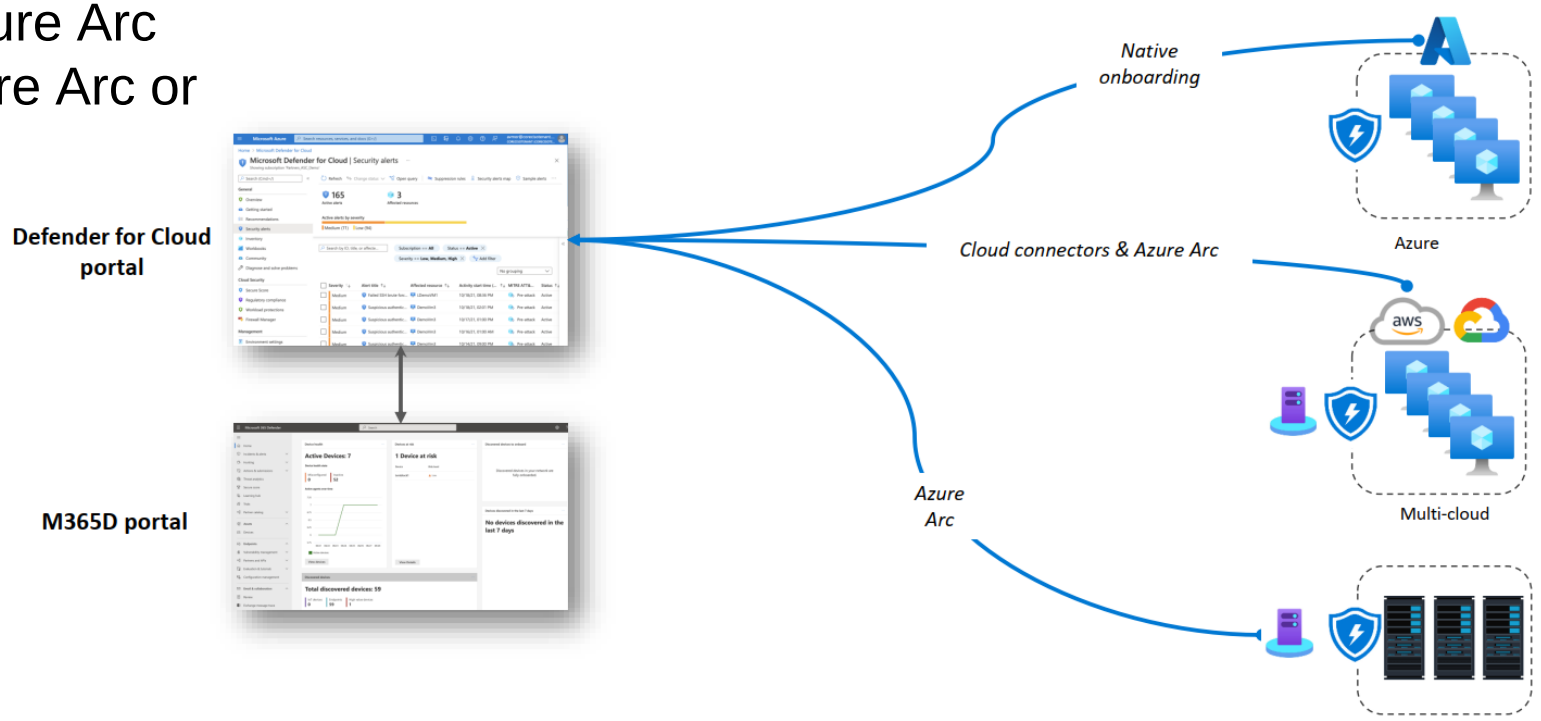
- Apply Quick fixes to recommendations
- Automate responses with Logic Apps
- Continuously export to Event Hub/Log Analytics
- Export to CSV



Defender for Servers in multicloud

All servers are secured the same way:

- Windows and Linux EC2 instances on AWS with Azure Arc
- Google VM instances with Azure Arc
- On-prem machines (with Azure Arc or directly)



Defender for Containers in multicloud

Support for many Kubernetes distributions

- AKS
- Amazon EKS
- Google GKE Standard clusters
- Kubernetes on-prem / IaaS

XV EDYCJA WDI WARSZAWSKIE DNI INFORMATYKI

Dziękujemy za oglądanie!

Zapraszamy do zadawania pytań
oraz oceny prelekcji pod nagraniem.

www.WarszawskieDniInformatyki.pl

5 kwietnia - 6 kwietnia 2024

PGE Narodowy + online

ORGANIZATOR GŁÓWNY: ACADEMIC PARTNERS

KOMITET ORGANIZACYJNY: kilkadziesiąt organizacji z sektora IT / data science (pełna lista na stronie wydarzenia)

XV EDYCJA WDI WARSZAWSKIE DNI INFORMATYKI

FEEDBACK

Ochrona środowiska multicloud narzędziami Microsoft

Konrad Sagała

https://warszawskiedniinformatyki.pl/user.html#!/lecture/WDI24-06d3/rate

www.WarszawskieDniInformatyki.pl

5 kwietnia - 6 kwietnia 2024

PGE Narodowy + online

ORGANIZATOR GŁÓWNY: ACADEMIC PARTNERS

KOMITET ORGANIZACYJNY: kilkadziesiąt organizacji z sektora IT / data science (pełna lista na stronie wydarzenia)