

Microsoft Defender for Cloud

Protect your multicloud and hybrid environments

Lukasz Szankowski
Security Cloud Solutions Architect



Securing multicloud environments

Top-of-mind

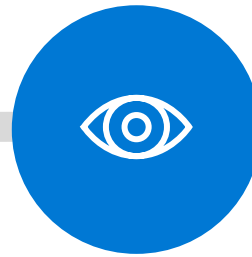
Develop and operate
secure apps in the
cloud



>54%

of enterprises do not
integrate security into
DevOps pipelines.¹

Visibility into security
and compliance



86%

of surveyed security decision
makers believe their
cybersecurity strategy doesn't
keep up with their multicloud
environments.²

Protect against
increasing,
sophisticated attacks



\$4.24M

is the average cost
of a breach, 2021.³

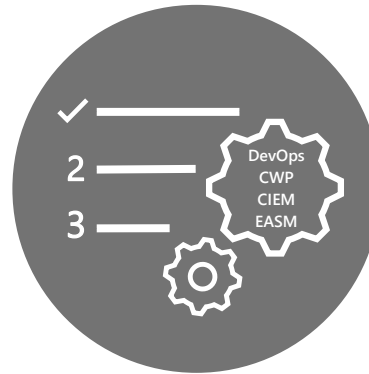
1. Microsoft Enterprise DevOps Report
2. Microsoft Cloud Security Priorities and Practices Research
3. Ponemon Institute, Cost of a Breach Report

Microsoft Defender for Cloud

Unify your DevOps
Security Management



Strengthen and manage your
cloud security posture







Protect your cloud
workloads

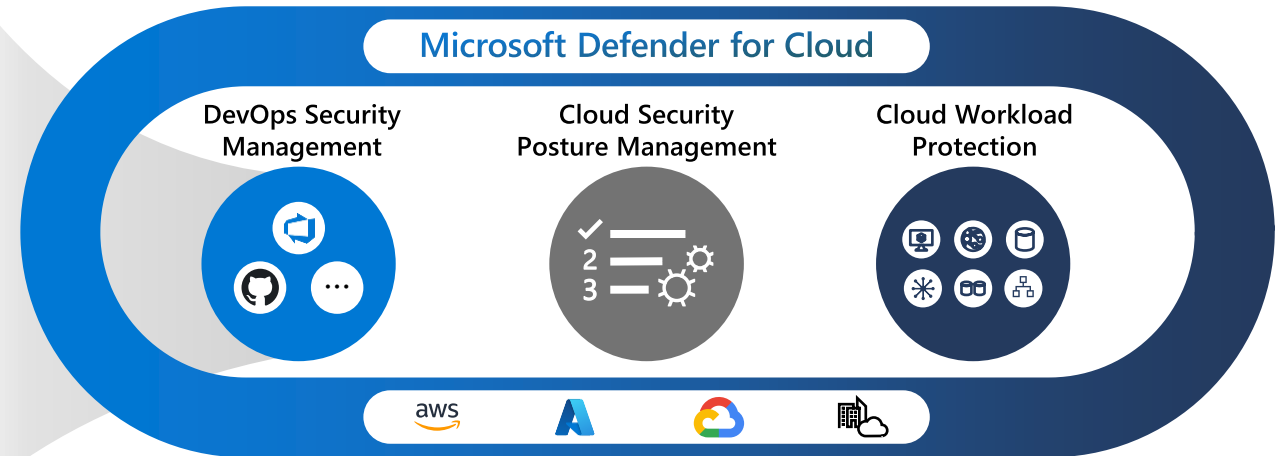


Unify DevOps
Security Management



Defender for DevOps

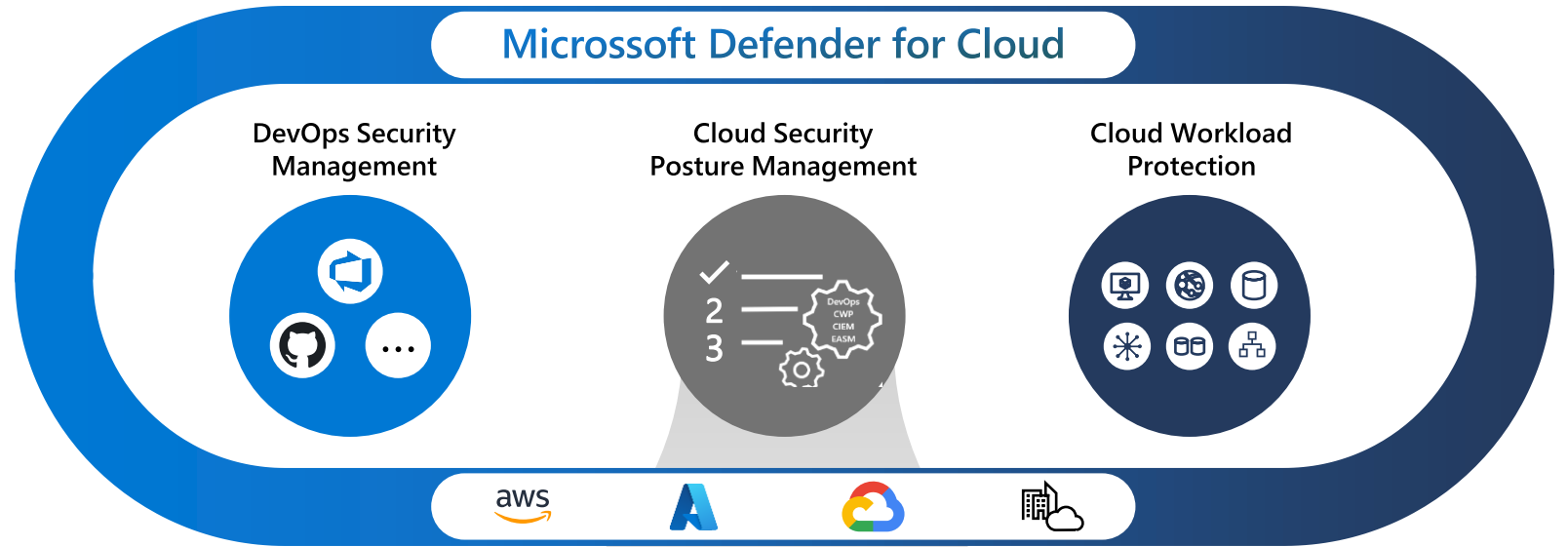
-  **DevOps posture visibility**
Code | Dependencies | Secrets | Container images | Infrastructure as code security insights
-  **Infrastructure as code security**
ARM | Bicep | Terraform | CloudFormation | and more
-  **Code to cloud contextualization**
Across multi-pipeline and multi-cloud environments
-  **Integrated workflows**
Pull request annotations | Developer ownership assignments







Strengthen and manage your
Security Posture with Microsoft
Defender for Cloud



Defender Cloud Security Posture Management



-  **Agentless and agent-based vulnerability scanning**
Visibility on software and CVEs | Disc snapshots | EDR
-  **Integrated data and insights**
Defender for DevOps | Defender EASM | Entra Permissions Management | Hybrid and multi-cloud environments
-  **Contextual cloud security and risk prioritization**
Attack path analysis to prioritize risk | Intelligent cloud security graph | Custom path queries on cloud security explorer
-  **Integrated workflows and automated remediation**
Regulatory compliance | Master group management | Multicloud Microsoft cloud security benchmark

Detect threats and protect your workloads

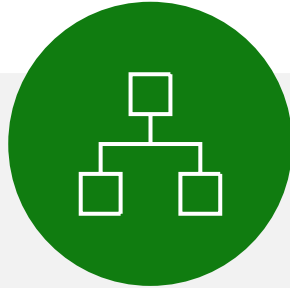


Threat protection for all layers of the cloud and on-prem



Threat detection

Prioritized alerts across compute, databases, the cloud service layer, and more



MITRE ATT&CK[®] framework mapping

Understand the effect across the adversary's attack lifecycle



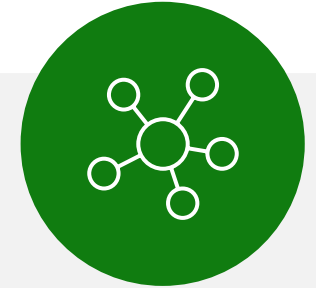
Leading threat intelligence

Rely on highly sophisticated and resource-specific alerts based on Microsoft's global threat intelligence



Agentless vulnerability assessment & management

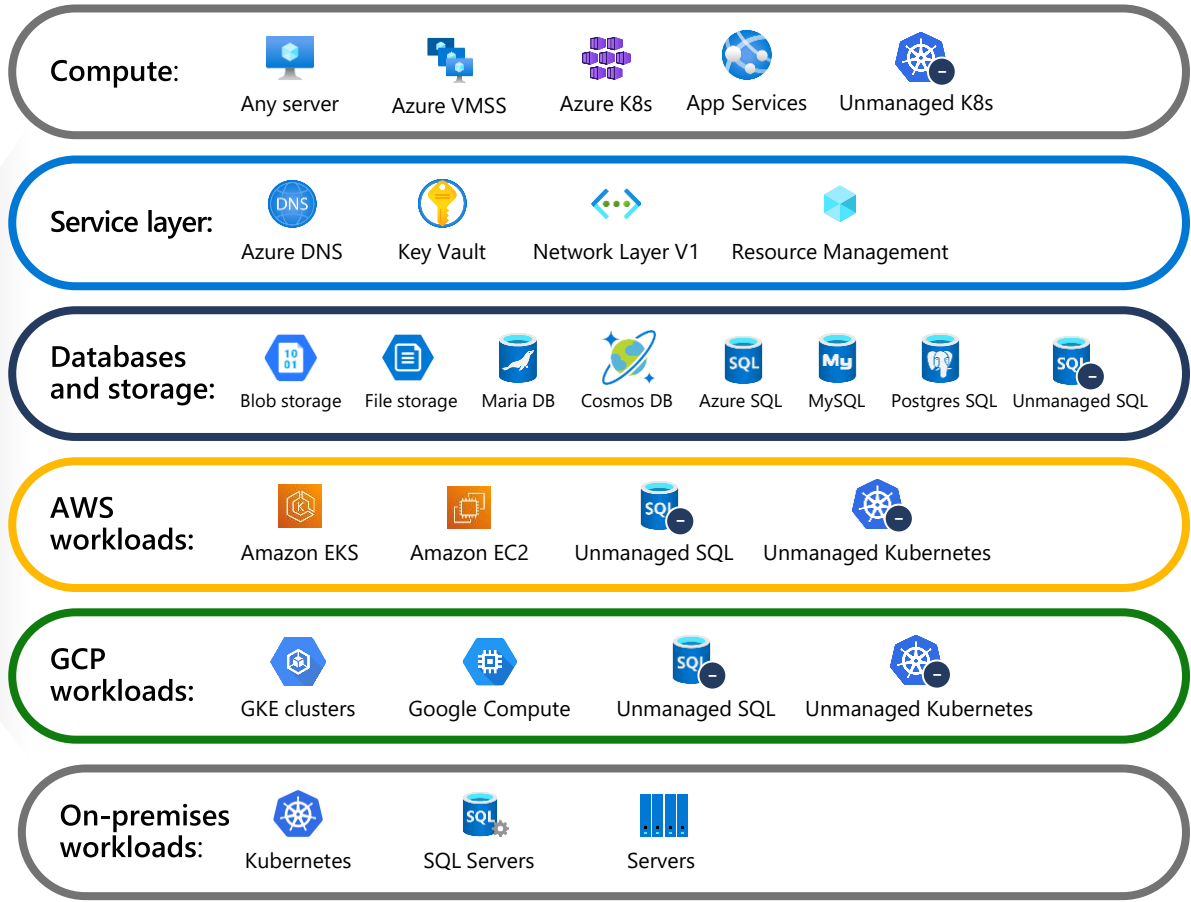
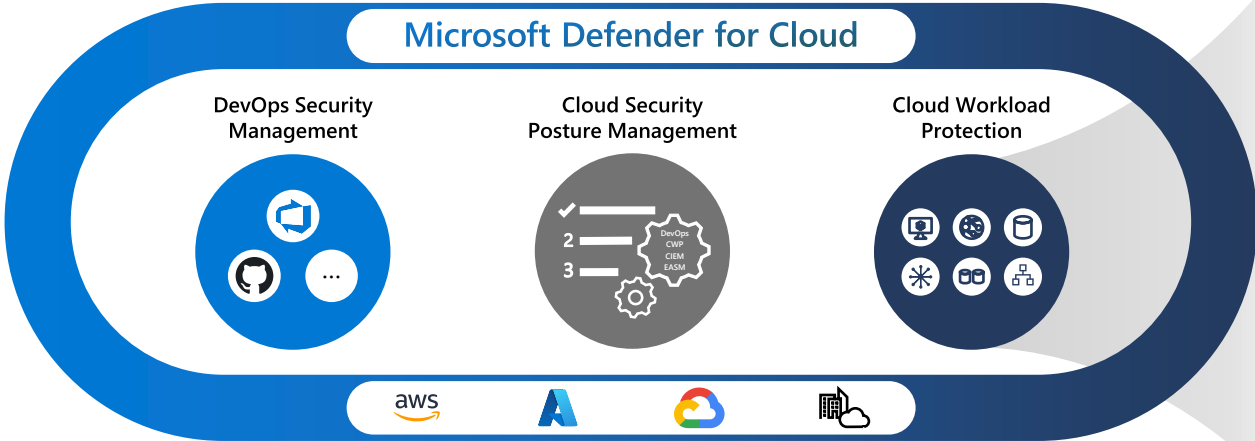
Identify and remediate vulnerabilities before they are exploited



Alert correlation

Prioritize more easily with connected alerts that are grouped into incidents

Cloud Workload Protection



Operationalize Defender for Cloud



Multicloud and hybrid protection

- Automatic onboarding for Azure subscriptions
- Use API connectors to onboard AWS and GCP accounts to posture management capabilities.
- Use the Azure Arc agent to onboard workloads outside of Azure and protect them against threats

Use API connectors for
agentless CSPM
enablement



Deploy the Azure Arc agent to enable
workload protection

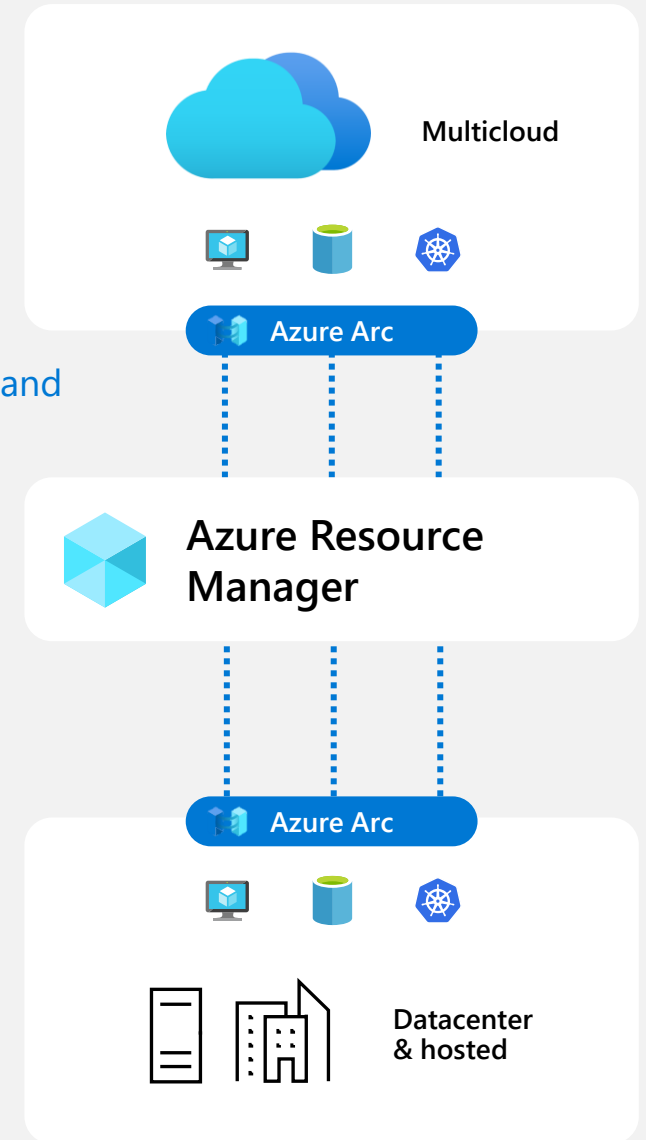
Built-in

Deploy Microsoft Defender for Cloud threat protection to your workloads anywhere with Azure Arc

- Extension installation, e.g. Log Analytics agent
- Enforce compliance and simplify audit reporting
- Asset organization and inventory with a unified view in the Azure Portal—Azure Tags
- Server owners can view and remediate to meet their compliance—RBAC in Azure

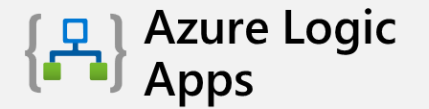
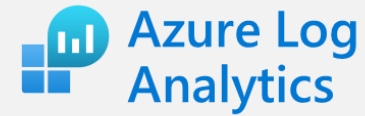
Azure Arc enables cloud management and security protections

Single control plane for any resource, anywhere



Respond and automate

- Leverage “Quick Fixes” for the fastest way to implement recommendations
- Automate threat alert responses with Azure Logic Apps and use the apps of your choice to create intelligent workflows
- Connect to Microsoft Sentinel and easily move between the portals when investigating and managing incidents





[Action required] Implement active recommendations assigned to you in Microsoft Defender for Cloud

You're assigned as the owner of several active Microsoft Defender for Cloud security recommendations in subscription 'Demo subscription'.

Implement these recommendations to enhance the security posture of your workloads.

Here is the list of Microsoft Defender for Cloud recommendations that require your attention:

Recommendation name	number of affected resources
MFA should be enabled on accounts with owner permissions on your subscription	10 (6 overdue)
Vulnerabilities in your virtual machines should be remediated	8 (8 overdue)
Management ports of virtual machines should be protected with just-in-time network access control	6

Required action

To harden your workloads based on identified security misconfigurations and weaknesses, select **Review recommendations** and implement the security recommendations in Microsoft Defender for Cloud.

[Review recommendations >](#)

