#Coding

Secure your application journey from earth to the cloud

Mario Cuomo & Edoardo Garofano


development innovation


Microsoft


CONSOFT
INFORMATICA


Burraconline
.com


present
your digital future


SWEN
Intersystem


AlmavivA


AlmavivA
DIGITALTEC

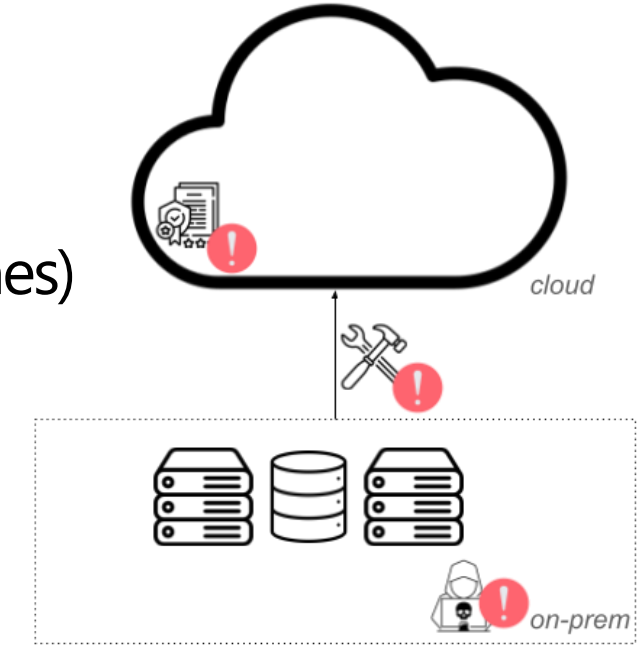
Agenda

- Why here?
- Security as an opportunity, not a blocker
- The security opportunity as a service
- Microsoft Defender for Cloud for every workload
- Microsoft Defender for Cloud Demos
- Q&A

Why here?

Monitor transitions from traditional workloads to hybrid cloud to speed-up the migration and checking for:

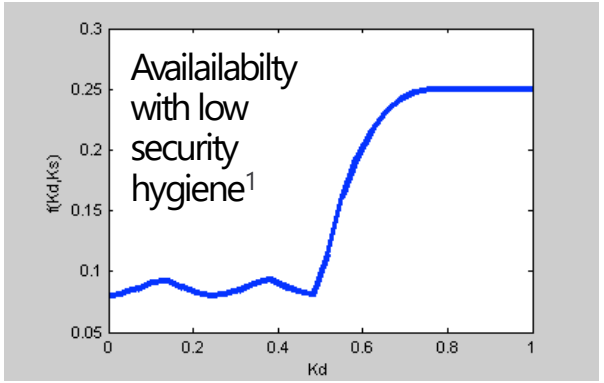
- Threats (already present?)
- Misconfigurations (moving to cloud exposes to new possible ones)
- Compliance needs



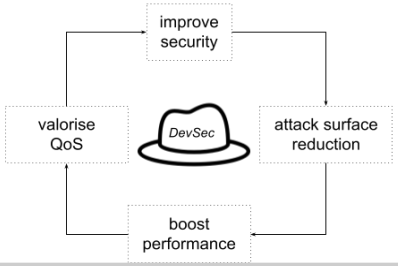
Security as an opportunity, not a blocker

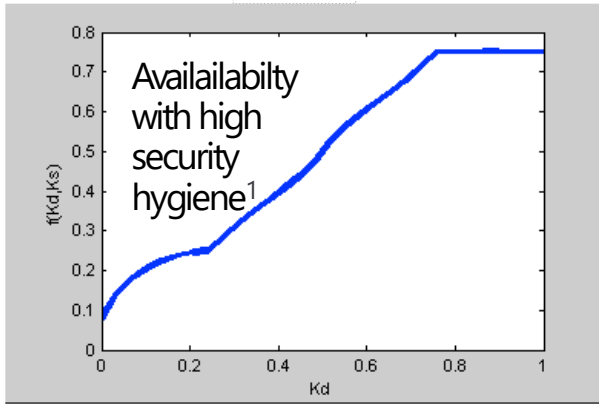
Security still sounds like an option but it's not!

- Security increases the availability of a workload (but availability is really a security KPI?)
- Implementation of security measures contribute to the general performance of workloads
- Without security one day the workload will have disruption – who will restore the application? Security or workload team?



VS





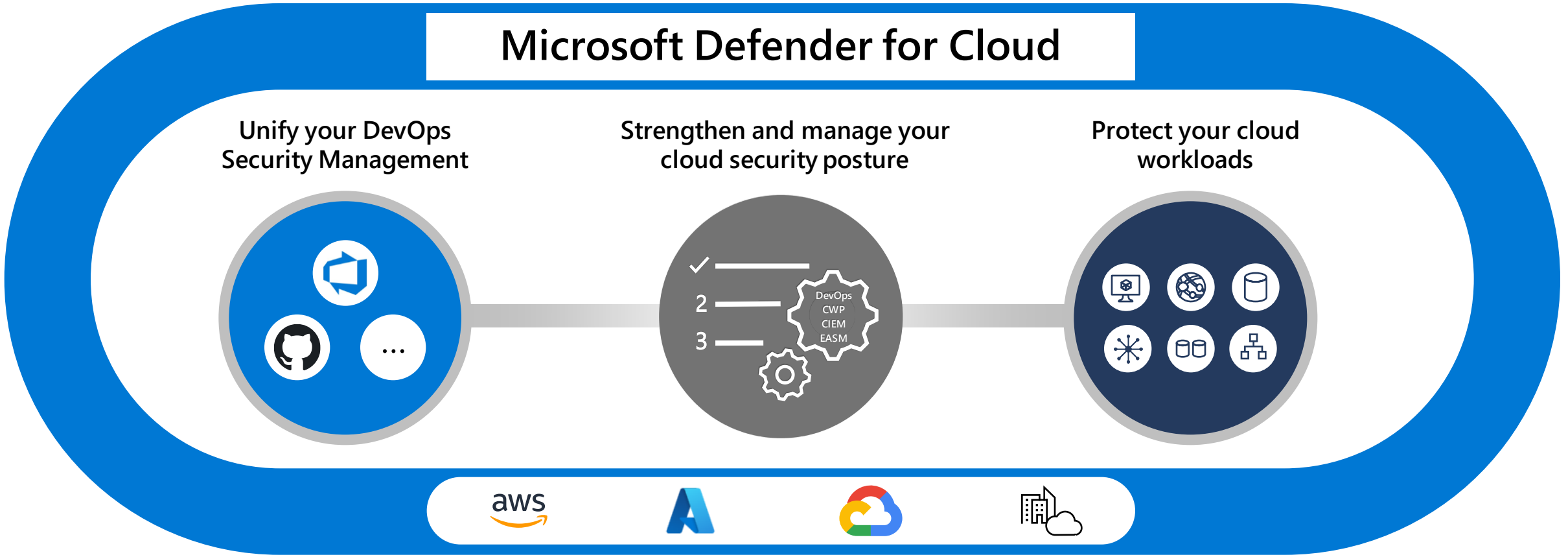
[1]Source: Considerations regarding security issues impact on systems availability

The security opportunity as a service

Once, also security platforms were workloads to be managed
(and in many cases still are)

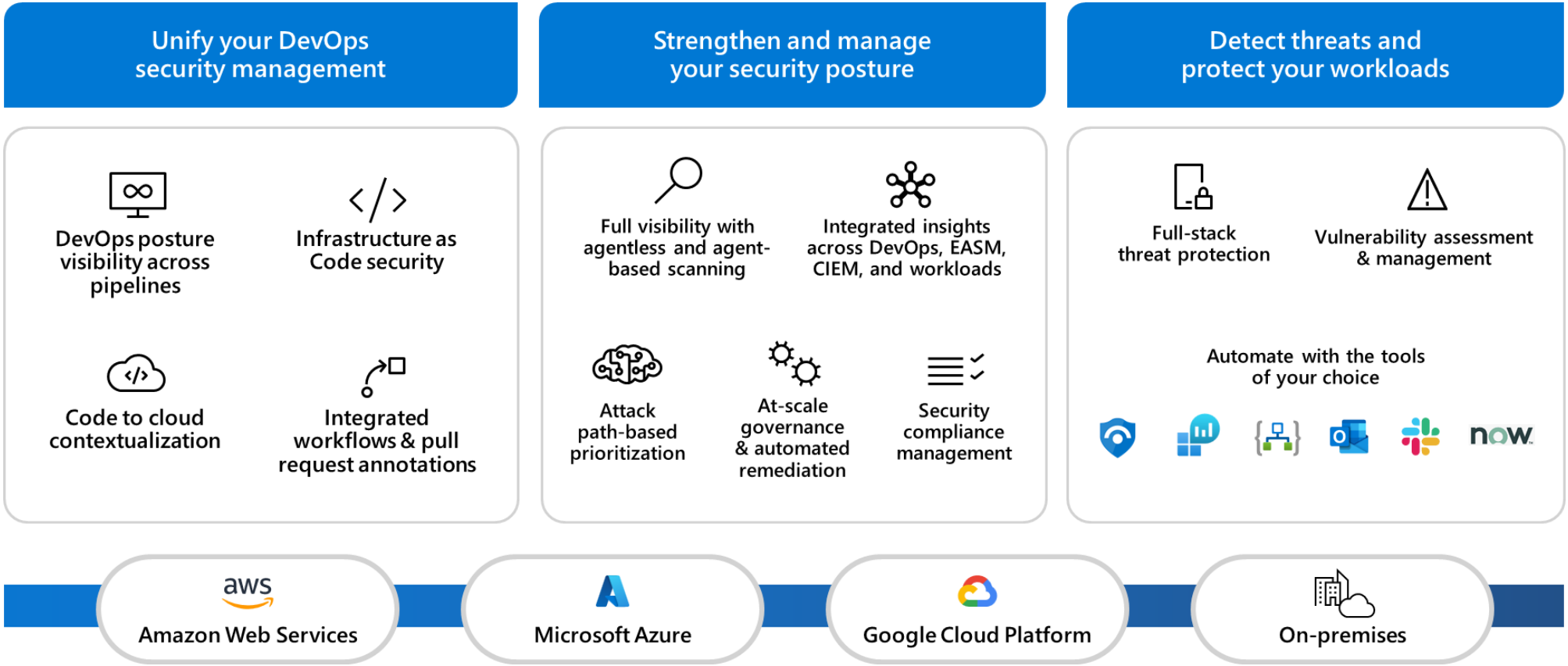
- What about having one single SaaS service to handle security of any workload?
- No infrastructure maintenance
- Single point of view of my assets, unified evaluation, unified threat detections

Core Value Propositions

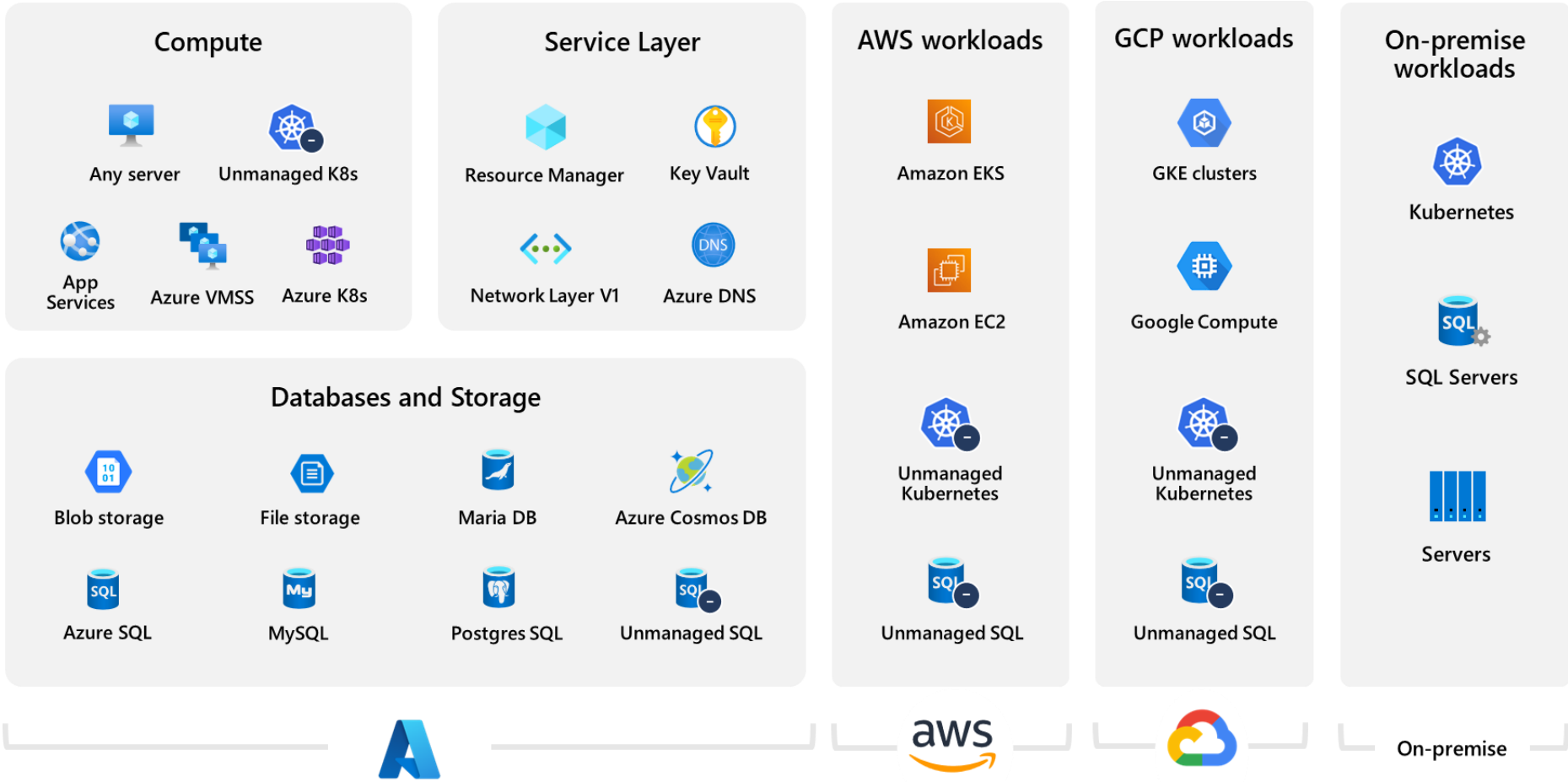


Microsoft Defender For Cloud

Cloud-native application protection across clouds and on-premises environments

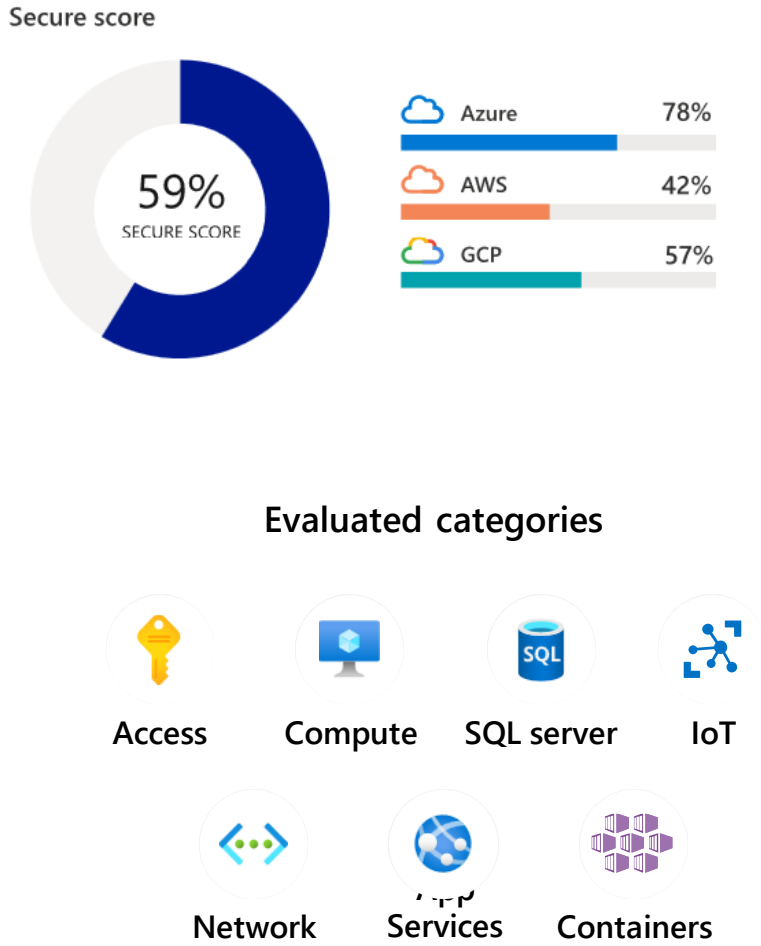


Full-stack coverage with dedicated detections



Secure Score

- Assess and implement best practices for security and compliance
- Cover all critical cloud resources across network, access, compute, databases, your service layer and more
- 450+out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements
- Use “Quick fix” to remediate with a single click or scale enforcement mechanisms to enforce policies to avoid configuration drifts

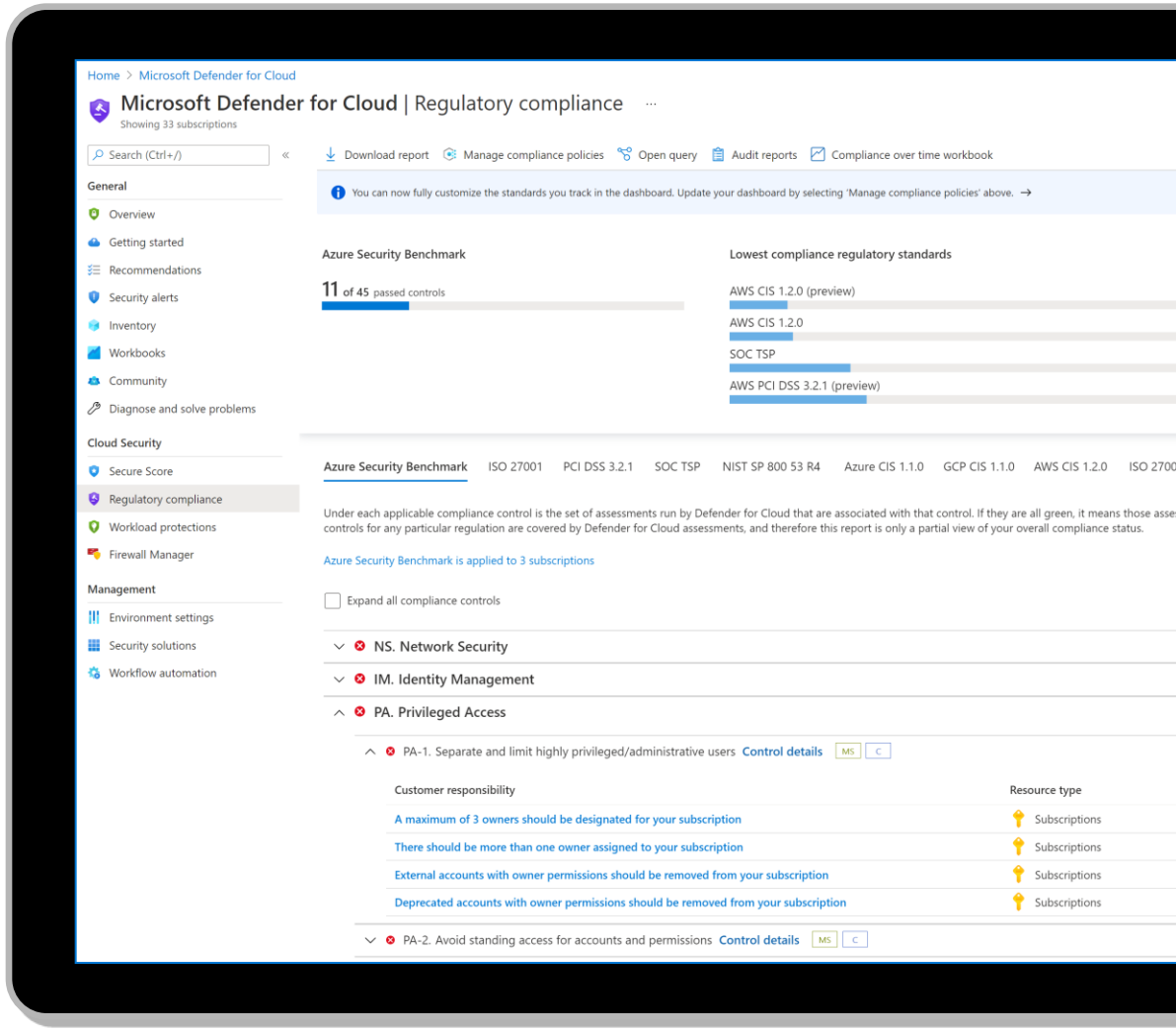


Compliance assessment and management

- Assess and manage your compliance status with a continuous assessment of your cloud resources
- Use industry standards, regulatory compliance frameworks, and vendor provided benchmarks to implement security and compliance best practices
- Create custom recommendations to meet unique organizational needs

Support for:

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices



Defender for DevOps architecture

DevOps posture visibility

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

Infrastructure as code security

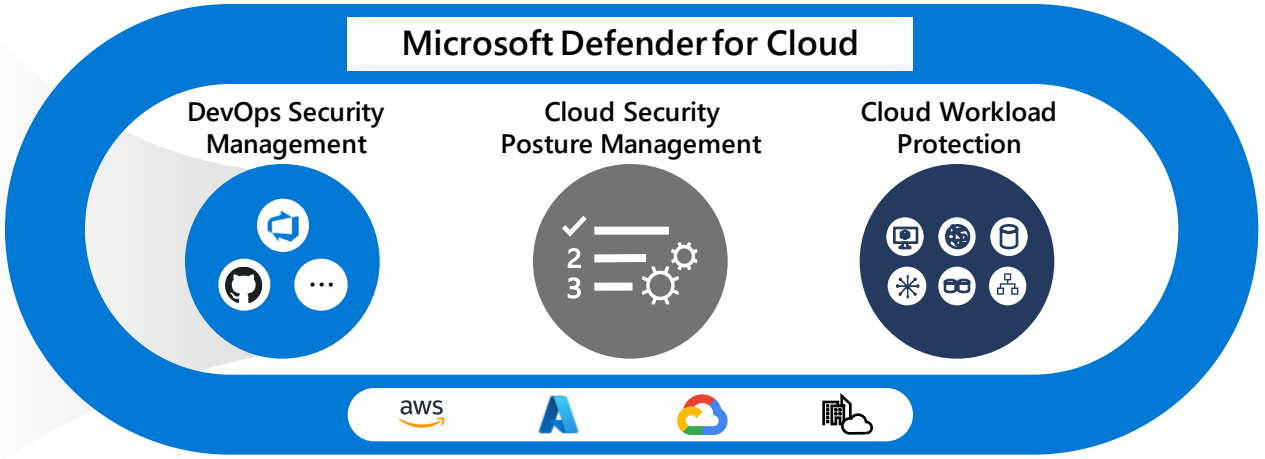
ARM | Bicep | Terraform | CloudFormation | And more

Code to cloud contextualization

Across multipipeline and multicloud environments

Integrated workflows

Pull request annotations | Developer ownership assignments



Microsoft Defender for Containers

Protect multi-cloud and hybrid container deployments

Hardening

Continuously assess and improve the security posture of your containerized environments and workloads

Vulnerability management

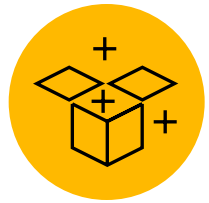
Reduce your attack surface by continuously scanning workloads to identify and manage container vulnerabilities

Advanced threat detection

Identify runtime threats with prioritized, container-specific alerts – using powerful insights from Microsoft Threat Intelligence

Multi-cloud support

Single container security solution for Kubernetes clusters, across Azure, AWS, GCP and on-premise



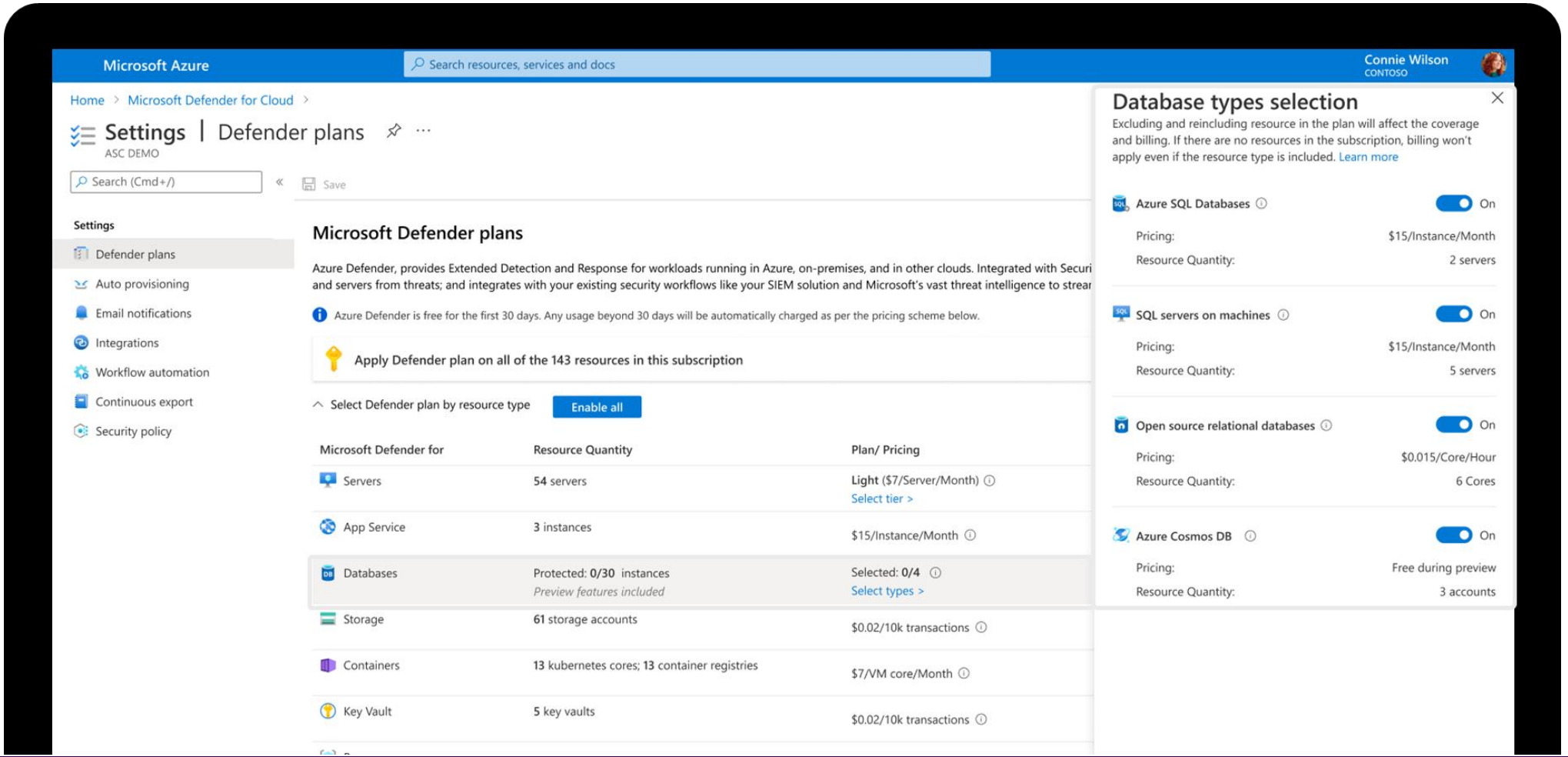
Deployment and monitoring

Frictionless deployment provisioning at scale with easy onboarding and support for standard Kubernetes monitoring tools

Protect your SQL workloads anywhere

Defender for SQL PaaS	Azure SQL Database	Azure SQL Managed Instance	Azure SQL Elastic Pools	Dedicated SQL pool in Azure Synapse
Defender for SQL IaaS	SQL Server on-prem	Azure Arc enabled SQL Server	SQL Server on Azure VM	SQL Server on any other cloud
Defender for OSS DB	Azure Database for MariaDB	Azure Database for MySQL	Azure Database for PostgreSQL	
Defender for Azure Cosmos DB	Azure Cosmos DB			

One-click enablement to protect your database estate



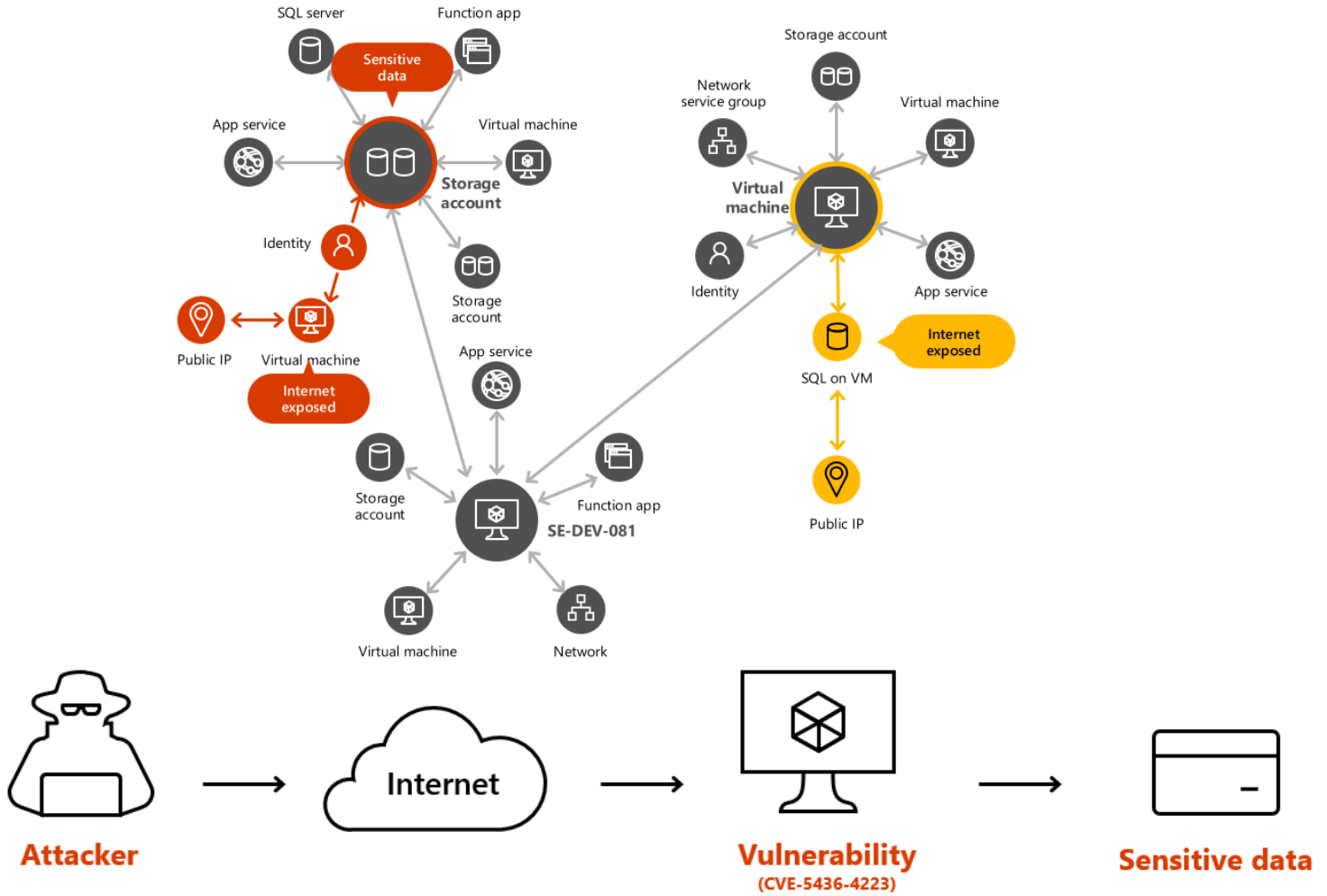
The multi-cloud landscape visibility and control problem

Lack of visibility and coverage across hybrid & multicloud environments

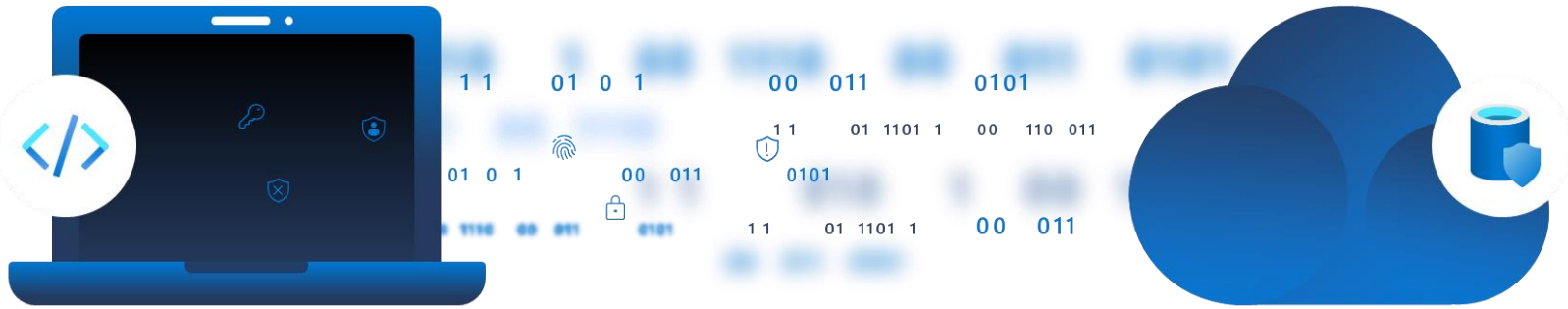
Overwhelming volume of security recommendations

Fragmented tools across different clouds

Overwhelming security recommendations don't help to prioritize security risks



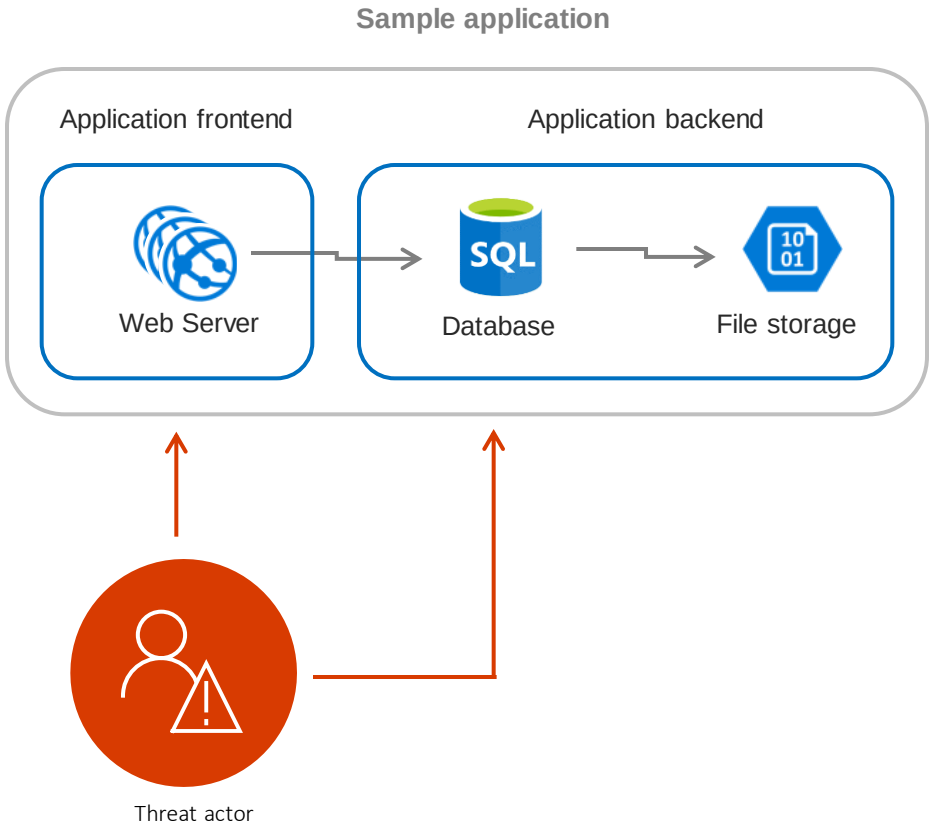
Demo 1 – Multi-Cloud CSPM and DevOps Security



Your databases are at risk!

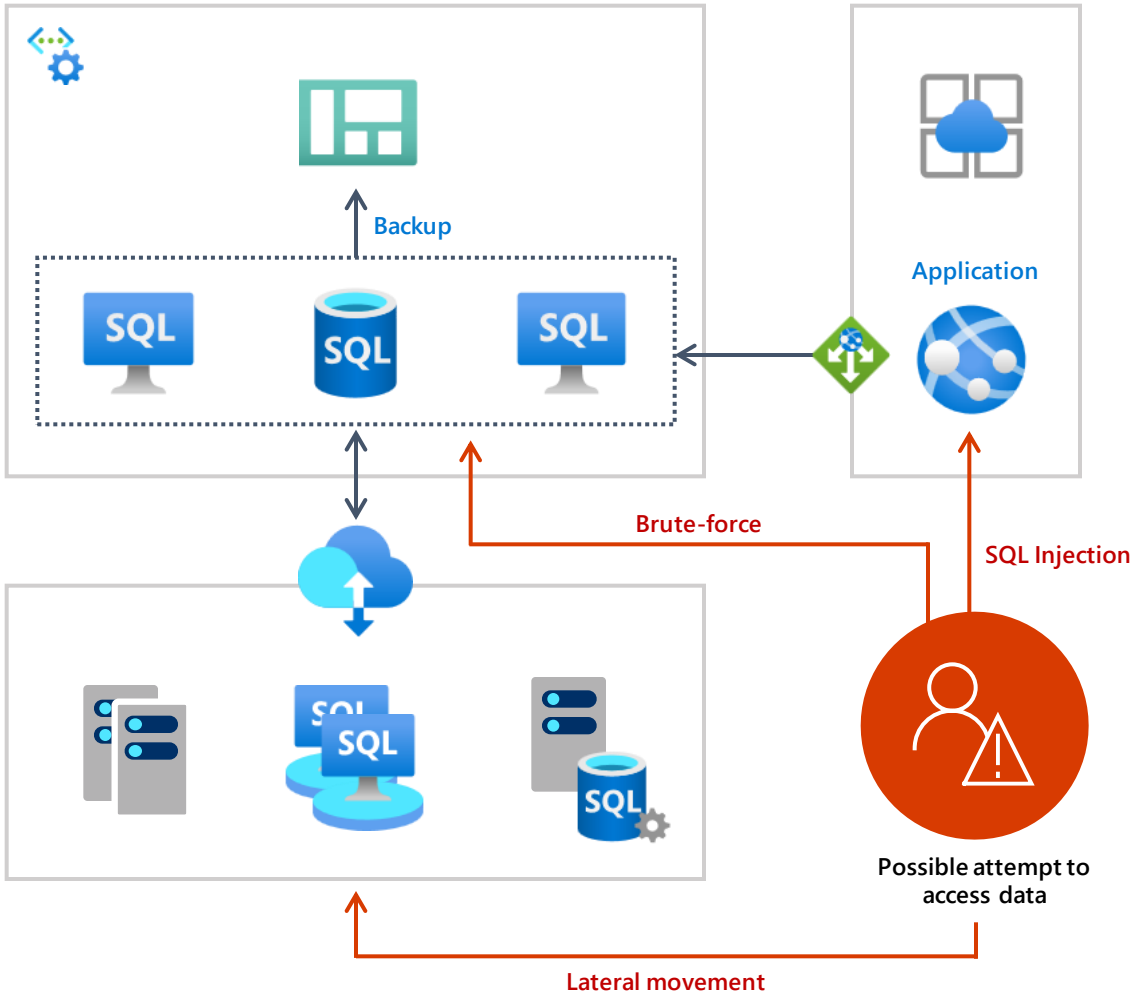
Databases contain your most sensitive data, making them a key target for attackers

- Databases have double the attack surface - database + frontend application
- Frontend attacks are extremely common as they are inherently exposed to end-users and usually internet-facing
- Frontend attacks can lead to sensitive data-leaks, data destruction and compromise database credentials



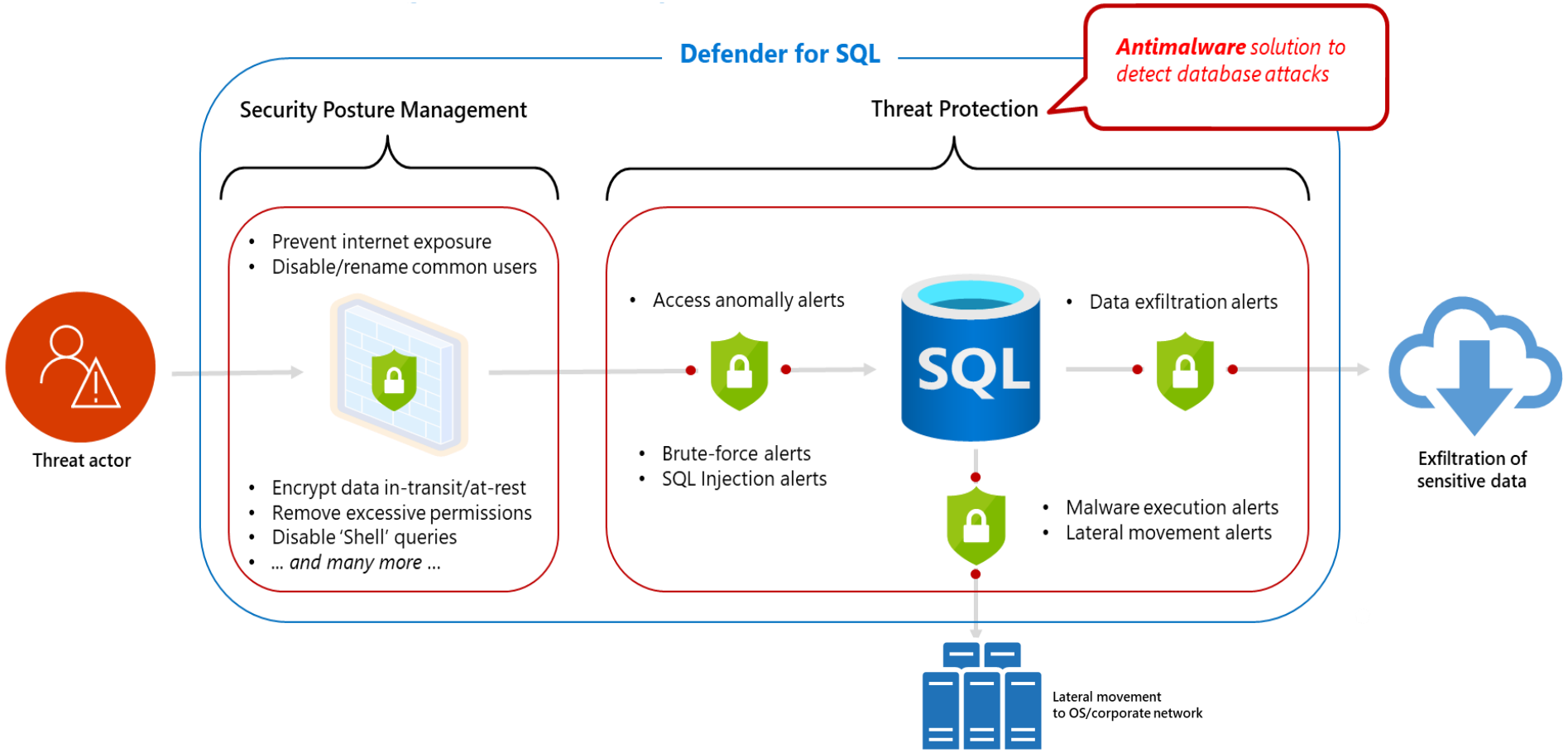
Most common database threats

- SQL injection attacks
- Brute-force attacks
- Unusual data exfiltration
- Suspicious access or queries

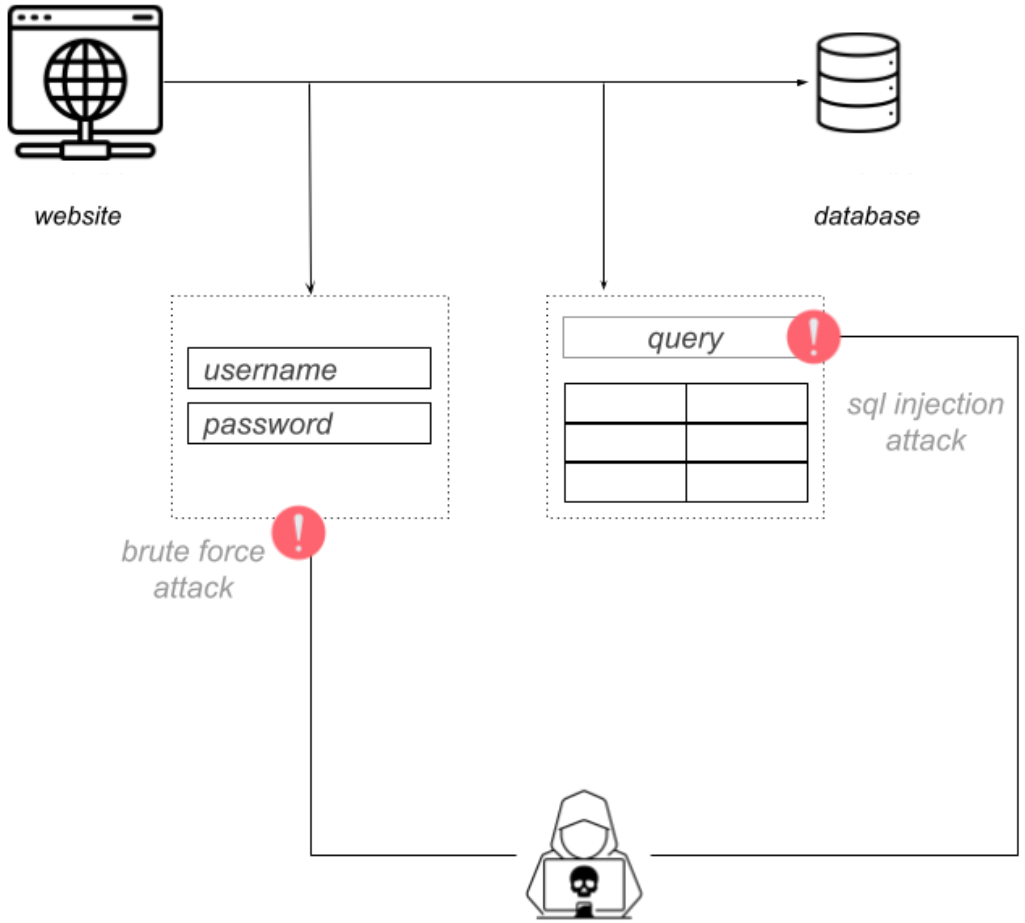


Database protection deep-dive

Defender for SQL two-layered database protection



Demo 2 – Detect SQL "anywhere" compromise



Pricing (good news only ☺)

Microsoft Defender for Cloud is free for the first 30 days!
Let's start to have fun with it 😉

Resource Type	Price
Microsoft Defender for Servers Plan 1	**€0.007**/Server/hour
Microsoft Defender for Servers Plan 2	**€0.019**/Server/hour
	Included data - 500 MB/day
Microsoft Defender for Containers	**€0.0087**/vCore/hour [4]
Microsoft Defender for SQL on Azure-connected databases	**€0.019**/Instance/hour[2]
Microsoft Defender for SQL outside Azure	**€0.014**/vCore/hour[3]
Microsoft Defender for MySQL	**€13.838**/Instance/month

Resource Type	Price
Microsoft Defender for PostgreSQL	**€13.838**/Instance/month
Microsoft Defender for MariaDB	**€0.019**/Instance/hour
Microsoft Defender for Azure Cosmos DB[5, 6]	**€0.0012** per 100 RUs/hour
Microsoft Defender for Storage[1]	**€0.0124** per storage account/hour[7]
Microsoft Defender for App Service	**€0.019**/App Service/hour
Microsoft Defender for Key Vault	N/A/10K transactions
Microsoft Defender for ARM	**€3.690**/1M API calls

https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/

Final considerations

- Go SaaS to deploy your workloads – it's easier to apply security measures without any operational impact!
- Use security as a booster for your workload's performance
- Defender for Cloud helps you in any kind of environment, choose yours and just enable it

Questions & Answers

Thanks *(english)*
谢谢 *(chinese)*
धन्यवाद *(hindi)*
Gracias *(spanish)*
Merci *(french)*
شكرا *(arabic)*

Grazie!

Спасибо *(russian)*
Obrigado *(portuguese)*
থ্যাংকয়ু *(Bengali)*
Danke *(German)*
ありがとう *(Japanese)*
감사합니다 *(Korean)*