#GLOBALAZURE 2026

#Milano

improove

TD SYNNEX

Grazie ai nostri sponsor 🙏

#Milano

Proteggere con Microsoft Defender for Cloud le istanze SQL ovunque si trovino

Lorenzo Grasseni

Security Consultant @ Overnet

Michele Sensalari

CTO @ Overnet

Agenda

- Data Protection
- Data on different SQL environments
- Database Threats
- Defender for SQL
- Azure Portal vs Security Portal

Need for Data Protection

Data is one of an organization's most valuable assets, but it’s constantly at risk.

External threats

Cyberattacks, ransomware, data breaches

Insider risks

Accidental data exposure, malicious insiders

Compliance challenges

Increasing regulatory requirements for data protection

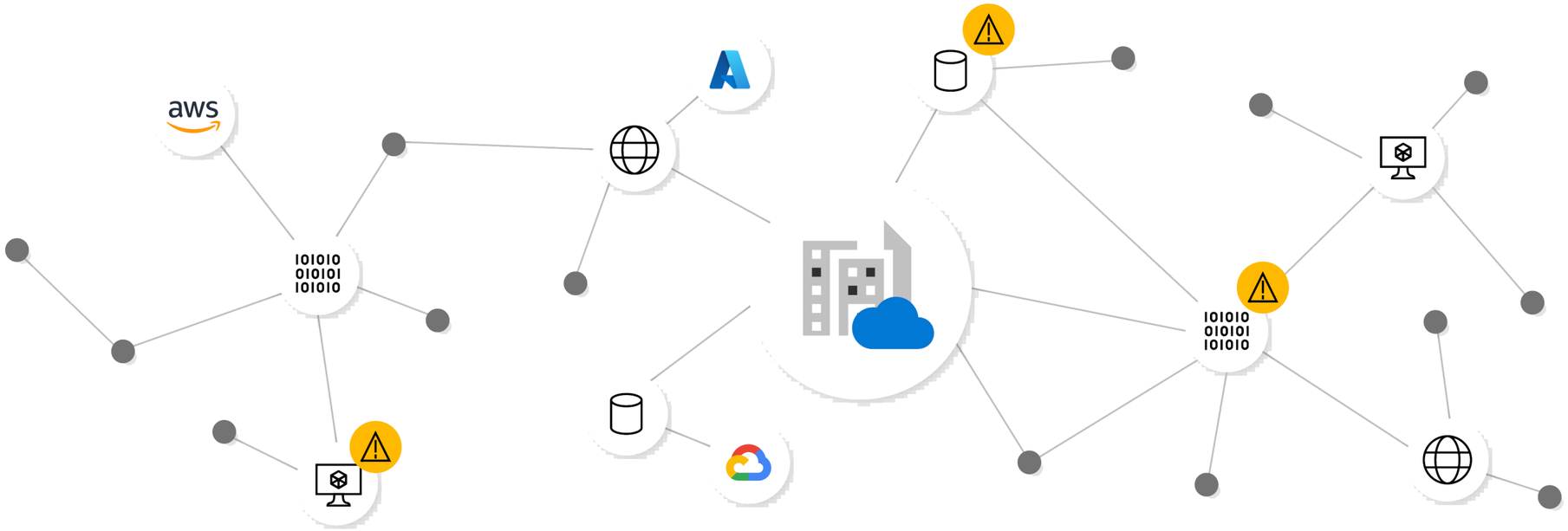
AI security risks

Protecting data used in AI-driven services

Organizations must take a **proactive** approach to **protect** and **govern** their data to reduce risk.

Data protection is a challenge

- Data assets are complex and dynamic (local and cloud)
- Getting ahead on threat requires visibility into data security posture
- Detecting ongoing data breach is critical



Data is everywhere

Collaboration tools

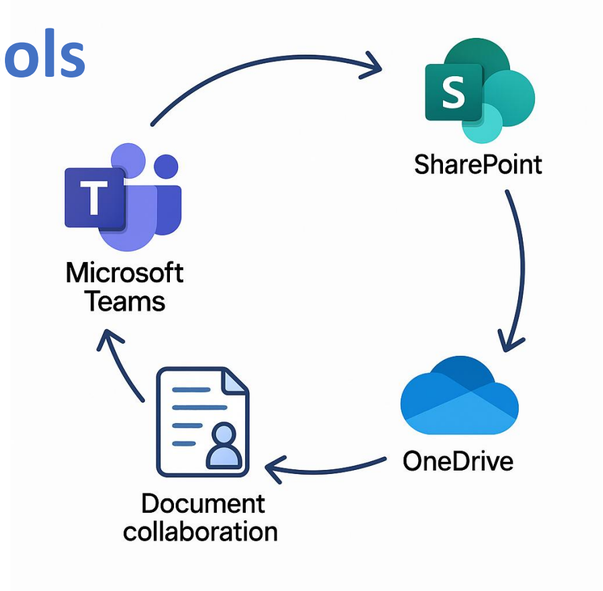
Exchange

Sharepoint

Onedrive

Teams

…



But also…

- Storage Account
  - Block Blob storage
  - Page Blob Storage
  - Azure File

- SQL:
  - local
  - cloud (Azure, GPC, AWS..)

Databases are a prime attack target

They make the world go round.

They are at the heart of every enterprise large or small.

They hold our money, our health, our digital lives.

They're where the AI training data lives, where the ransomware raiders go to pillage and what attackers target

…

IT Security: Cost, Complexity, and Real Risk (2026)

- Global average cost of a data breach: ~$4.44 M (-9% vs 2024) First reduction after 5 years of growth - thanks to AI and automation
- Average identification and containment time: 241 days
- In the USA: average cost ~10.2 M$ (all-time high)

- Silos security: 70-130 average tools per organization
- Only 10-20% of the features actually used
- Impact: TCO +30-35%, slower detection, more human error
- Integrated platforms: up to −$1.25 million per single violation
- Cloud, storage and non-integrated data = increased risk and costs

Fragmented security vs. integrated platform

Fragmented security: independent and poorly integrated instruments

- Many consoles, manual correlation, reactive processes
- Higher costs: duplicate licenses and increased operational load
- Risks: Slower detection and higher probability of error

Integrated security platform

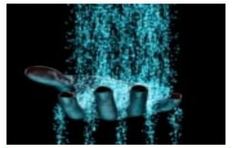
- A single view on identity, endpoint, cloud e dati
- Automation, native correlation and faster response
- Benefits: Reduction of TCO and average cost of a breach

Most Famous Database Attack

HealthEquity says data breach impacts 4.3 million people

HSA provider HealthEquity has determined that a cybersecurity incident disclosed earlier this month has compromised the information of 4,300,000 people.

BILL TOULAS JULY 29, 2024 11:54 AM 1



Hackers leak 2.7 billion data records with Social Security numbers

Almost 2.7 billion records of personal information for people in the United States were leaked on a hacking forum, exposing names, social security numbers, all known physical addresses, and possible aliases.

LAWRENCE ABRAMS AUGUST 11, 2024 10:17 AM 24

Patelco notifies 726,000 customers of ransomware data breach

Patelco Credit Union warns customers it suffered a data breach after personal data was stolen in a RansomHub ransomware attack earlier this year.

BILL TOULAS AUGUST 26, 2024 03:30 PM 3

MediSecure: Ransomware gang stole data of 12.9 million people

MediSecure, an Australian prescription delivery service provider, revealed that roughly 12.9 million people had their personal and health information stolen in an April ransomware attack.

SERGIU GATLAN JULY 19, 2024 01:05 PM 0

Pure Storage confirms data breach after Snowflake account hack

Pure Storage, a leading provider of cloud storage systems and services, confirmed on Monday that attackers breached its Snowflake workspace and gained access to what the company describes as telemetry information

SERGIU GATLAN JUNE 11, 2024 08:48 AM 3

Keytronic reports losses of over $17 million after ransomware attack

Electronic manufacturing services provider Keytronic has revealed that it suffered losses of over $17 million due to a May ransomware attack.

SERGIU GATLAN AUGUST 05, 2024 12:49 PM 0

Toyota confirms third-party data breach impacting customers

Toyota confirmed that customer data was exposed in a third-party data breach after a threat actor leaked an archive of 240GB of stolen data on a hacking forum.

SERGIU GATLAN AUGUST 19, 2024 04:51 PM 5

Payment gateway data breach affects 1.7 million credit card owners

Payment gateway provider Slim CD has disclosed a data breach that compromised credit card and personal data belonging to almost 1.7 million individuals.

BILL TOULAS SEPTEMBER 09, 2024 10:34 AM 2

Neiman Marcus confirms data breach after Snowflake account hack

Luxury retailer Neiman Marcus confirmed it suffered a data breach after hackers attempted to sell company's database stolen in recent Snowflake data theft attacks.

LAWRENCE ABRAMS JUNE 25, 2024 10:43 AM 0

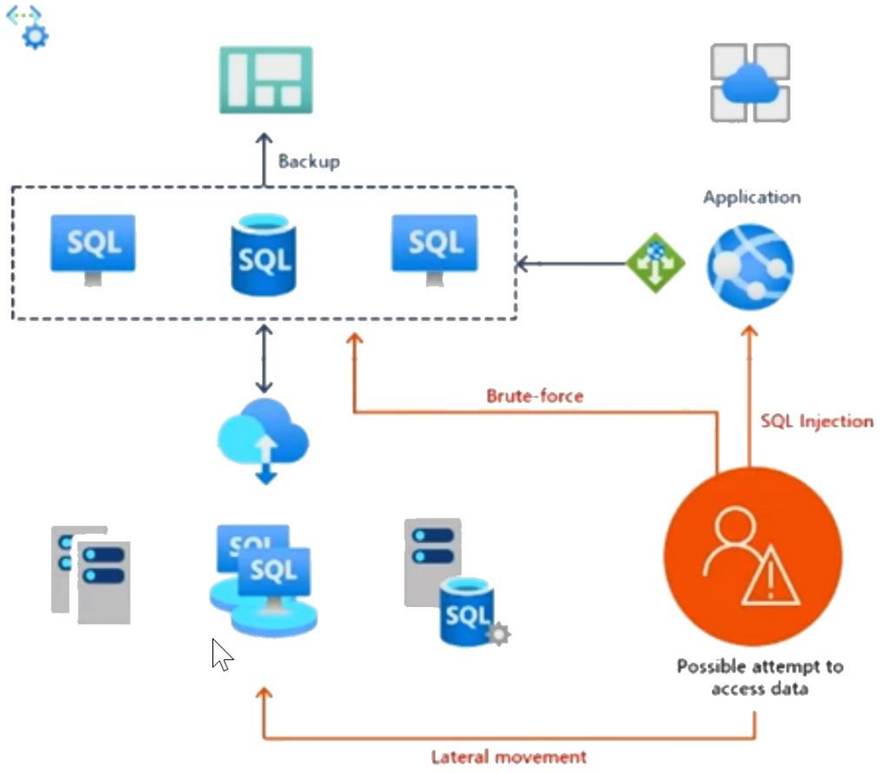
BBC suffers data breach impacting current, former employees

The BBC has disclosed a data security incident that occurred on May 21, involving unauthorized access to files hosted on a cloud-based service, compromising the personal information of BBC Pension Scheme members.

BILL TOULAS MAY 30, 2024 10:02 AM 0

Common database threats

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



What workloads do we need to protect?

SQL Server, Instance, Database

SQL as IaaS

SQL Server on Azure VM

Azure Arc enabled SQL Server

SQL Server on premises

SQL Server on Google Compute Engine VMs

Sql Server on AWS EC2

Azure SQL Database

Azure SQL Managed Instance

Azure SQL Elastic Pools

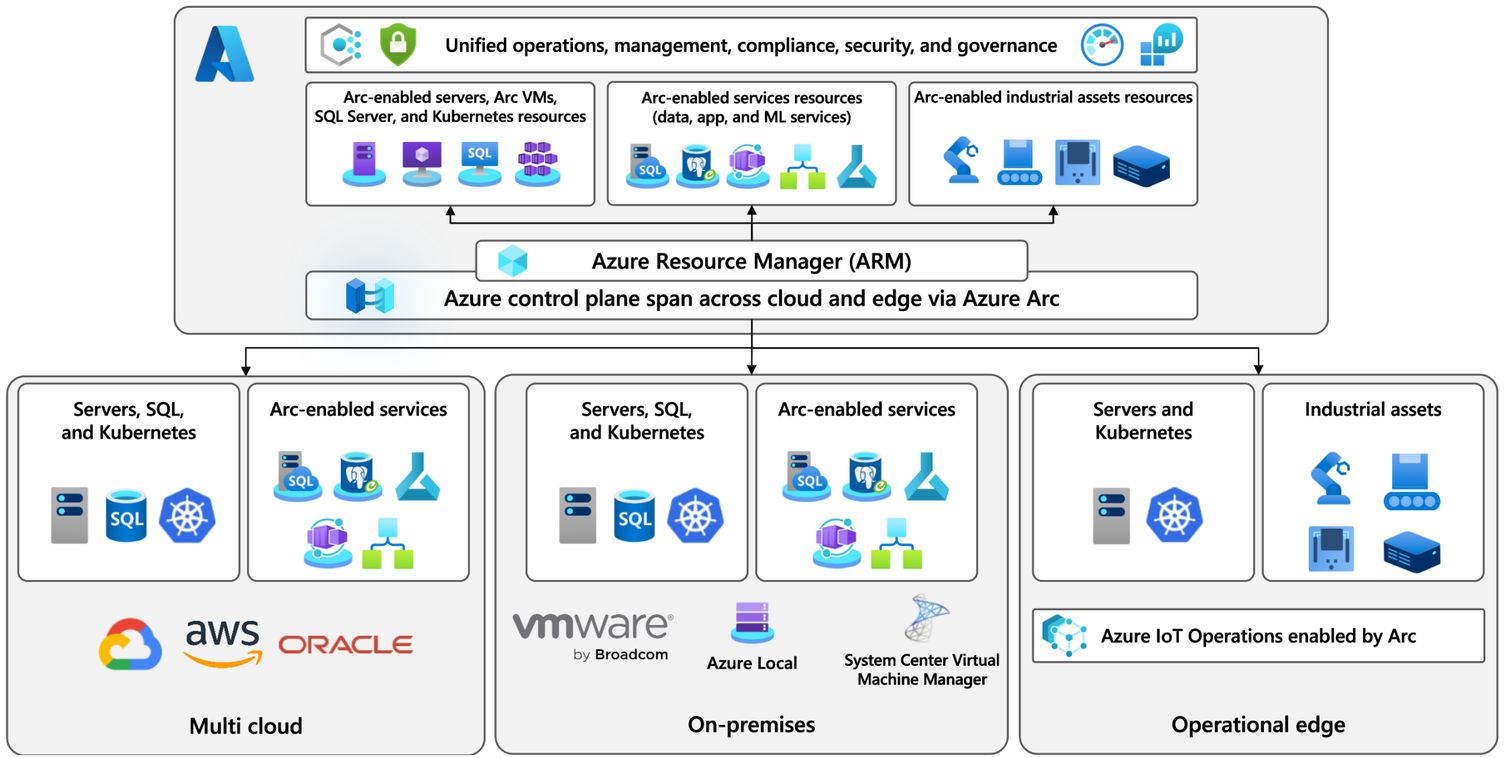
Dedicated SQL pool in Azure Synapse

SQL Server AWS RDS Custom

SQL as PaaS

Azure ARC

Azure ARC Architecture



Azure Arc simplifies **governance and management** by delivering a consistent **multicloud** and **on-premises** management platform.

Azure Arc provides a **centralized**, unified way to:

- Manage your entire environment together by projecting your existing **non-Azure** and/or **on-premises** resources into Azure Resource Manager.
- Manage **virtual machines**, Kubernetes clusters, and **databases** as if they are running in Azure.
- Use familiar Azure services and management capabilities, regardless of where your resources live.

Azure ARC: Server vs SQL

Azure Arc for Servers

- **Level** | **Infrastructure**
- **Resource** | HybridCompute / Machines
- **Agent** | Connected Machine Agent
- **Focus** | Server-Level Management

Use Cases

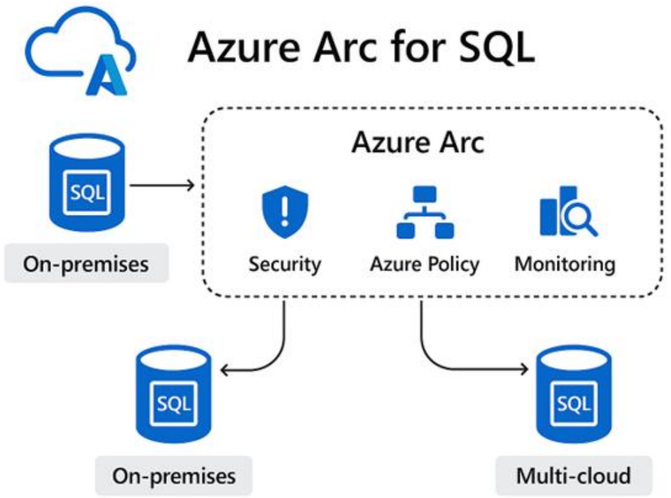
- Governance
- Security & Compliance
- Monitoring

Azure Arc for SQL

- **Level** | Workload
- **Resource** | SQL Server Instances
- **Agent** | SQL Extension
- **Focus** | Database-Level Management

Use Cases

- Security & Compliance
- Data & Auditing



Azure ARC for SQL

Centralized Management

Manage SQL Servers outside Azure from the Azure portal.
Apply **Azure Policy** for compliance across hybrid environments.

Security & Compliance

Integrates with **Microsoft Defender for SQL** for:

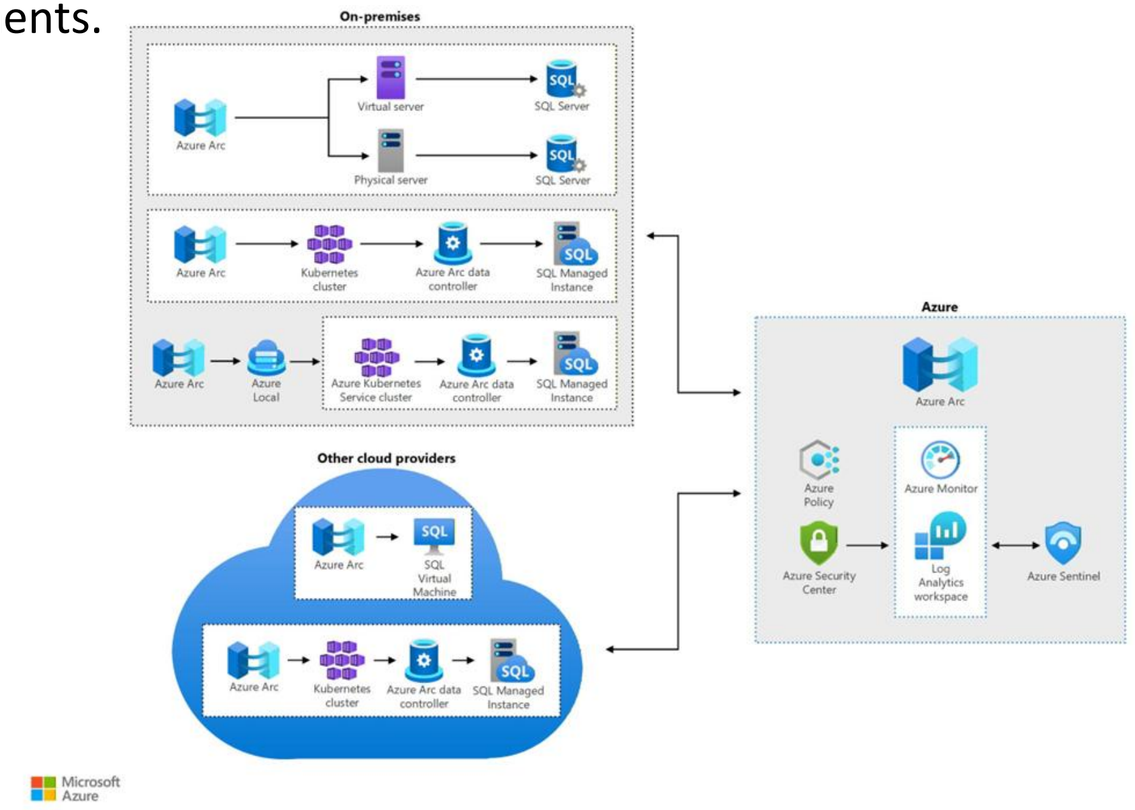
- **Advanced Threat Protection** (detect SQL injection, anomalous access).
- **Vulnerability Assessment** (misconfigurations, weak permissions).

Inventory & Monitoring

Collects metadata for inventory and health checks.
Enables **Log Analytics** and **Azure Monitor** integration.

Hybrid Benefits

Works across **on-premises**, **AWS**, **GCP**, and **Azure**.



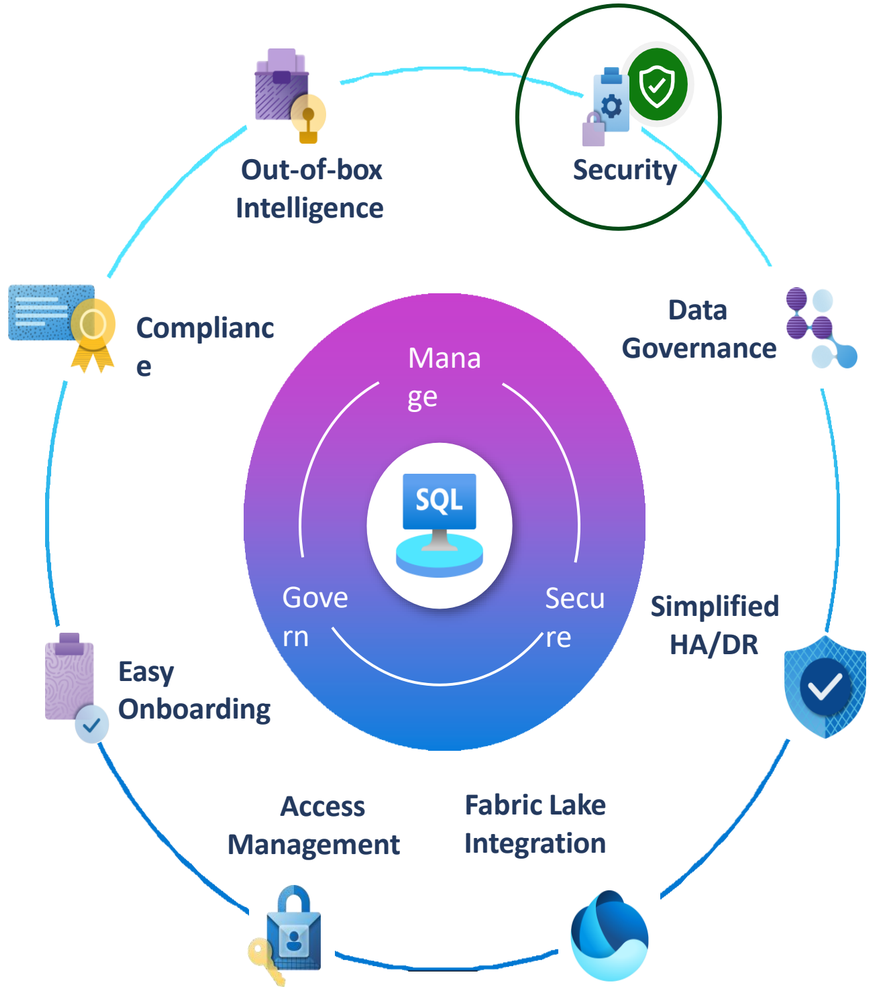
What is the SQL extension?

The SQL extension is a management tool that is currently available on all Azure SQL virtual machines and SQL servers connected through Azure Arc.

It helps to:

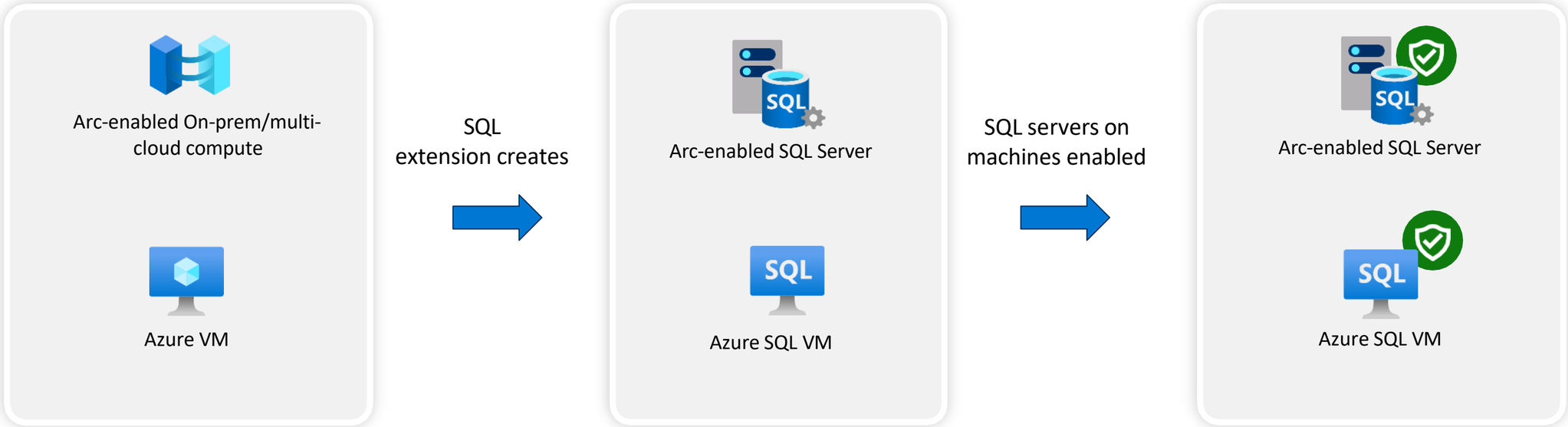
- Facilitate a smoother migration process to Azure
- Enable large-scale management of your SQL environment
- Enhance the security posture of

  your databases



Enhanced agent architecture

- Defender targets resources created by SQL extension
- SQL extension already utilizes a proven bi-directional comm. channel
- Defender will leverage SQL extension comm. channel instead of MMA/AMA
- Enablement and protection process

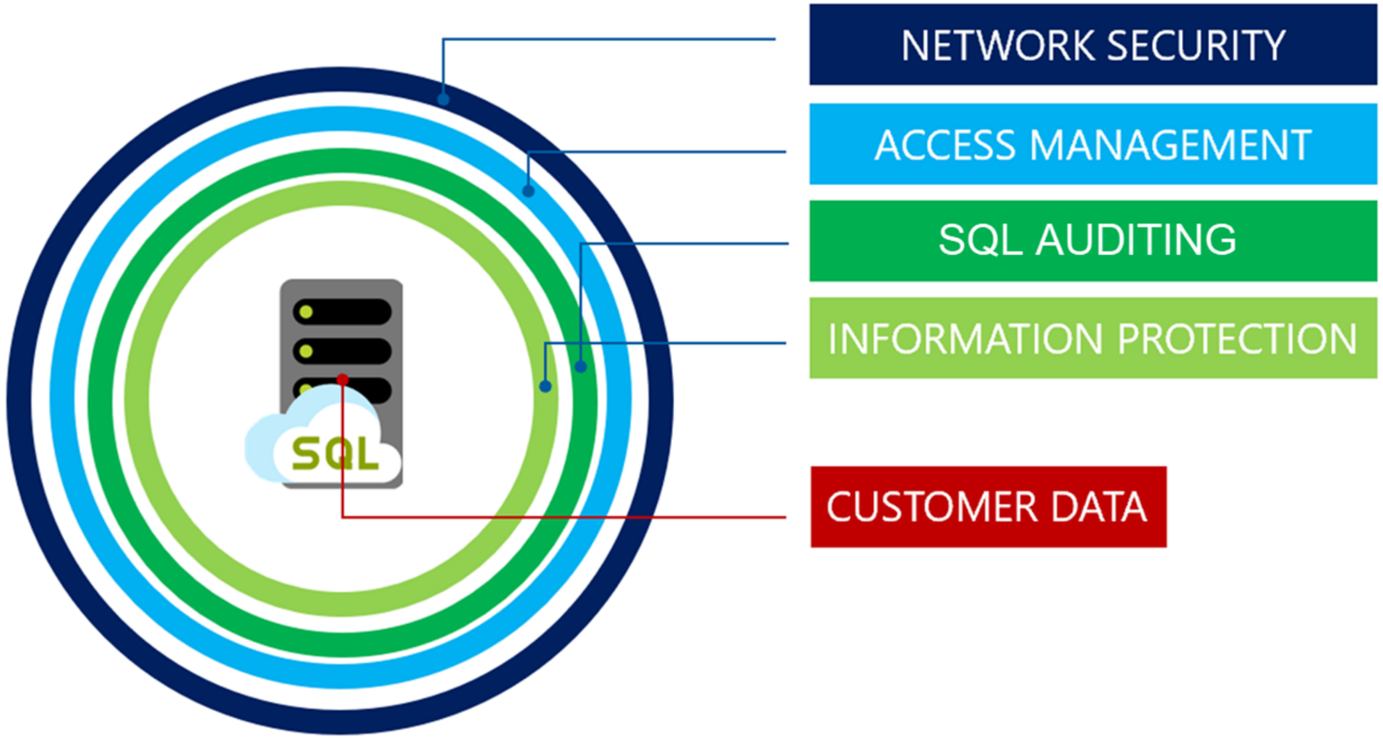


Demo
Azure ARC

How to protect workloads?

Database Security
Control Plane vs Data Plane

Control Plane
Use built-in security tools for SQL



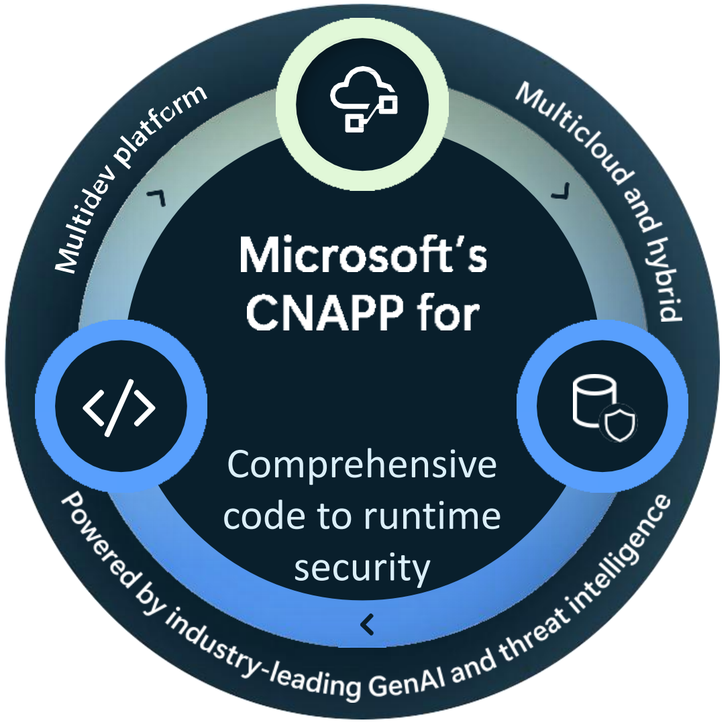
Data Plane
Microsoft Defender for Cloud

Continuously reduce risk

Contextual and prioritized security posture management
across the entire cloud application lifecycle

Enable secure development

Prevent vulnerabilities and misconfiguration in code



Remediate threats faster

Near real-time detection and response for cloud workloads, data and APIs
in a unified SecOps experience

AWS Azur Google Cloud Azure DevOps GitHub GitLa

CSPM: Cloud Security Posture Management; CIEM: Cloud Identity and Entitlement Management; CWP: Cloud Workload Protection; CDR; Cloud Detection and Response

Defender for Cloud: CSPM + CWPP

Cloud Security Posture Management (CSPM)

Is a core feature of Microsoft Defender for Cloud. CSPM provides continuous visibility into the security state of your cloud assets and workloads, offering actionable guidance to improve your security posture across Azure, AWS, and GCP.

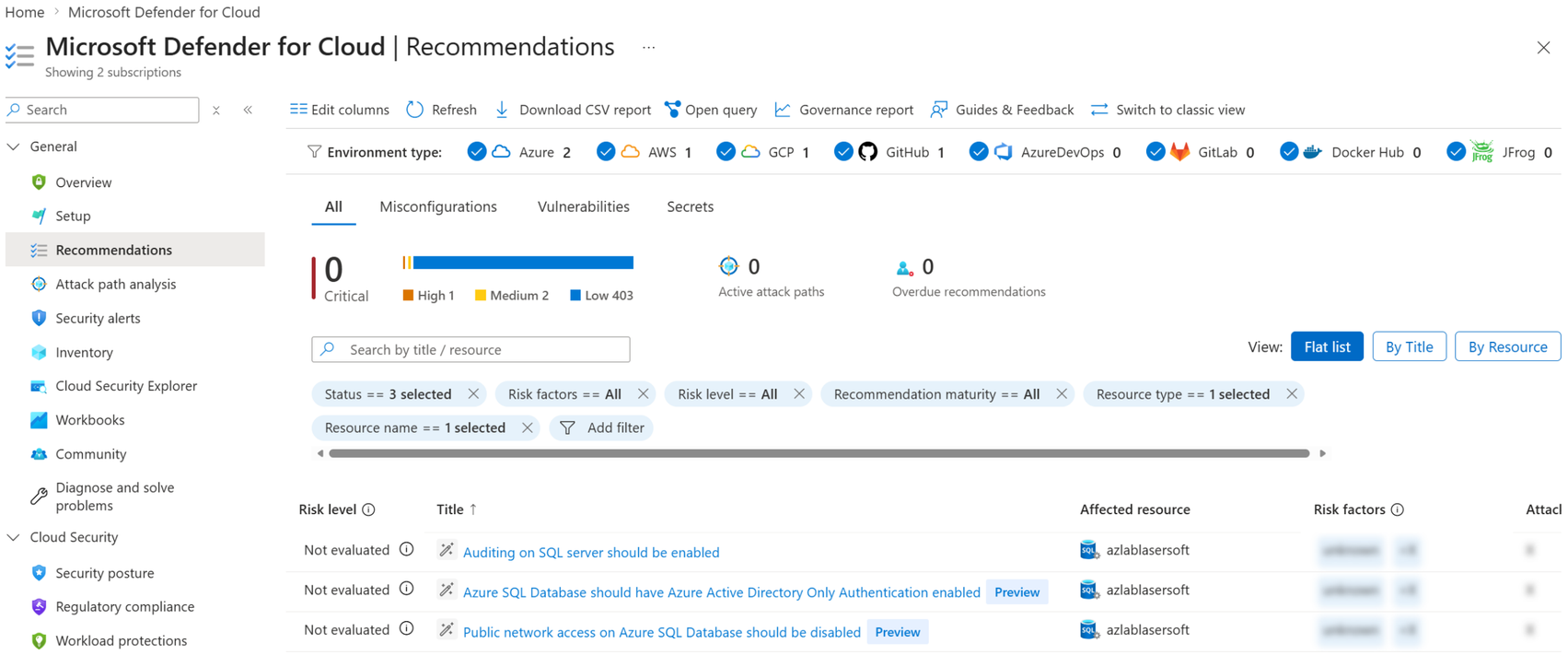
- **Foundational CSPM** (free): Enabled by default for all onboarded subscriptions and accounts.

- **Defender CSPM** (paid): Provides extra capabilities beyond the foundational CSPM plan, including advanced CSPM tools for cloud visibility and compliance monitoring. This version of the plan offers more advanced security posture features such as:

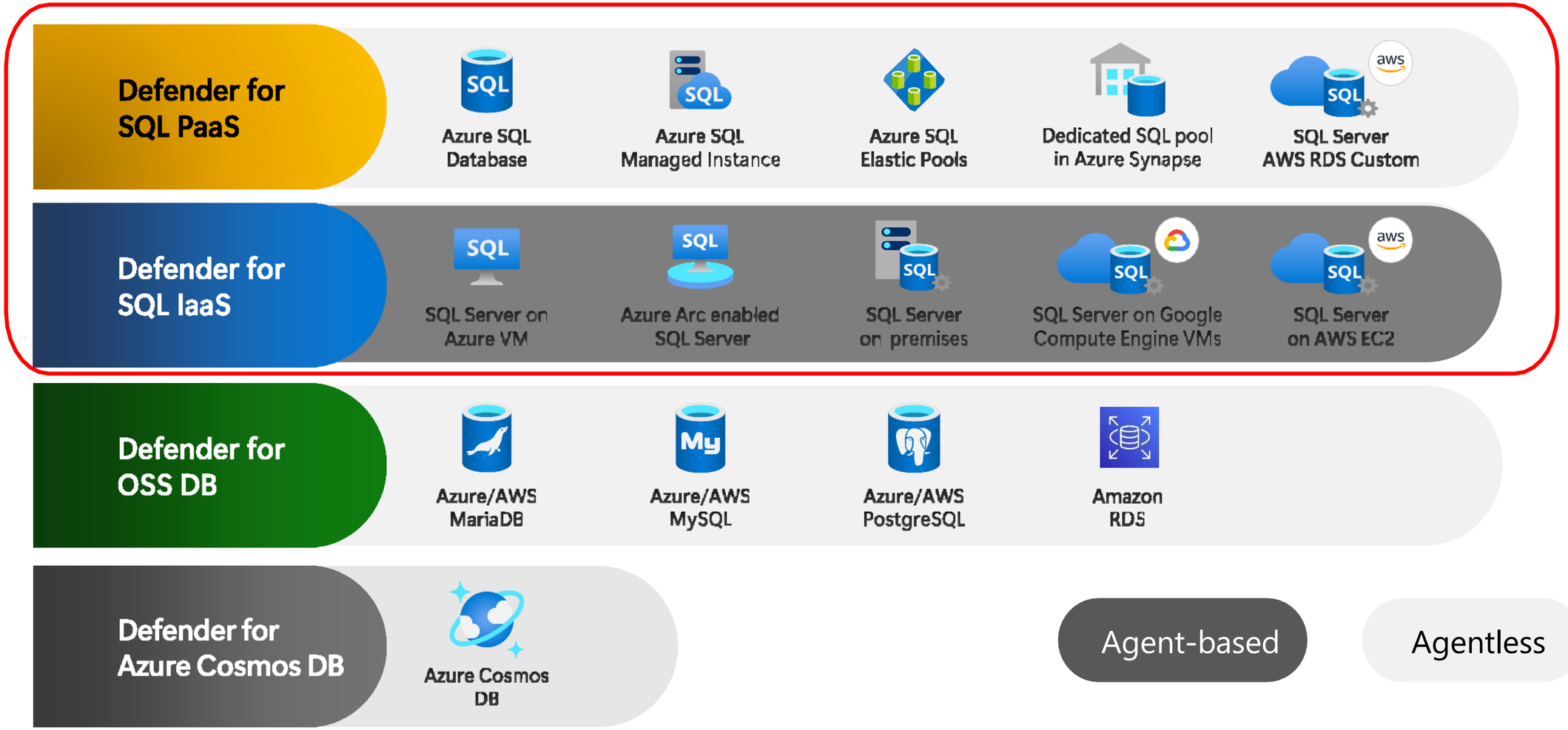
  - AI security posture,
  - Attack path analysis,
  - Risk prioritization,
  - Internet Exposure Analysis,
  - External Attack Surface,
  - Agentless scanning,
  - CIEM (Cloud Infrastructure Entitlement Management),
  - DevOps (GitHub / Azure DevOps)
  - Advanced Support multi-cloud.

Database Posture - Recommendations

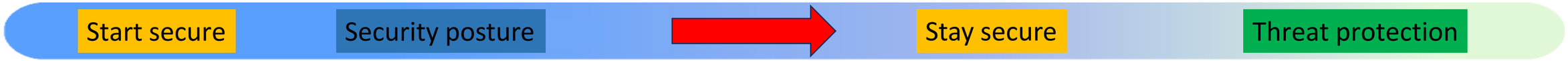
- SQL Server without TDE
- Auditing disabled
- Missing data classification
- Soft delete non active
- Backup policy
- Vulnerability Assessment not enabled
- ....



CWPP: Defender for Database plans



Defender for Database security



Centralize Multicloud and hybrid security

One-click enablement to protect your databases across Azure, AWS RDS and on-premises workloads.

Find Database Vulnerability and posture risk

Flag database security vulnerabilities, such as misconfigurations, excessive permissions, and internet exposure across PaaS and IaaS databases.

Detect and Respond to database threads

Gain actionable insights with MITRE ATT&CK-mapped database alerts, enriched by Microsoft threat intelligence.

Respond to Threads with confidence

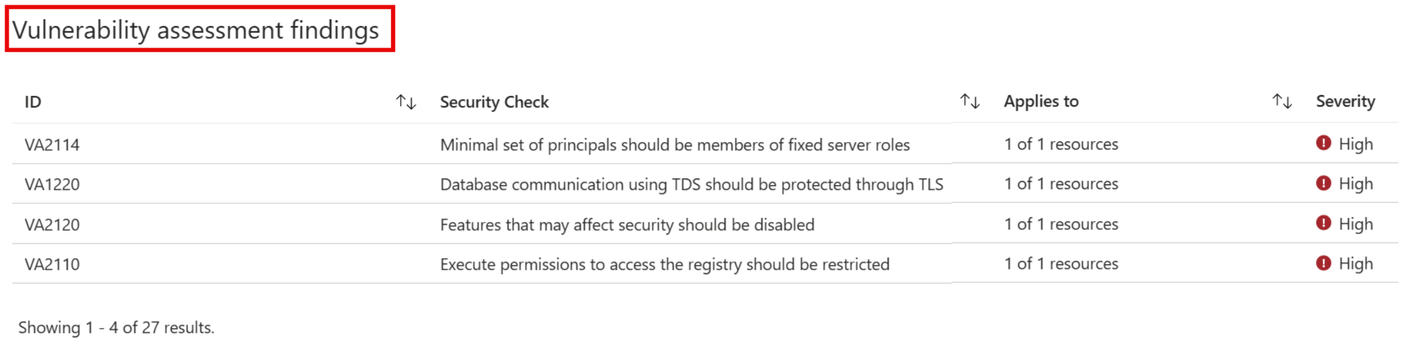
Get exclusive database threat protection with Microsoft Defender for Cloud, plus seamless threat response via Sentinel, Security Copilot, and Microsoft Defender XDR

Azure SQL DB | Azure SQL VM | Azure Arc SQL | AWS RDS | PostgreSQL | MySQL | Maria DB

Defender for Database

SQL vulnerability assessment

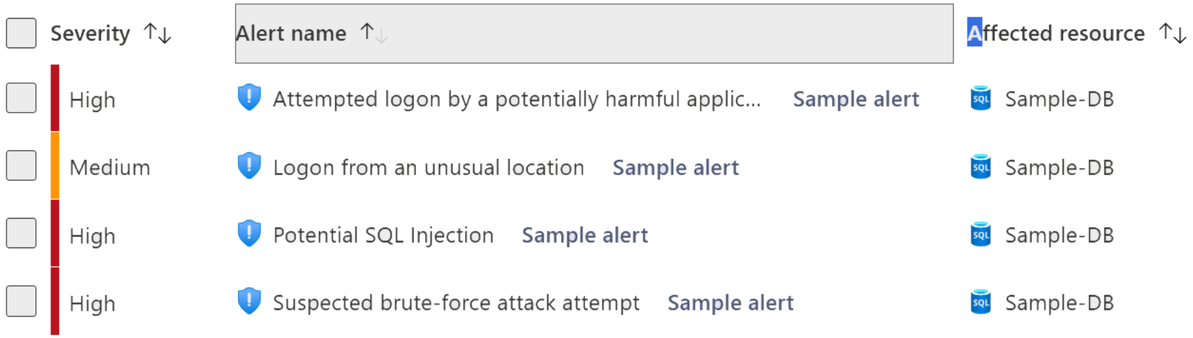
Scan databases to discover, track, and remediate vulnerabilities.



Vulnerability assessment findings

ID	Security Check	Applies to	Severity
VA2114	Minimal set of principals should be members of fixed server roles	1 of 1 resources	High
VA1220	Database communication using TDS should be protected through TLS	1 of 1 resources	High
VA2120	Features that may affect security should be disabled	1 of 1 resources	High
VA2110	Execute permissions to access the registry should be restricted	1 of 1 resources	High

Showing 1 - 4 of 27 results.



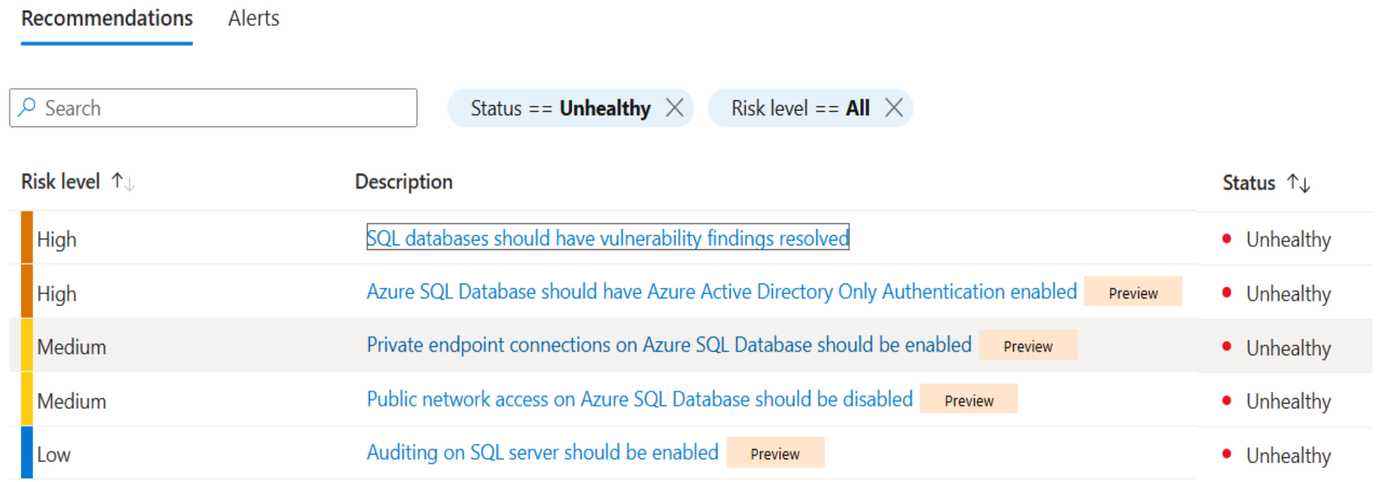
Severity	Alert name	Affected resource
High	Attempted logon by a potentially harmful applic... Sample alert	Sample-DB
Medium	Logon from an unusual location Sample alert	Sample-DB
High	Potential SQL Injection Sample alert	Sample-DB
High	Suspected brute-force attack attempt Sample alert	Sample-DB

SQL Advanced Threat Protection

Mitigate threats by receiving detailed security alerts and recommended actions based on SQL Advanced Threat Protection

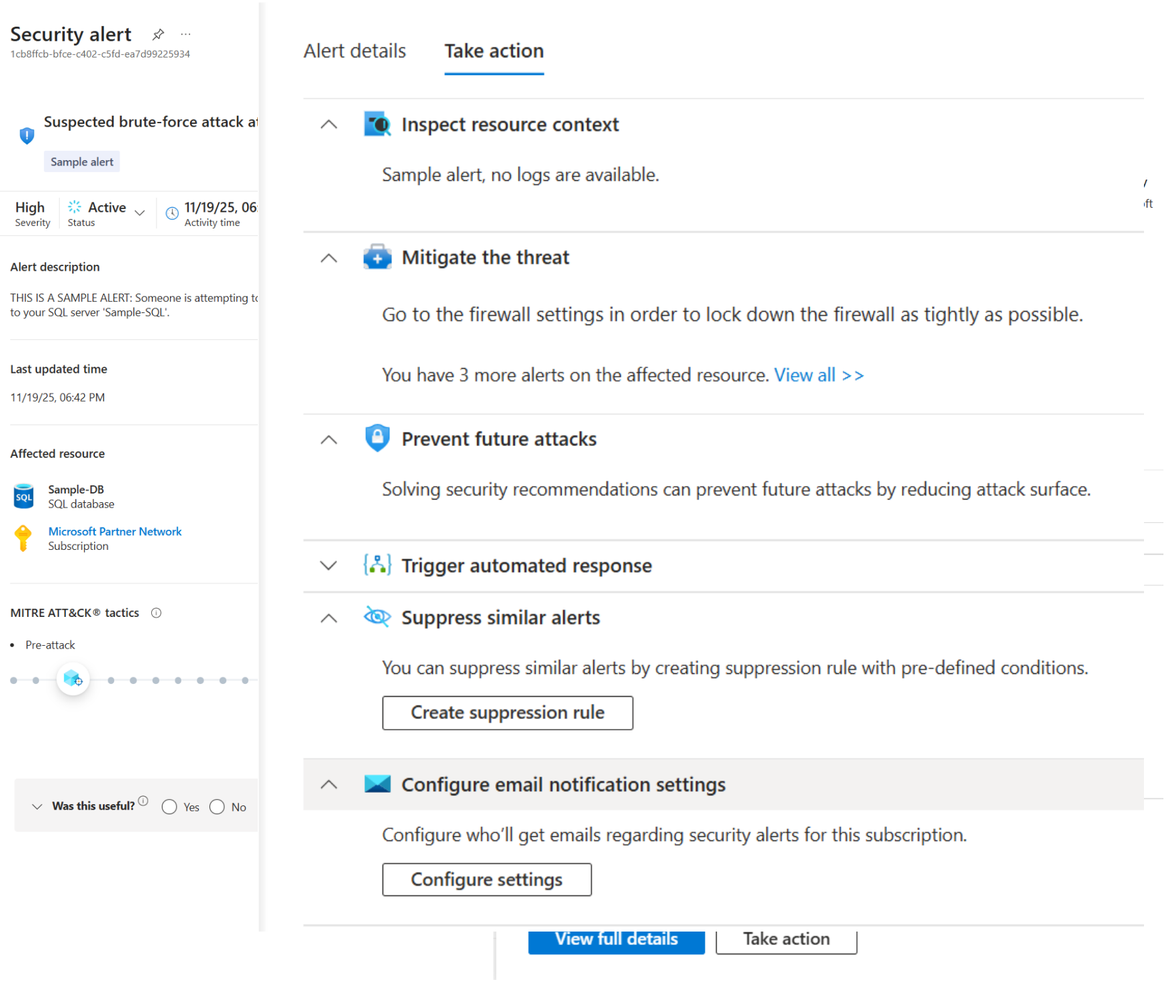
SQL vulnerability assessment

- Address security vulnerabilities and strengthen your database protection
- Enhance your security stance
- Express and Classic configuration
- Removal of the SQL VA in SQL Server Management Studio 19.1
- Report includes:
  - Permission settings
  - Feature settings
  - Database configurations



SQL Advanced Threat Protection

- **Proactive protection** against common threats like SQL Injection and unauthorized access.
- **Faster response** time thanks to detailed alerts and actionable recommendations.
- **Simple management** without requiring advanced security expertise.



Demo
Defender for Database

#Milano

Slide e video:
https://www.globalazuremilano.it