Well-Architected:
Public Cloud Security Posture

10.10.2022

elisa

A SUSTAINABLE
FUTURE THROUGH
DIGITALISATION

Cloud Security Posture Management (CSPM)

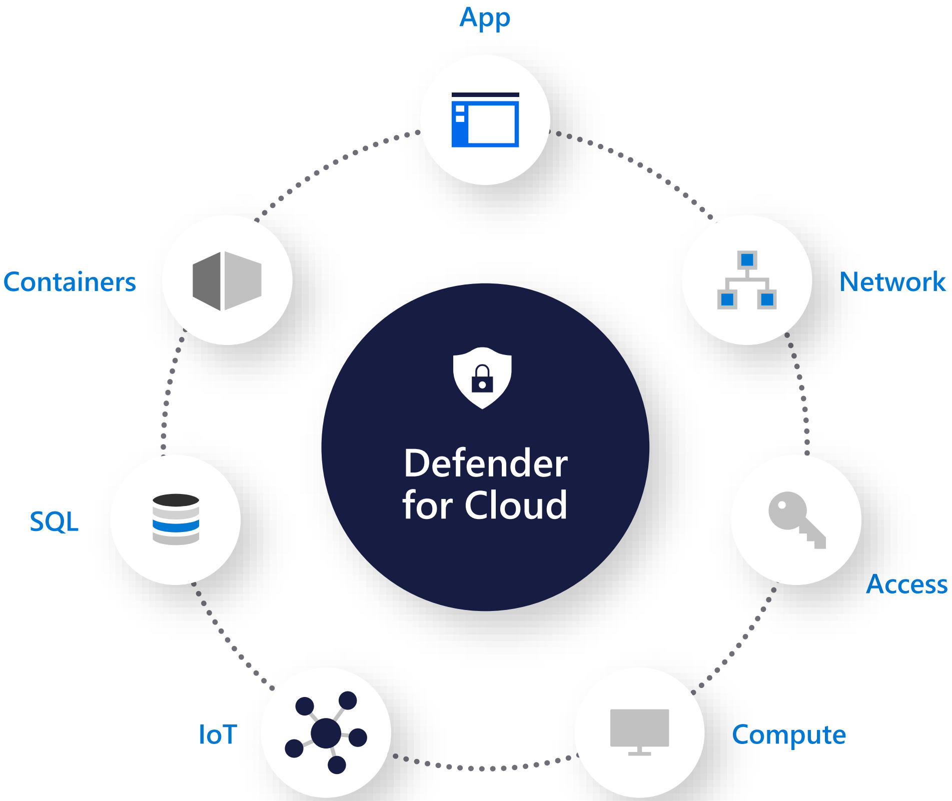
- Visualization of security posture of all cloud assets in a holistic way
- Identifying misconfiguration and cyber threats
- Continuous monitoring of assets and remediation based on recommendations

- Should be part of Cloud Operations

Defender for Cloud

Industry's most mature cloud native CSPM

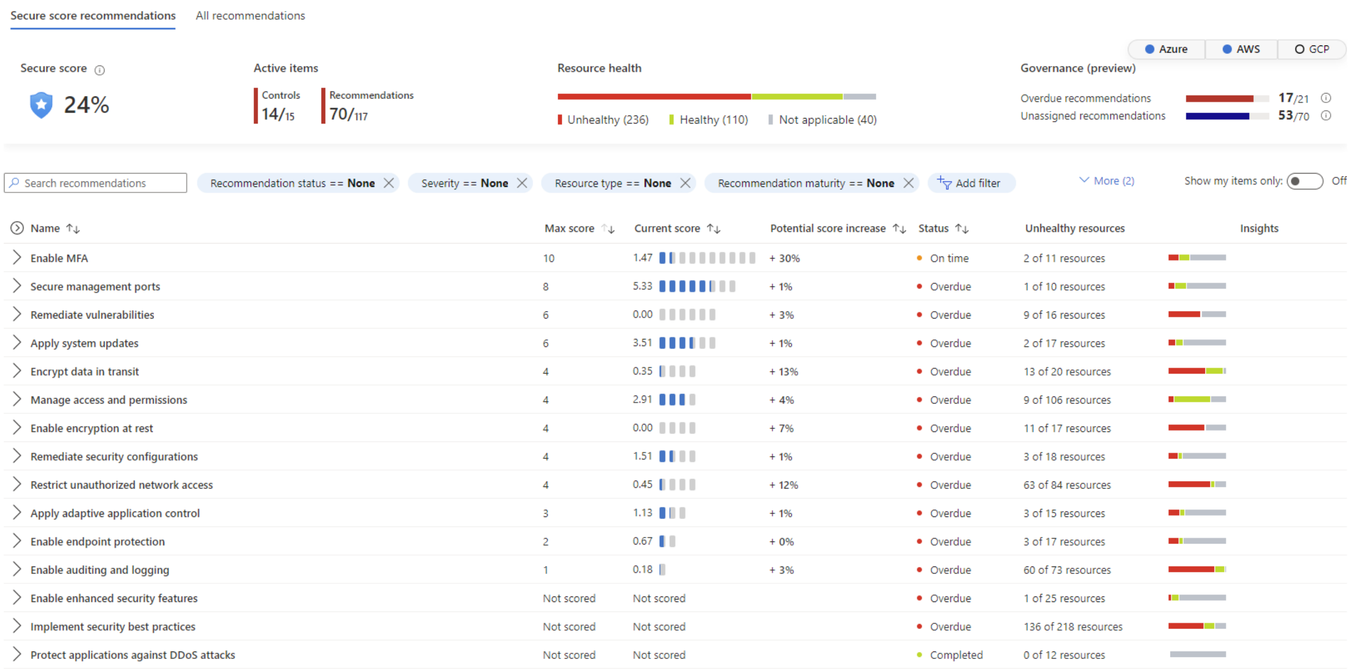
- → Get a bird's-eye security posture view across Azure, and other supported public clouds
- → Continuously monitor and protect all your cross-cloud resources
- → Actionable best practice recommendations going beyond NIST/CIS
- → Get visibility into the compliance state of your Azure environment



Multi-cloud coverage

Microsoft Azure · aws Amazon Web Services · Google Cloud

Secure score recommendations - example



Secure score recommendations | All recommendations

Azure | AWS | GCP

Secure score
24%

Active items
Controls 14/15
Recommendations 70/117

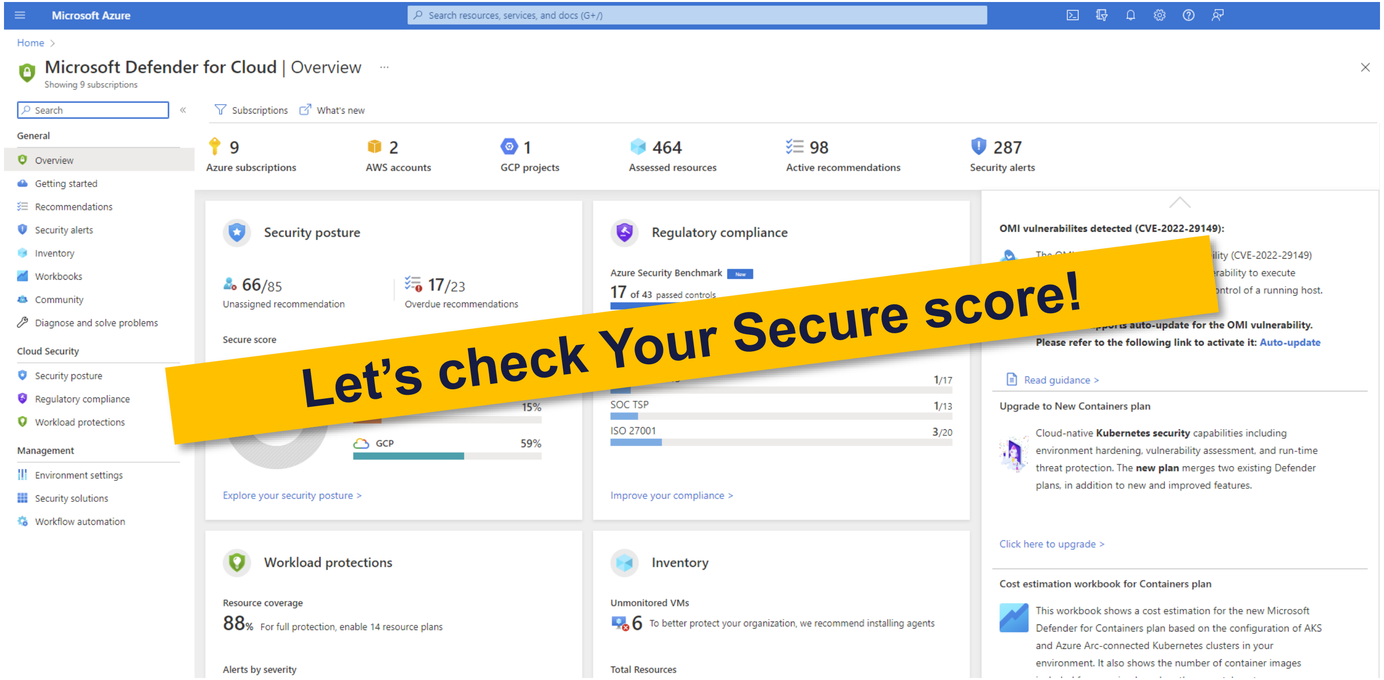
Resource health
Unhealthy (236) | Healthy (110) | Not applicable (40)

Governance (preview)
Overdue recommendations 17/21
Unassigned recommendations 53/70

Search recommendations | Recommendation status == **None** | Severity == **None** | Resource type == **None** | Recommendation maturity == **None** | Add filter | More (2) | Show my items only: Off

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	1.47	+ 30%	● On time	2 of 11 resources	
Secure management ports	8	5.33	+ 1%	● Overdue	1 of 10 resources	
Remediate vulnerabilities	6	0.00	+ 3%	● Overdue	9 of 16 resources	
Apply system updates	6	3.51	+ 1%	● Overdue	2 of 17 resources	
Encrypt data in transit	4	0.35	+ 13%	● Overdue	13 of 20 resources	
Manage access and permissions	4	2.91	+ 4%	● Overdue	9 of 106 resources	
Enable encryption at rest	4	0.00	+ 7%	● Overdue	11 of 17 resources	
Remediate security configurations	4	1.51	+ 1%	● Overdue	3 of 18 resources	
Restrict unauthorized network access	4	0.45	+ 12%	● Overdue	63 of 84 resources	
Apply adaptive application control	3	1.13	+ 1%	● Overdue	3 of 15 resources	
Enable endpoint protection	2	0.67	+ 0%	● Overdue	3 of 17 resources	
Enable auditing and logging	1	0.18	+ 3%	● Overdue	60 of 73 resources	
Enable enhanced security features	Not scored	Not scored		● Overdue	1 of 25 resources	
Implement security best practices	Not scored	Not scored		● Overdue	136 of 218 resources	
Protect applications against DDoS attacks	Not scored	Not scored		● Completed	0 of 12 resources	

Secure score recommendations



Microsoft Azure

Search resources, services, and docs (G+/)

Home >

Microsoft Defender for Cloud | Overview ···

Showing 9 subscriptions

Search

General
- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security
- Security posture
- Regulatory compliance
- Workload protections

Management
- Environment settings
- Security solutions
- Workflow automation

Subscriptions | What's new

9	Azure subscriptions
2	AWS accounts
1	GCP projects
464	Assessed resources
98	Active recommendations
287	Security alerts

Security posture

66/85 Unassigned recommendation

17/23 Overdue recommendations

Secure score

15%

GCP 59%

Explore your security posture >

Regulatory compliance

Azure Security Benchmark New

17 of 43 passed controls

1/17

SOC TSP 1/13

ISO 27001 3/20

Improve your compliance >

OMI vulnerabilites detected (CVE-2022-29149):

The OM… …ility (CVE-2022-29149) …rability to execute …ontrol of a running host.

…pports auto-update for the OMI vulnerability. Please refer to the following link to activate it: Auto-update

Read guidance >

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

Click here to upgrade >

Cost estimation workbook for Containers plan

This workbook shows a cost estimation for the new Microsoft Defender for Containers plan based on the configuration of AKS and Azure Arc-connected Kubernetes clusters in your environment. It also shows the number of container images

Workload protections

Resource coverage

88% For full protection, enable 14 resource plans

Alerts by severity

Inventory

Unmonitored VMs

6 To better protect your organization, we recommend installing agents

Total Resources

Let's check Your Secure score!

Public Cloud Security Posture Analysis and Remediation as a Service

- Expert led one-time analysis and remediation of current situation
  - Close co-operation with applications' owners and/or vendors

- Ability to onboard customer to continuous monitoring and start of remediation service

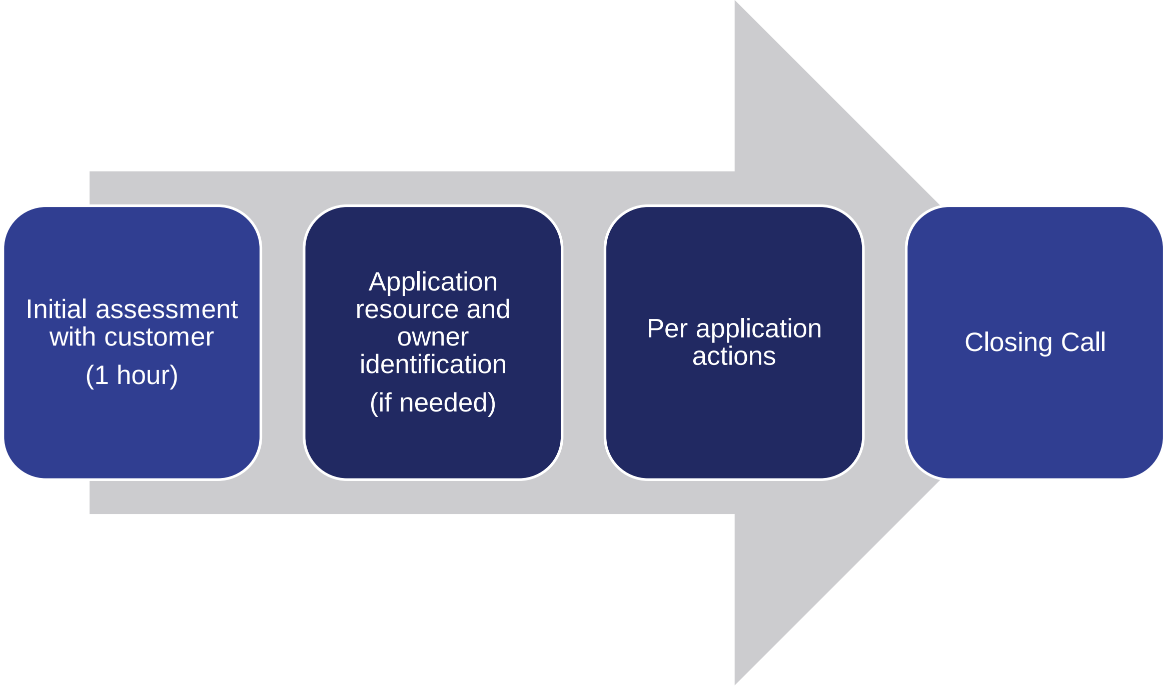
elisa

Non-Public

Scope

- Azure workloads that are deployed in customer’s Azure environment
- All workload types are supported
- Assessments uses only free Azure posture management features

Phasing



Initial assessment with customer

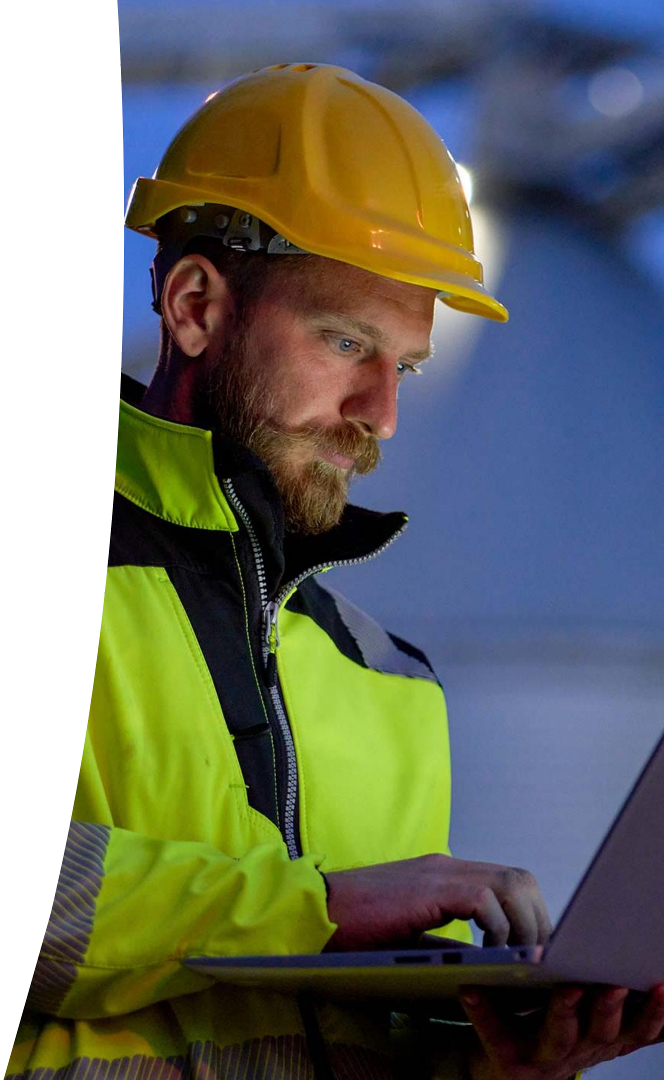
(1 hour)

Application resource and owner identification

(if needed)

Per application actions

Closing Call



Timeline: Depends on applications and availability of customer/provider resources

Initial assessment

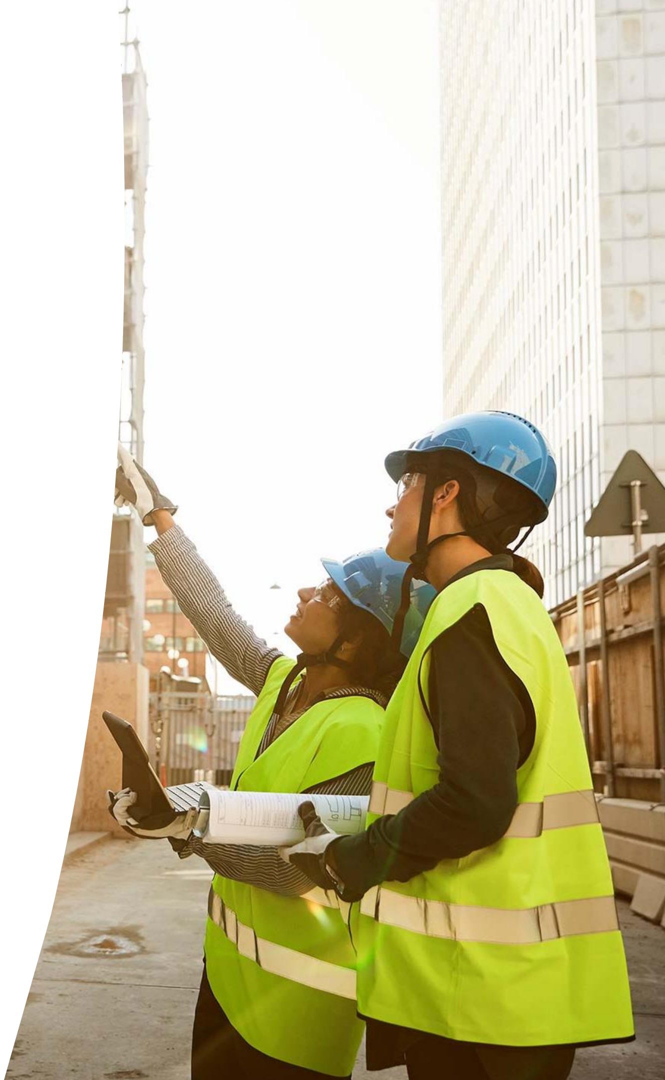
- Overview for Defender for Cloud information
  - Secure Score
  - Recommendations
  - High level configuration check for Defender for Cloud
- First application
  - Identification
  - Tags
  - Recommendations → Actions

Application resource and owner identification (if needed)

- Information can be used in **automated actions** and is needed for per application actions in this service

- Every resource is mapped to application and owner is identified

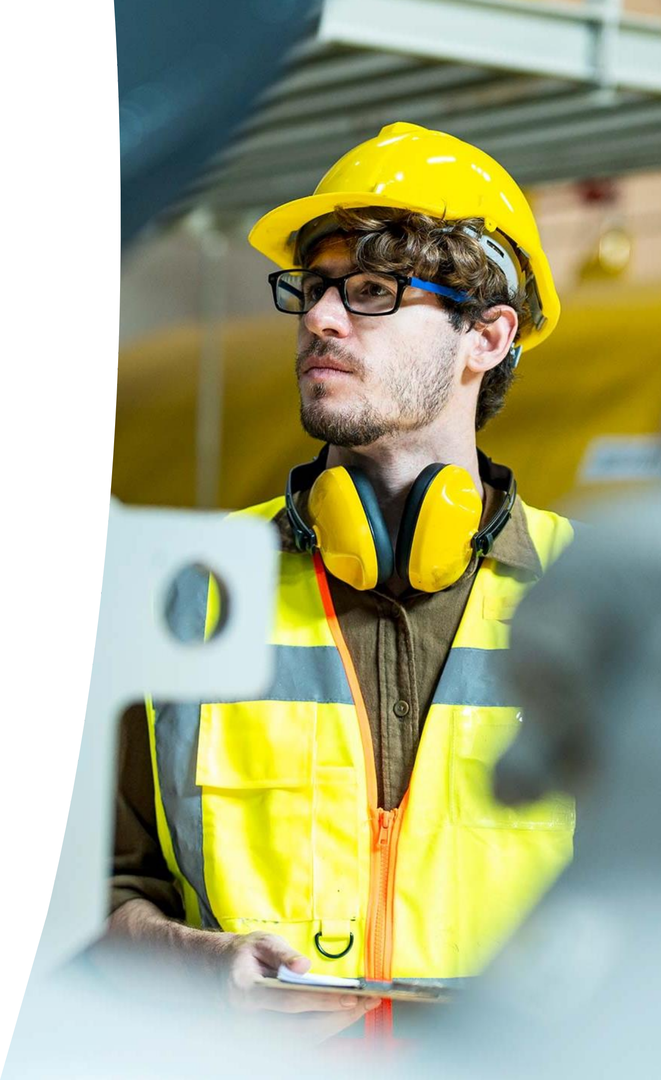
- Documented in Tags: Application, Owner



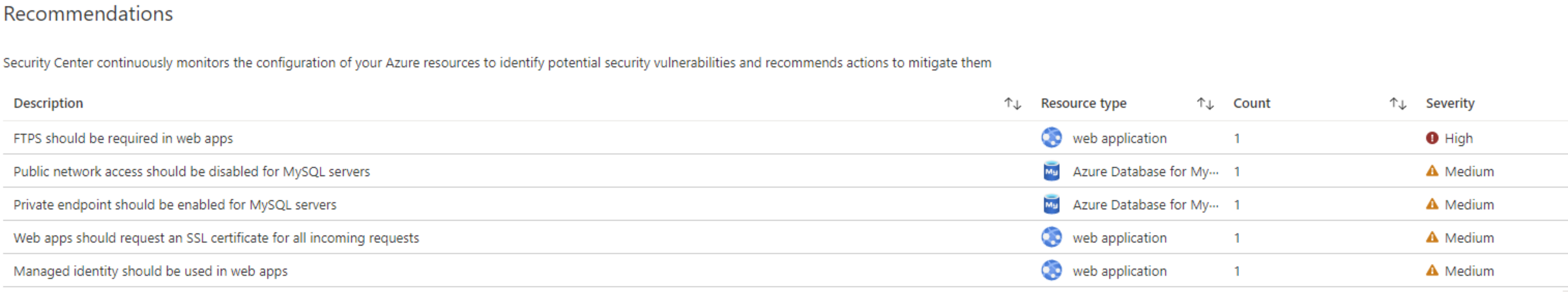
Per application actions

- Identify needed changes - Workshop if needed
- Work with application owner or 3rd party provider

- Implement changes or document exempt



Example – Wordpress based website (PaaS)



Recommendations

Security Center continuously monitors the configuration of your Azure resources to identify potential security vulnerabilities and recommends actions to mitigate them

Description	Resource type	Count	Severity
FTPS should be required in web apps	web application	1	High
Public network access should be disabled for MySQL servers	Azure Database for My...	1	Medium
Private endpoint should be enabled for MySQL servers	Azure Database for My...	1	Medium
Web apps should request an SSL certificate for all incoming requests	web application	1	Medium
Managed identity should be used in web apps	web application	1	Medium

Actions taken by Elisa

- Workshop with vendor to check if changes are possible
- Enable FTPS, HTTPS enforcement
- Exempt Private Endpoint requirements as virtual network is not feasiable

Time used (2 hours)

- 1 hour workshop with vendor
- 1 hour for changes and exempt documentation

Pre-requirements

- All permissions are subscription-level permissions

- **Reader** + **Tag Contributor** permissions for application resource and owner identification
- **Security reader** permissions for assessment phase
- **Contributor** permissions for enablement of Cloud Workload Protection and governance audits

Deliverables

✓ All applications in Azure evaluated and security recommendations either **Fixed** or **Exempted**

Resources are mapped to applications and are documented in Azure (Tags)

Applications' ownership is clarified and documented in Azure (Tags)

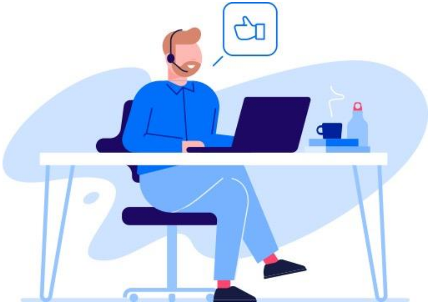
Documentation of findings and actions that have been taken

Pricing

- 750€ fixed pricing for initial assessment and actions for the first application
- Next applications for time and material basis
  - Estimate per application is 1-8 hours

Optional work items

- Posture analysis for other public clouds by using Microsoft Defender for Cloud
- Continuous posture monitoring by Elisa with SLA backed start of remediation
- Workload protection assessment and configuration based on Defender for Cloud – also in other clouds and on-premises
- Hardened landing zone configuration to avoid posture management affects afterwards



A SUSTAINABLE
FUTURE THROUGH
DIGITALISATION