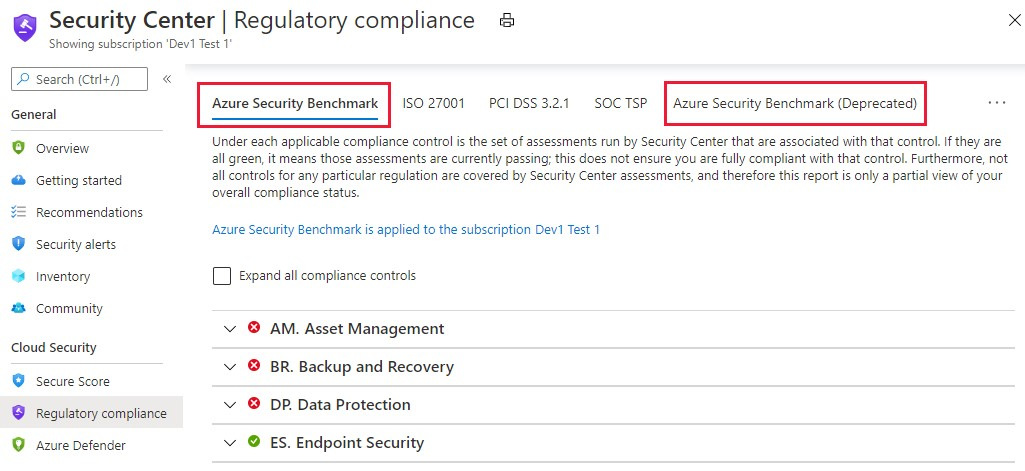
**Microsoft Cloud Security Benchmark**

The Microsoft Cloud Security Benchmark (MCSB) is a set of recommendations and best practices provided by Microsoft to enhance the security of applications and data in the cloud.



**Purpose:**

The MCSB aims to provide clear and concrete guidance on how to securely configure cloud resources hosted on Azure.

**Focus:**

The benchmark focuses on cloud-centric control areas and provides recommendations consistent with well-known security benchmarks such as the Center for Internet Security (CIS) Controls, National Institute of Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS)

**Versions:**

The benchmark has gone through different versions, including Azure Security Benchmark (ASB) v2, ASB v3, and MCSB v1.

**Control Domains:**

The benchmark covers various control domains related to cloud security, including network security, identity and access management, data protection, and more.

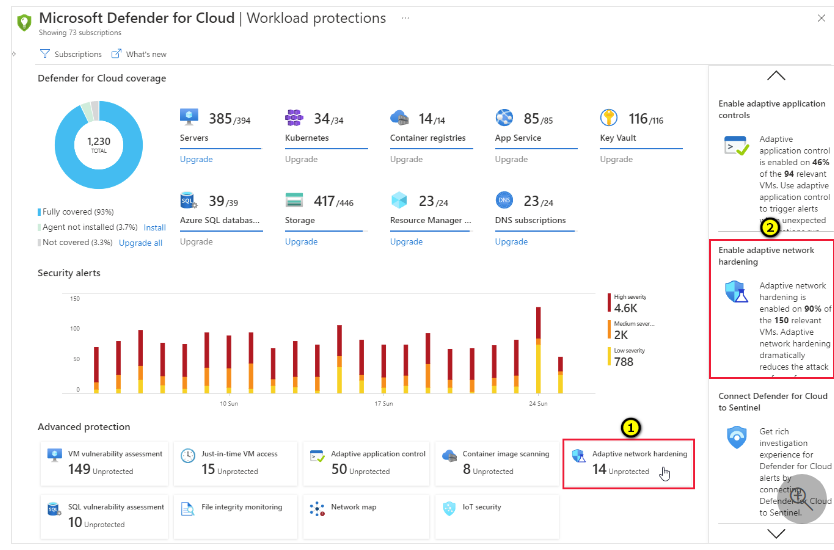
**Feedback and Participation:**

Microsoft encourages users to provide feedback and actively participate in the development and improvement of the benchmark.

**Security Controls:**

**Network Security:**

Network Security covers controls to secure and protect networks, including securing virtual networks, establishing private connections, preventing, and mitigating external attacks, and securing DNS.



**Identity Management:**

Its use for managing user identities, authentication methods, access controls, and privilege management to ensure proper user access and reduce the risk of unauthorized access.

**Data Protection:**

Guidance on securing data at rest and in transit, implementing encryption, managing data classification and handling, and protecting against data leaks or breaches.

**Privileged access:**

Privileged Access covers controls to protect privileged access to your Azure tenant and resources, including a range of controls to protect your administrative model, administrative accounts, and privileged access workstations against deliberate and inadvertent risk.

**Asset Management:**

Asset management security control benchmark in Azure" refers to a set of standards and practices that guide how you manage and secure the valuable digital assets you use in Microsoft's Azure cloud platform.

**Logging and threat detection:**

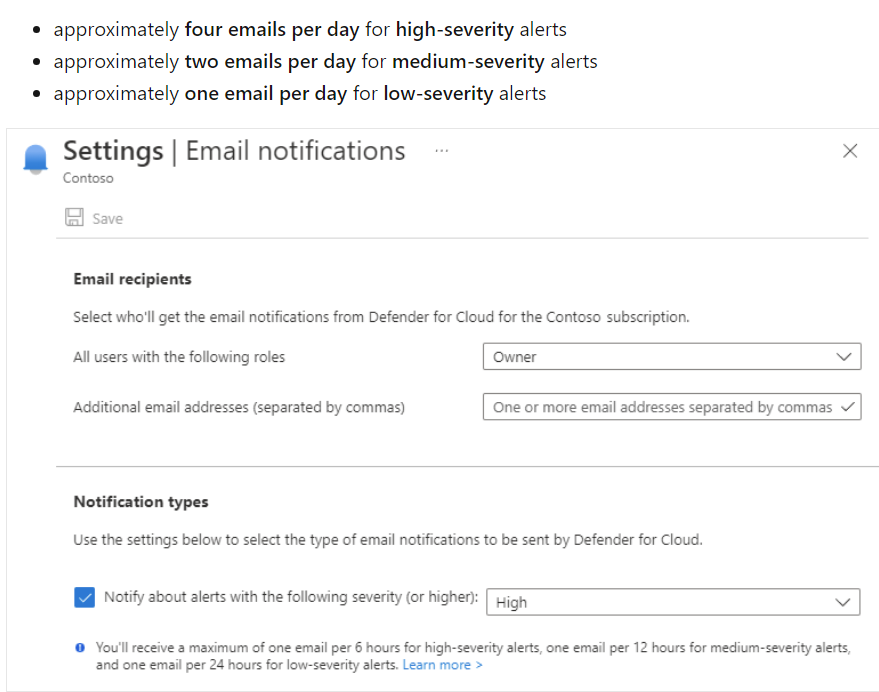
Logging and Threat Detection covers controls for detecting threats on Azure and enabling, collecting, and storing audit logs for Azure services, including enabling detection, investigation, and remediation processes with controls to generate high-quality alerts with native threat detection in Azure services.

A screenshot of a computer

Description automatically generated

**Incident Response:**

This plan outlines how to quickly identify, respond to, and recover from any security problems that could affect your digital assets or data within Azure.



**Posture and vulnerability management:**

Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting, and correction in Azure resources.

**Endpoint security:**

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

A screenshot of a computer

Description automatically generated

**Backup and recovery:**

Backup and Recovery covers controls to ensure that data and configuration backups at the different service tiers are performed, validated, and protected.

**DevOps Security:**

Guidance on integrating security practices into the DevOps process, including secure development, continuous integration and deployment (CI/CD) pipelines, and secure configuration management.

**Pros:**

1. It helps you meet security and compliance requirements for your cloud workloads.
2. It provides clear and concrete guidance on how to securely configure your cloud resources.
3. It enables you to accelerate both initial and ongoing onboarding/assessments of your cloud environments

**Cons:**

1. It may not cover all the specific security needs of your organization or industry.
2. It may require additional tools or services to implement or monitor the recommendations.
3. It may change over time as new threats or technologies emerge

**Security baselines for Azure**

Security baselines for Azure are like checklists that tell you how to make your Azure services more secure. They are based on best practices from experts and organizations. They help you avoid common security mistakes and protect your data and resources from threats.

**API Management:**

API management in Azure is a service that helps you **publish, secure, and monitor your APIs** across different environments.

This security baseline applies guidance from the [Microsoft cloud security benchmark version 1.0](https://learn.microsoft.com/en-us/security/benchmark/azure/overview) to API Management. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to API Management.

**App Service:**

[Azure App Service is a platform as a service (PaaS) that lets you build and host web apps, mobile back ends, and RESTful APIs in various languages without managing infrastructure](https://learn.microsoft.com/en-us/azure/app-service/overview).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to App Service.

**Application Gateway:**

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Application Gateway.

**Active Directory Domain Services:**

Azure Active Directory Domain Services (Azure AD DS) is a cloud service in Microsoft Azure that brings the features of traditional Windows server-based Active Directory to the cloud. It lets you manage user identities, logins, and access permissions for your applications and computers in a similar way to how you'd do it in an office network.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Active Directory Domain Services.

**Azure Cosmos DB:**

Azure Cosmos DB is a service that lets you store and access different kinds of data quickly and easily. It can work with many programming languages and devices.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Cosmos DB.

**Azure Database for MySQL:**

Azure Database for MySQL is a service that lets you host a MySQL database in the Microsoft cloud. It is powered by the MySQL community edition, which is a popular open-source relational database.

the Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Database for MySQL - Flexible Server.

**Azure DDoS Protection:**

Azure DDoS Protection is a service that helps you protect your Azure resources from distributed denial of service (DDoS) attacks. DDoS attacks are attempts to make your service unavailable by overwhelming it with fake traffic.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure DDoS Protection.

**Azure DNS:**

Azure DNS is a service that lets you host your DNS domains in the Microsoft cloud. DNS domains are used to translate human-readable names, such as www.example.com, into IP addresses, such as 192.168.1.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure DNS.

**Azure Firewall:**

Azure Firewall is a service that lets you protect your Azure Virtual Network resources from unwanted network traffic.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Firewall.

**Azure Kubernetes Service (AKS):**

[Azure Kubernetes Service (AKS) is a **managed Kubernetes service** that lets you run containerized applications in Azure without having to manage the Kubernetes control plane](https://learn.microsoft.com/en-us/azure/aks/intro-kubernetes).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Kubernetes Service (AKS).

**Azure Load Balancer:**

[Azure Load Balancer is a service that **evenly distributes load (incoming network traffic) across a group of backend resources or servers**](https://learn.microsoft.com/en-us/azure/load-balancer/load-balancer-overview).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Load Balancer.\

**Azure Monitor:**

[Azure Monitor is a monitoring solution that collects, analyzes, and responds to telemetry data from your cloud and on-premises environments](https://learn.microsoft.com/en-us/azure/azure-monitor/overview).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Monitor.

**Azure Private Link:**

Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Private Link.

**Azure Public IP:**

[A public IP address in Azure is a resource that allows an Azure resource to communicate with the Internet or other public-facing Azure services](https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-public-ip-address).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure Public IP.

**Azure SQL:**

[Azure SQL is a family of cloud-based products that use the SQL Server database engine in Azure1](https://learn.microsoft.com/en-us/azure/azure-sql/azure-sql-iaas-vs-paas-what-is-overview?view=azuresql-vm). Azure SQL offers different options to suit your needs.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure SQL.

**Azure functions:**

[Azure Functions is a serverless compute platform that lets you run your code in response to events without managing any infrastructure](https://azure.microsoft.com/en-us/products/functions/).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Functions.

**Key vault:**

[Azure Key Vault is a cloud service that provides a secure store for secrets, such as passwords, certificates, API keys, or cryptographic keys](https://www.bing.com/search?q=what+is+azure+private+link&form=ANNH01&refig=c507833e93f9424fb6af1222168d14cf&showconv=1).

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Functions.

**Network watcher:**

Azure Network Watcher is a service provided by Microsoft Azure that offers a suite of tools to monitor, diagnose, and gain insights into the health and performance of your network resources within an Azure virtual network.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Network Watcher.

**Vmss:**

Virtual Machine Scale Sets (VMSS) is a feature in Microsoft Azure that allows you to deploy and manage a group of identical virtual machines (VMs) with the same configuration, such as the operating system, programs, and data.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual Machine Scale Sets.

**Virtual Machine-Linux:**

Azure, a VM Linux refers to a virtual machine running a Linux operating system within the Azure cloud environment.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual Machines - Linux Virtual Machines.

**Virtual Machine-Windows:**

In Azure, a VM Windows refers to a virtual machine running a Windows operating system within the Azure cloud environment.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual Machines - Windows Virtual Machines.

**Virtual network:**

An Azure Virtual Network (VNet) is a network or environment within Microsoft Azure that allows you to run virtual machines (VMs) and applications in the cloud.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual Network.

**Azure VPN Gateway:**

Azure VPN Gateway is a service provided by Microsoft Azure that enables you to establish secure, cross-premises connectivity between your virtual network within Azure and on-premises IT infrastructure.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to VPN Gateway.

**Azure Nat gateway:**

Azure NAT Gateway is a fully managed and highly resilient Network Address Translation (NAT) service provided by Microsoft Azure. It allows instances within a private subnet to connect outbound to the internet while remaining fully private.

The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Azure NAT Gateway.