Azure security baseline for Azure DDoS Protection

Article • 02/25/2025

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Azure DDoS Protection. 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.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

> **Note**
>
> **Features** not applicable to Azure DDoS Protection have been excluded. To see how Azure DDoS Protection completely maps to the Microsoft cloud security benchmark, see the full Azure DDoS Protection security baseline mapping file .

Security profile

The security profile summarizes high-impact behaviors of Azure DDoS Protection, which may result in increased security considerations.

Expand table

Service Behavior Attribute	Value
Product Category	Networking, Security
Customer can access HOST / OS	No Access
Service can be deployed into customer's virtual network	False
Stores customer content at rest	False

Asset management

For more information, see the Microsoft cloud security benchmark: Asset management.

AM-2: Use only approved services

Features

Azure Policy Support

Description: Service configurations can be monitored and enforced via Azure Policy. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Use Microsoft Defender for Cloud to configure Azure Policy to audit and enforce configurations of your Azure resources. Use Azure Monitor to create alerts when there is a configuration deviation detected on the resources.

Reference: DDOS Protection Policy

Logging and threat detection

For more information, see the Microsoft cloud security benchmark: Logging and threat detection.

LT-4: Enable logging for security investigation

Features

Azure Resource Logs

Description: Service produces resource logs that can provide enhanced service-specific metrics and logging. The customer can configure these resource logs and send them to their own data sink like a storage account or log analytics workspace. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Customer

Configuration Guidance: Configure DDoS diagnostic logs, including notifications, mitigation reports and mitigation flow logs.

Reference: View and configure DDoS diagnostic logging

Next steps

- See the Microsoft cloud security benchmark overview
- Learn more about Azure security baselines