AZURE SECURITY CENTER

Get unmatched hybrid security management and threat protection functionality

ACTIVATE THE PROTECTION YOU NEED

Microsoft uses a wide variety of physical, infrastructure, and operational controls to protect Azure, but these are additional steps you must take to help protect your workloads. Use the Security Center to quickly strengthen your security measures and protect your resources from threats.

ADMINISTRATION OF SECURITY MEASURES FOR YOUR WORKLOADS IN THE CLOUD

Quickly assess your security measures using the Security Score. This feature provides recommendations with numerical values to help you rank responses in order of priority.

Be sure to use best practices and correct common configuration errors for Azure infrastructure as a service (IaaS) and platform as a service (PaaS) resources, which can be:

- Do not implement system updates on virtual machines (VMs).
- Unnecessary exposure to the Internet through connection points facing the public.
- Data not encrypted in transit or storage.

AZURE SECURITY CENTER

Protect your Linux and Windows servers

Security Center helps protect Windows servers and clients with Microsoft Defender Advanced Threat Protection. Besides, it protects Linux servers with behavioral analysis. For every attack that is attempted or carried out, you receive a detailed report and recommended solutions.

Protect servers running on Azure and other clouds with advanced controls. Just-in-Time access to virtual machines reduces the area exposed to brute force attacks using RDP / SSH, one of the most common threats, with more than 100,000 attack attempts on Azure Virtual Machines per month. Use the Standard level to mitigate this threat.

As you add applications to virtual machines in Azure, block malicious applications, including those that do not mitigate anti-malware solutions, using adaptive application controls. Machine Learning automatically applies new application whitelist policies to virtual machines.

Protect your native cloud applications

Fix vulnerabilities in web applications, such as plugins and exposed web pages, which are a frequent target of attackers. The Standard level helps protect applications running in Azure App Service, because it marks the behavior that could happen through web application firewall instruments. It also helps protect other cloud services, such as VM Scale Sets and Containers.

Configure and expand security beyond azure quickly

• Extend security management and threat protection to virtual machines in the local environment.

• Easily provision an agent for server workloads running in the local environment.

• Assess your security with a unified view of your hybrid cloud workloads.

• Connect tools and processes you already use, such as a SIEM (Event Management and Security Information) system, or integrate partner security solutions.

• Reduce investment and reallocate resources using your own or third-party security controls.

HOW DOES SECURITY CENTER WORK?

When Security Center is activated, a monitoring agent is automatically deployed on Azure Virtual Machines instances. On local virtuals machines, you must deploy the agent manually. Security Center begins by assessing the security status of all your virtual machines, networks, applications, and data.

Our analysis engines analyze the data and Machine Learning synthesizes it. Security Center provides recommendations and threat alerts to protect your workloads. You will know immediately if an attack or abnormal activity has occurred.

Gather security information in an-Azure Monitor workspace for big data query functionality. You can also query the data using REST APIs, PowerShell cmdlets, or integration with a SIEM system I've already used, like Azure Sentinel.