Get tips from Azure Security Center

10 minutes

A great place to start when examining the security of your Azure-based solutions is **Azure Security Center**. Security Cent monitoring service that provides threat protection across all of your services both in Azure, and on-premises. Security Ce

- Provide security recommendations based on your configurations, resources, and networks.
- Monitor security settings across on-premises and cloud workloads, and automatically apply required security to nev as they come online.
- Continuously monitor all your services, and perform automatic security assessments to identify potential vulnerabilit they can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines and services. You define a list of allowed applications to ensure that only the apps you validate are allowed to execute.
- Analyze and identify potential inbound attacks, and help to investigate threats and any post-breach activity that mi occurred.
- Provide just-in-time access control for ports, reducing your attack surface by ensuring the network only allows traffi require.

Azure Security Center is part of the Center for Internet Security (CIS) recommendations.

Available tiers

Azure Security Center is available in two tiers:

1. *Free*. Available as part of your Azure subscription, this tier is limited to assessments and recommendations of Azure only.
2. *Standard*. This tier provides a full suite of security-related services including continuous monitoring, threat detectio time access control for ports, and more.

To access the full suite of Azure Security Center services, you will need to upgrade to a Standard tier subscription. You ca the 30-day free trial from within the Azure Security Center dashboard in the Azure portal. After the 30-day trial period is Azure Security Center is $15 per node per month.

Usage scenarios

You can integrate Security Center into your workflows and use it in many ways. Here are two examples.

1. Use Security Center for incident response.

   Many organizations learn how to respond to security incidents only after suffering an attack. To reduce costs and da important to have an incident response plan in place before an attack occurs. You can use Azure Security Center in stages of an incident response.

Close
Assess
Stabilize

You can use Security Center during the detect, assess, and diagnose stages. Here are examples of how Security Cent
useful during the three initial incident response stages:

- *Detect*. Review the first indication of an event investigation. For example, you can use the Security Center dash
review the initial verification that a high-priority security alert was raised.
- *Assess*. Perform the initial assessment to obtain more information about the suspicious activity. For example, c
more information about the security alert.
- *Diagnose*. Conduct a technical investigation and identify containment, mitigation, and workaround strategies.
example, follow the remediation steps described by Security Center in that particular security alert.

2. Use Security Center recommendations to enhance security.

You can reduce the chances of a significant security event by configuring a security policy, and then implementing t
recommendations provided by Azure Security Center.

- A *security policy* defines the set of controls that are recommended for resources within that specified subscrip
resource group. In Security Center, you define policies according to your company's security requirements.
- Security Center analyzes the security state of your Azure resources. When Security Center identifies potential s
vulnerabilities, it creates recommendations based on the controls set in the security policy. The recommendati
you through the process of configuring the needed security controls. For example, if you have workloads that
require the *Azure SQL Database Transparent Data Encryption* (TDE) policy, turn off the policy at the subscriptic
and enable it only in the resources groups where SQL TDE is required.

ⓘ **Important**

To upgrade a subscription to the Standard tier, you must be assigned the role of *Subscription Owner*, *Subscription Contributor*, or *Security Admin*.

Next unit: Identity and access

Continue >