* 6 minutes

Tailwind Traders is broadening its use of Azure services. It still has on-premises workloads with current security-related configuration best practices and business procedures. How does the company ensure that all of its systems meet a minimum level of security and that its information is protected from attacks?

Many Azure services include built-in security features. Tools on Azure can also help Tailwind Traders with this requirement. Let’s start by looking at Azure Security Center.

## What’s Azure Security Center?

[Azure Security Center](https://azure.microsoft.com/services/security-center) is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises. The term *security posture* refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.

Security Center can:

* Monitor security settings across on-premises and cloud workloads.
* Automatically apply required security settings to new resources as they come online.
* Provide security recommendations that are based on your current configurations, resources, and networks.
* Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
* Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use *adaptive application controls* to define rules that list allowed applications to ensure that only applications you allow can run.
* Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
* Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

This short video explains how Security Center can help harden your networks, secure and monitor your cloud resources, and improve your overall security posture.

## Understand your security posture

Tailwind Traders can use Security Center to get a detailed analysis of different components in its environment. Because the company’s resources are analyzed against the security controls of any governance policies it has assigned, it can view its overall regulatory compliance from a security perspective all from one place.

See the following example of what you might see in Azure Security Center.

![Azure Security Center dashboard showing policy compliance, resource security hygiene, and threat protection.](data:image/png;base64;base64,)

Azure Security Center dashboard showing policy compliance, resource security hygiene, and threat protection.

Let’s say that Tailwind Traders must comply with the Payment Card Industry’s Data Security Standard (PCI DSS). This report shows that the company has resources that it needs to remediate.

In the **Resource security hygiene** section, Tailwind Traders can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Here’s an example.

![Azure Security Center dashboard showing the resource security hygiene section. Recommendations are categorized as low, medium, and high.](data:image/png;base64;base64,)

Azure Security Center dashboard showing the resource security hygiene section. Recommendations are categorized as low, medium, and high.

### What’s secure score?

[Secure score](https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls/) is a measurement of an organization’s security posture.

Secure score is based on *security controls*, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control.

Here’s an example from the Azure portal showing a score of 57 percent, or 34 out of 60 points.

![A screenshot of the Azure portal showing a score of 57 percent, or 34 out of 60 points.](data:image/png;base64;base64,)

A screenshot of the Azure portal showing a score of 57 percent, or 34 out of 60 points.

Following the secure score recommendations can help protect your organization from threats. From a centralized dashboard in Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, data, apps, devices, and infrastructure.

Secure score helps you:

* Report on the current state of your organization’s security posture.
* Improve your security posture by providing discoverability, visibility, guidance, and control.
* Compare with benchmarks and establish key performance indicators (KPIs).

## Protect against threats

Security Center includes advanced cloud defense capabilities for VMs, network security, and file integrity. Let’s look at how some of these capabilities apply to Tailwind Traders.

* **Just-in-time VM access** Tailwind Traders will configure just-in-time access to VMs. This access blocks traffic by default to specific network ports of VMs, but allows traffic for a specified time when an admin requests and approves it.
* **Adaptive application controls** Tailwind Traders can control which applications are allowed to run on its VMs. In the background, Security Center uses machine learning to look at the processes running on a VM. It creates exception rules for each resource group that holds the VMs and provides recommendations. This process provides alerts that inform the company about unauthorized applications that are running on its VMs.
* **Adaptive network hardening** Security Center can monitor the internet traffic patterns of the VMs, and compare those patterns with the company’s current network security group (NSG) settings. From there, Security Center can make recommendations about whether the NSGs should be locked down further and provide remediation steps.
* **File integrity monitoring** Tailwind Traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

## Respond to security alerts

Tailwind Traders can use Security Center to get a centralized view of all of its security alerts. From there, the company can dismiss false alerts, investigate them further, remediate alerts manually, or use an automated response with a *workflow automation*.

Workflow automation uses Azure Logic Apps and Security Center connectors. The logic app can be triggered by a threat detection alert or by a Security Center recommendation, filtered by name or by severity. You can then configure the logic app to run an action, such as sending an email, or posting a message to a Microsoft Teams channel.

## Next unit: Detect and respond to security threats by using Azure Sentinel

[Continue](https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/3-detect-respond-threats-sentinel/)

Need help? See our [troubleshooting guide](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.2-protect-threats-security-center&documentId=30cf7f3d-15ac-dba8-1b8b-797fb7057195&versionIndependentDocumentId=7e2343a0-f406-925d-de9e-8cf406b29c6b&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F2-protect-threats-security-center.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F2-protect-threats-security-center&author=rknapp) or provide specific feedback by [reporting an issue](https://docs.microsoft.com/en-us/learn/support/troubleshooting?uid=learn.azure.protect-against-security-threats-azure.2-protect-threats-security-center&documentId=30cf7f3d-15ac-dba8-1b8b-797fb7057195&versionIndependentDocumentId=7e2343a0-f406-925d-de9e-8cf406b29c6b&contentPath=%2FMicrosoftDocs%2Flearn-pr%2Fblob%2Flive%2Flearn-pr%2Fazure-fundamentals%2Fprotect-against-security-threats-azure%2F2-protect-threats-security-center.yml&url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Flearn%2Fmodules%2Fprotect-against-security-threats-azure%2F2-protect-threats-security-center&author=rknapp#report-feedback).