Create a Security Policy

1. At the Security Center main menu, select **Security policy**. Select the subscription that you want to use. Under **POLICY COMPONENTS**, select **Security policy**:
2. For each security configuration you want to monitor, select **On**. Security Center will continuously assess the configuration of your environment and when vulnerability exists, Security Center will generate a security recommendation. Select **Off** if the security configuration is not recommended or not relevant. For example, in a dev/test environment you might not require the same level of security as a production environment. After selecting the policies that are applicable to your environment, click **Save**.

Wait until Security Center processes these policies and generates recommendations. Some configurations, such as system updates and OS configurations can take up to 12 hours, while network security groups and encryption configurations can be assessed almost instantly. Once you see recommendations in the Security Center dashboard, you can proceed to the next step.

Assess security of resources

1. According to the security policies that were enabled, Security Center will provide a set of security recommendations as needed. You should start by reviewing the virtual machine and computers recommendations. On the Security Center dashboard, click **Overview**, and click **Compute**.

Review each recommendation by prioritizing recommendations in red (high priority). Some of these recommendations have remediation that can be implemented directly from Security Center, such as the [endpoint protection issues](https://docs.microsoft.com/azure/security-center/security-center-install-endpoint-protection). Other recommendations have only guidelines to apply the remediation, such as the missing disk encryption recommendation.

1. Once you address all relevant compute recommendations, you should move on to the next workload: networking. On the Security Center dashboard, click **Overview**, and click **Networking**.

The networking recommendations page has a list of security issues for network configuration, internet facing endpoints, and network topology. Just like **Compute**, some networking recommendations will provide integrated remediation, and some others will not.

1. Once you address all relevant networking recommendations, you should move on to the next workload: storage & data. On the Security Center dashboard, click **Overview**, and click **Storage & data**.

The **Data resources** page contains recommendations around enabling auditing for Azure SQL servers and databases, enabling encryption for SQL databases, and enabling encryption of your Azure storage account. If you don’t have these workloads, you will not see any recommendation. Just like **Compute**, some SQL & storage recommendations will provide integrated remediation, and some others will not.

1. Once you address all relevant SQL & storage recommendations, you should move on to the next workload: Applications. On the Security Center dashboard, click **Overview**, and click **Applications**.

The **Applications** page contains recommendations for web application firewall deployment, and general guidelines for application hardening. If you don’t have virtual machine or computers with web applications running on Internet Information Service (IIS), you will not see these recommendations.