

Mediante las directivas, Defender for Cloud analiza periódicamente el estado de cumplimiento de los recursos para identificar posibles debilidades o errores de configuración de seguridad. Luego, proporciona recomendaciones sobre cómo corregir esos problemas. Las recomendaciones son el resultado de la evaluación de los recursos con respecto a las directivas pertinentes y la identificación de los recursos que no cumplen los requisitos definidos.

Defender for Cloud realiza sus recomendaciones de seguridad en función de las iniciativas elegidas. Cuando una directiva de una iniciativa se compara con los recursos y se encuentra que uno o varios no se ajustan al cumplimiento normativo, se presenta como una recomendación en Defender for Cloud.

Las **recomendaciones** son acciones que se deben llevar a cabo para proteger y consolidar los recursos. Cada recomendación proporciona la siguiente información:

- Descripción breve del problema
- Pasos de corrección que se deben llevar a cabo para implementar la recomendación.
- Recursos afectados.

En la práctica, funciona de la siguiente manera:

1. Azure Security Benchmark es una **iniciativa** que contiene requisitos.

Por ejemplo, las cuentas de Azure Storage deben restringir el acceso a la red para reducir su superficie expuesta de ataques.

2. La iniciativa incluye varias **directivas**, cada una con un requisito de un tipo de recurso específico. Estas directivas aplican los requisitos en la iniciativa.

Para seguir con el ejemplo, el requisito de almacenamiento se aplica con la directiva "Las cuentas de almacenamiento deben restringir el acceso a la red mediante el uso de reglas de red virtual".

3. Microsoft Defender for Cloud evalúa constantemente las suscripciones conectadas. Si detecta un recurso que no cumple una directiva, muestra una **recomendación** para corregir esa situación y reforzar la seguridad de los recursos que no cumplan los requisitos de seguridad.

Home > Visual Studio Enterprise Subscription

## Visual Studio Enterprise Subscription | Security

Subscription

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
**Security**  
Events  
Cost Management  
Cost analysis  
Cost alerts  
Budgets  
Advisor recommendations  
Billing  
Invoices  
External services  
Payment methods  
Partner information

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations Security alerts Azure Defender On

Learn more  
About Microsoft Def

10 0

### Recommendations

Security Center continuously monitors the configuration of your Azure resources to identify potential security vulnerabilities and recommends actions to mitigate them

Description	Resource type	Count	Severity
Machines should have a vulnerability assessment solution	virtual machine	1	Medium
Storage account should use a private link connection	storage account	1	Medium
Storage accounts should restrict network access using virtual network rules	storage account	1	Medium
Subscriptions should have a contact email address for security issues	subscription	1	Low
Guest Configuration extension should be installed on machines	virtual machine	1	Medium

View additional recommendations in Defender for Cloud >

Por ejemplo, si una cuenta de Azure Storage de alguna de sus suscripciones protegidas no está protegida con reglas de red virtual, aparecerá la recomendación para endurecer la seguridad de esos recursos.

Por lo tanto, (1) una iniciativa incluye (2) directivas que generan (3) recomendaciones específicas del entorno.