Microsoft Defender for Cloud es un sistema unificado de administración de la seguridad de la infraestructura que refuerza la posición de seguridad de sus centros de datos y ofrece protección contra amenazas avanzada para las cargas de trabajo híbridas en la nube (en Azure o fuera de Azure) y en el entorno local.

Proteger los recursos es un esfuerzo conjunto entre el proveedor de nube, Azure y usted, el cliente. Cuando migra a la nube, debe asegurarse de que las cargas de trabajo estén seguras y, al mismo tiempo, cuando se migra a IaaS (infraestructura como servicio), el cliente tiene una responsabilidad mayor que cuando se encontraba en PaaS (plataforma como servicio) y SaaS (software como servicio). Microsoft Defender para la nube le proporciona las herramientas necesarias para reforzar la red, proteger los servicios y asegurarse de que tiene la mejor posición de seguridad.

Microsoft Defender for Cloud aborda los tres desafíos de seguridad más urgentes:

- **Cargas de trabajo que cambian con rapidez**: se trata tanto de una fortaleza como de un desafío de la nube. Por un lado, los usuarios finales pueden hacer más cosas. por el otro, ¿cómo puede asegurarse de que los servicios en constante evolución que los usuarios utilizan y crean se rigen según los estándares de seguridad y siguen los procedimientos recomendados de seguridad?

- **Ataques cada vez más sofisticados**: no importa dónde ejecute las cargas de trabajo, los ataques son cada vez más sofisticados. Debe proteger las cargas de trabajo de la nube pública que son, en realidad, una carga de trabajo con conexión a Internet que puede dejarlo incluso más vulnerable si no sigue los procedimientos recomendados de seguridad.

- **Las aptitudes de seguridad son escasas**: el número de alertas de seguridad y de sistemas de alertas sobrepasa considerablemente la cantidad de administradores con la experiencia y los antecedentes necesarios para garantizar que los entornos estén protegidos. Mantenerse actualizado respecto de los ataques más recientes es un desafío constante, lo que no permiten quedarse donde mismo mientras el mundo de la seguridad es un frente en continuo cambio.

Para ayudarlo a protegerse contra estos desafíos, Security Center le brinda las herramientas para que haga lo siguiente:

- **Reforzamiento de la posición de seguridad**: Security Center evalúa el entorno y le permite entender el estado de los recursos y si son seguros.

- **Protección frente a amenazas**: Security Center evalúa las cargas de trabajo y genera alertas de seguridad y recomendaciones para la prevención de amenazas.

- **Protección con mayor rapidez**: En Security Center, todo se hace a la velocidad de la nube. Al integrarse de manera nativa, la implementación de Security Center es sencilla y le proporciona aprovisionamiento automático y protección con los servicios de Azure.

Architecture

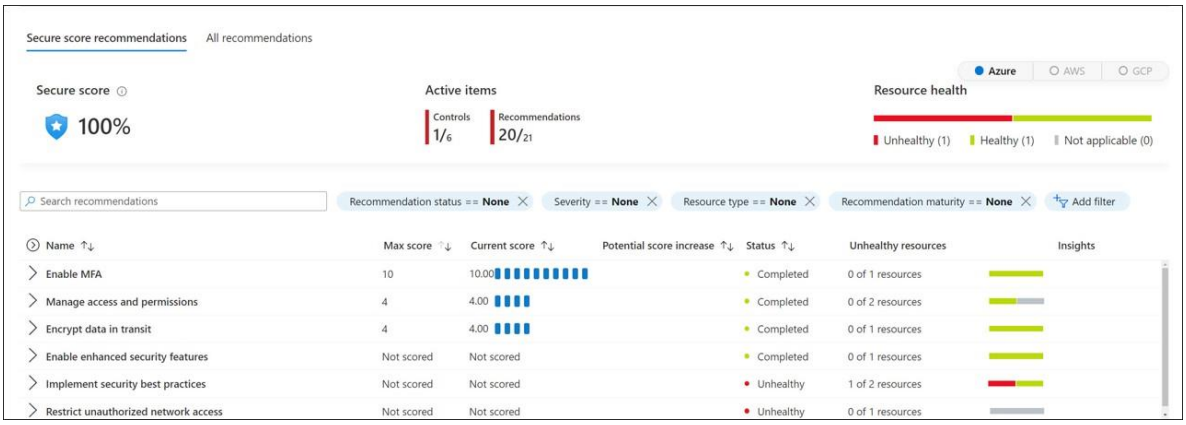
Como Security Center forma parte nativa de Azure, los servicios de PaaS en Azure (como Service Fabric, bases de datos SQL y cuentas de almacenamiento) los supervisa y protege Security Center sin necesidad de realizar ninguna implementación.

Además, Security Center protege las máquinas virtuales y los servidores (Windows y Linux) que no son de Azure, tanto en la nube como en el entorno local, instalando en ellos el agente de Log Analytics. Las máquinas virtuales de Azure se aprovisionan automáticamente en Security Center.

Los eventos recopilado de los agentes y de Azure se correlacionan en el motor de análisis de seguridad para brindarle recomendaciones a medida (tareas de protección) que debe seguir para garantizar que las cargas de trabajo sean seguras, y alertas de seguridad. Debe investigar estas alertas tan pronto como sea posible para asegurarse de que no haya ataques malintencionados en sus cargas de trabajo.

Al habilitar Security Center, la directiva de seguridad que tiene integrada se refleja en Azure Policy como una iniciativa integrada en la categoría Security Center. La iniciativa integrada se asigna automáticamente a todas las suscripciones registradas de Security Center (niveles Gratis o Estándar). La iniciativa integrada contiene solo las directivas de auditoría.

Security Center facilita la mitigación de las alertas de seguridad al agregar una Puntuación de seguridad. Las puntuaciones de seguridad ahora están asociadas con cada recomendación que recibe para ayudarle a comprender la importancia que cada una de ellas tiene para la posición de seguridad general. Esto resulta esencial para permitirle clasificar por orden de prioridad el trabajo de seguridad.



Recomendaciones de Microsoft Defender for Cloud

El valor básico de Microsoft Defender para la nube reside en sus recomendaciones. Las recomendaciones se adaptan a las preocupaciones de seguridad concretas que se encuentran en las cargas de trabajo, y Security Center se ocupa de administrar la seguridad por usted, no solo detectando vulnerabilidades, sino también proporcionándole instrucciones específicas para eliminarlas. De este modo, Security Center le permite no solo establecer las directivas de seguridad, sino también aplicar los estándares de seguridad en todos los recursos.

Las recomendaciones lo ayudan a disminuir la superficie expuesta a ataques en cada uno de los recursos. Aquí se incluyen las máquinas virtuales de Azure, los servidores que no son de Azure y los servicios de PaaS de Azure, como cuentas de SQL y Storage, etc., donde cada tipo de recurso se evalúa de manera distinta y tiene sus propios estándares.

Examen de imágenes de contenedor en Azure Container Registry para detectar vulnerabilidades

Microsoft Defender para la nube puede examinar las imágenes de contenedor en Azure Container Registry (ACR) en busca de vulnerabilidades.

El examen de imágenes funciona analizando los paquetes u otras dependencias definidas en el archivo de imagen de contenedor y, a continuación, comprobando si hay vulnerabilidades conocidas en esos paquetes o dependencias (con tecnología de una base de datos de evaluación de vulnerabilidades de Qualys).

El examen se desencadena automáticamente al insertar nuevas imágenes de contenedor en Azure Container Registry. Las vulnerabilidades encontradas se mostrarán como recomendaciones de Security Center y se incluirán en la Puntuación de seguridad junto con información sobre cómo aplicar revisiones para reducir la superficie de ataque que permitían. ASC muestra el estado del examen para reflejar el progreso del examen (**Sin analizar, Examen en curso, Error de examen y Completado**).

Protección de PaaS

Security Center lo ayuda a detectar amenazas en los servicios de PaaS de Azure. Puede detectar amenazas dirigidas a servicios de Azure como Azure App Service, Azure SQL, cuenta de Azure Storage y otros servicios de datos. También puede aprovechar la integración nativa con el análisis de comportamiento de usuarios y entidades (UEBA) de Microsoft Cloud App Security para realizar la detección de anomalías en los registros de actividad de Azure.

Licencias

- **El plan de tarifa gratuita de Security Center** se habilitará en todas las suscripciones a Azure vigentes una vez que visite el panel de Microsoft Defender para la nube en Azure Portal; también puede habilitarlo mediante programación a través de una API.
- **Nivel estándar**: para aprovechar las funcionalidades avanzadas de administración de seguridad y detección de amenazas, debe actualizar al plan de tarifa estándar. Dicho plan se puede probar de forma gratuita durante 30 días.