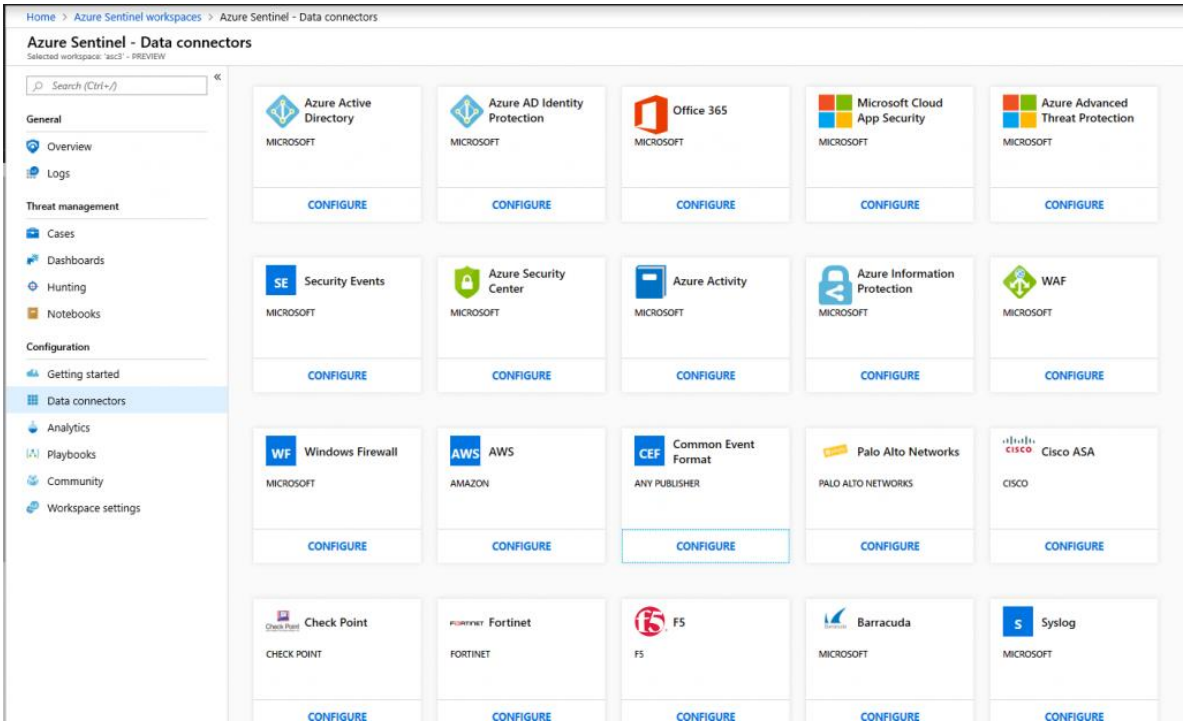
Configuración de conexiones de datos a Sentinel

Para incorporar Microsoft Sentinel, primero debe conectarse a sus orígenes de seguridad. Microsoft Sentinel incluye varios conectores para soluciones de Microsoft, que están disponibles inmediatamente y proporcionan integración en tiempo real, entre las que se incluyen las soluciones de Protección contra amenazas de Microsoft y orígenes de Microsoft 365, incluido Microsoft 365, Azure AD, Azure ATP y Microsoft Cloud App Security, entre otros. Además, hay conectores integrados al amplio ecosistema de seguridad para soluciones que no son de Microsoft. También puede usar el formato de evento común, Syslog o las API de REST para conectar los orígenes de datos con Microsoft Azure Sentinel.



Métodos de conexión de datos

Microsoft Sentinel admite los siguientes métodos de conexión de datos:

- **Integración de servicio a servicio**: algunos servicios se conectan de forma nativa, como AWS y los servicios Microsoft. Estos servicios aprovechan Azure Foundation para una integración de serie. Con tan solo unos clics, se pueden conectar las soluciones siguientes:
- Amazon Web Services: CloudTrail
- Actividad de Azure
- Inicios de sesión y pistas de auditoría de Azure AD
- Azure AD Identity Protection
- Azure Advanced Threat Protection
- Azure Information Protection

Configuración de conexiones de datos a Sentinel

- Microsoft Defender for Cloud
- Cloud App Security
- Servidor de nombres de dominio
- Microsoft 365
- ATP de Microsoft Defender
- Firewall de aplicaciones web de Microsoft
- Firewall de Windows
- Eventos de seguridad de Windows

Soluciones externas mediante una API

algunos orígenes de datos se conectan mediante las API proporcionadas por el origen de datos conectado. Normalmente, la mayoría de las tecnologías de seguridad proporcionan un conjunto de API a través de las cuales se pueden recuperar registros de eventos. Las API se conectan a Microsoft Sentinel, recopilan tipos de datos específicos y los envían a Azure Log Analytics

Soluciones externas mediante un agente

Microsoft Sentinel se puede conectar mediante un agente a cualquier otro origen de datos que pueda realizar streaming de registro en tiempo real mediante el protocolo de Syslog. El agente de Microsoft Sentinel, que se basa en el agente de Log Analytics, convierte los registros con formato CEF a un formato que Log Analytics puede ingerir. Dependiendo del tipo de dispositivo, el agente se instala directamente en el dispositivo o en un servidor Linux dedicado.

Opciones de conexión del agente

Para conectar su dispositivo externo a Microsoft Sentinel, el agente debe implementarse en una máquina dedicada (máquina virtual o local) para admitir la comunicación entre el dispositivo y Microsoft Sentinel. Puede implementar el agente automáticamente o de forma manual. La implementación automática solo está disponible si su máquina dedicada es una nueva máquina virtual que crea en Azure.

Configuración de conexiones de datos a Sentinel

Requisitos previos globales

Activación de una suscripción de Azure

Área de trabajo de Log Analytics.

Para habilitar Microsoft Sentinel, necesita permisos de colaborador en la suscripción en la que reside el área de trabajo de Microsoft Sentinel.

Para usar Microsoft Sentinel, necesita permisos de colaborador o lector en el grupo de recursos al que pertenece el área de trabajo.

Es posible que se necesiten permisos adicionales para conectarse a orígenes de datos específicos.

Microsoft Sentinel es un servicio de pago.