MICROSOFT ZERO TRUST

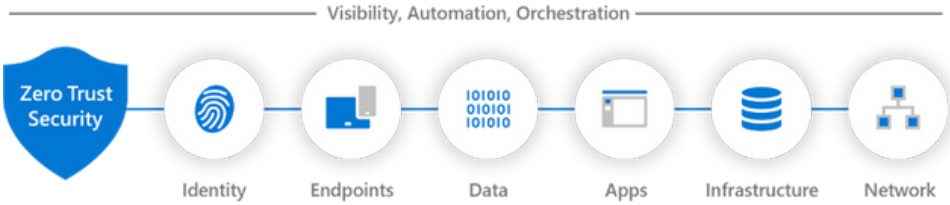
Microsoft

## Servicios Administrados Microsoft

Contamos con diferentes modelos de servicios: consultoría, implementación por proyecto o soporte administrado con especialistas certificados en Microsoft. Trabaje con un administrador de cuentas técnico para evaluar, revisar, definir, planificar y entregar su entorno tecnológico de Microsoft deseado, todo alineado a sus objetivos.

Aprovecha las ventajas de tu licenciamiento con una estrategia de seguridad en la nube, a fin de garantizar la mayor protección de información.

## Adopción seguridad Zero Trust




## Microsoft Defender

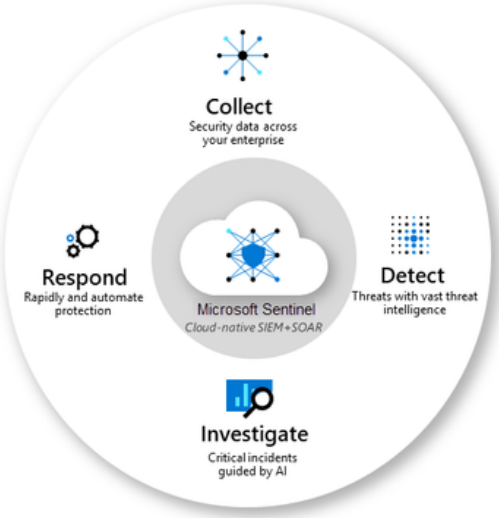
Microsoft Defender es una suite de seguridad unificada que protege contra ransomware, malware y otras ciberamenazas en diversos dispositivos y entornos. Incluye varios componentes especializados:

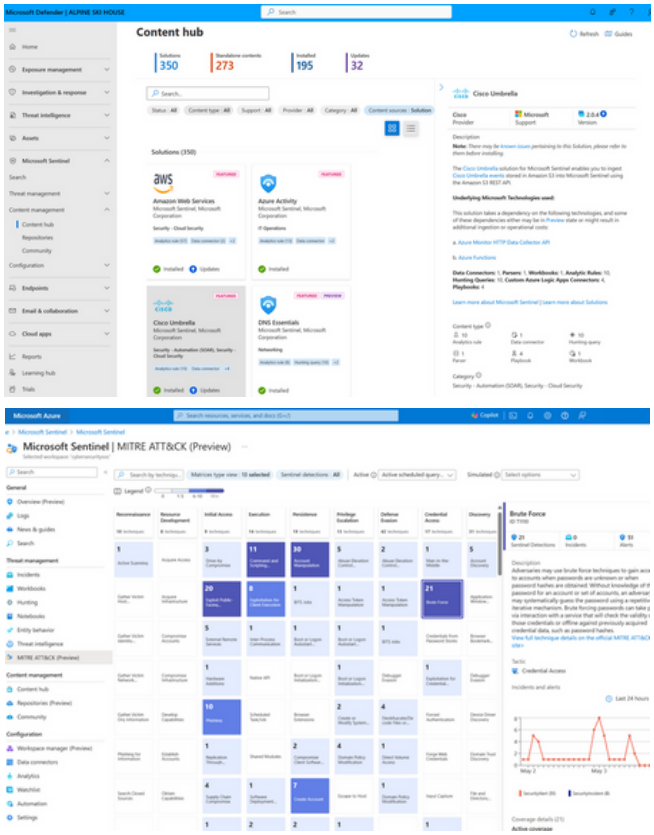
- **Microsoft Defender XDR:** Detección y respuesta extendidas (XDR) que interrumpe automáticamente los ataques más sofisticados.
- **Microsoft Defender para Empresas:** Solución de seguridad de nivel empresarial para pequeñas y medianas empresas (hasta 300 empleados), rentable y fácil de usar.
- **Microsoft Defender para punto de conexión:** Protección completa contra amenazas para dispositivos finales, como PC, Mac y móviles.
- **Microsoft Defender para Office 365**: Protege el correo electrónico, los documentos y otros datos en la suite de Microsoft 365.
- **Microsoft Defender for Cloud:** Protección de la carga de trabajo en la nube (CWPP), gestión de la postura de seguridad (CSPM) y seguridad para aplicaciones nativas (CNAPP) en entornos híbridos y multinube.
- **Microsoft Defender for Identity:** Protección basada en inteligencia contra amenazas avanzadas y actividades maliciosas que afectan las identidades.
- **Microsoft Defender for Cloud Apps:** Un agente de seguridad de acceso a la nube (CASB) que protege las aplicaciones SaaS.


## Microsoft Sentinel

Microsoft Sentinel es una solución de seguridad en la nube, nativa de Azure, que unifica la administración de eventos e información de seguridad (SIEM) y la orquestación, automatización y respuesta de seguridad (SOAR) para detectar, investigar y responder a amenazas de ciberseguridad.

- **SIEM en la nube:** Solución de gestión de eventos e información de seguridad (SIEM) nativa de la nube, impulsada por inteligencia artificial (IA), que permite supervisar y analizar datos de seguridad en toda la empresa.
- **Detección de amenazas:** Utiliza IA para identificar amenazas potenciales y actividades sospechosas en entornos complejos.




## ¿Cómo funciona?

- **Recopilación de Datos:** Se conectan diversas fuentes de datos, como usuarios, dispositivos, aplicaciones e infraestructura, tanto en la nube como en entornos locales.
- **Análisis con IA:** La inteligencia artificial y los análisis de seguridad se aplican a los datos para detectar patrones y anomalías.
- **Detección y Respuesta:** Se generan alertas sobre posibles amenazas, y se pueden activar playbooks (cuadernos de estrategias) para automatizar las acciones de respuesta.

## Beneficios

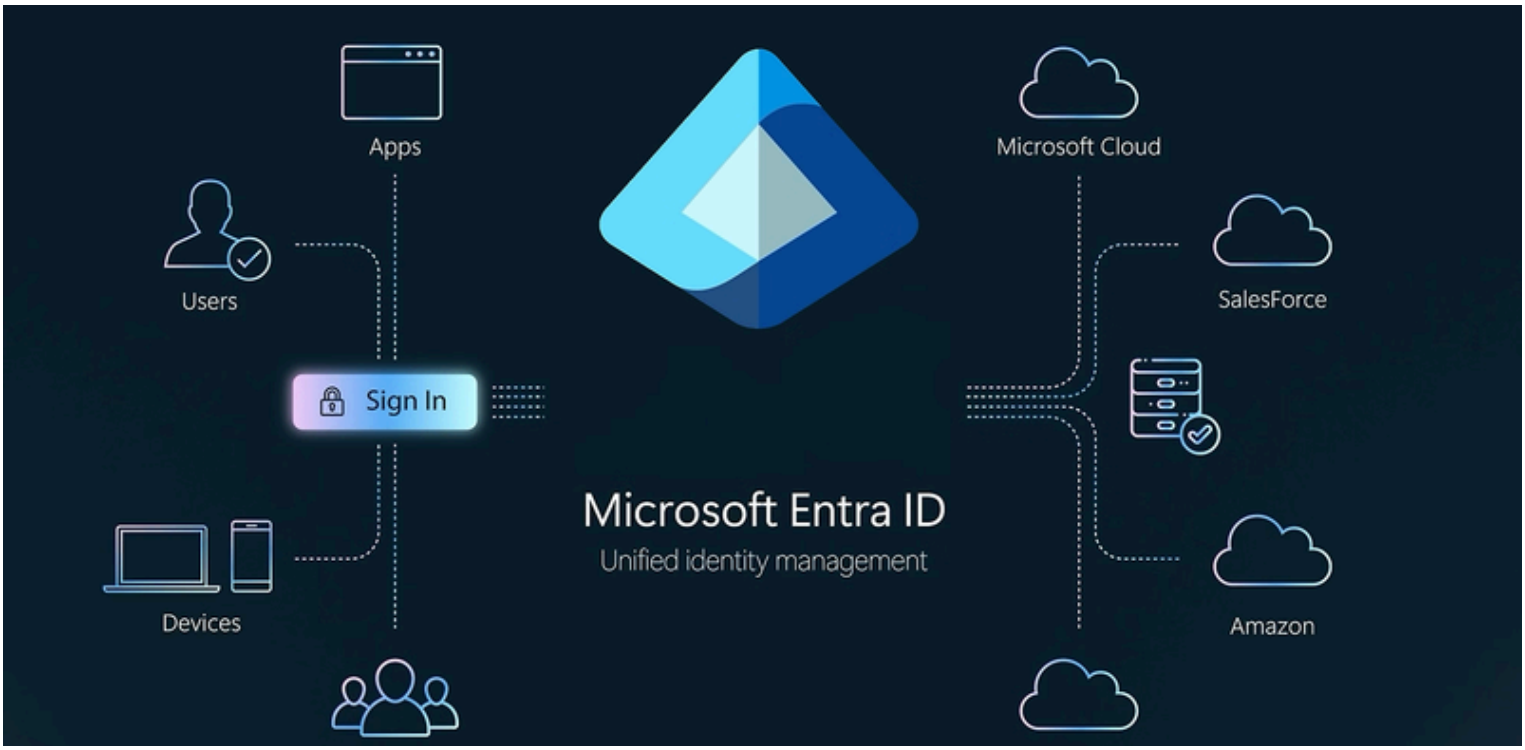
**Seguridad Nativa de la Nube:** Se integra perfectamente en el entorno de Azure, proporcionando una solución escalable y rentable.
**Análisis Inteligente:** Aprovecha la inteligencia de amenazas y la IA para ofrecer análisis de seguridad más profundos.
**Protección de Múltiples Entornos:** Ofrece seguridad unificada para infraestructuras híbridas y multinube


## Microsoft Entra

Anteriormente Azure Active Directory

Microsoft Entra es un servicio de seguridad que administra y protege el acceso a aplicaciones y datos para las organizaciones. Esta familia de productos ayuda a las empresas a implementar la identidad y el acceso en entornos de nube y locales, estableciendo un modelo de Zero Trust y asegurando el acceso para empleados, clientes y cargas de trabajo de IA.

- **Microsoft Entra ID:** Administra y protege identidades para garantizar que los usuarios adecuados tengan acceso a las aplicaciones y servicios correctos.
- **Microsoft Entra ID Protection:** Detecta vulnerabilidades y riesgos en la identidad del usuario para prevenir ataques.
- **Microsoft Entra ID Governance:** Garantiza automáticamente que las personas apropiadas tengan el acceso adecuado a las aplicaciones y los servicios necesarios en el momento preciso.




## Funciones principales

- **Protección de identidades:** Ayuda a proteger las identidades de empleados y clientes.
- **Acceso a la red:** Permite el acceso seguro a cualquier aplicación, ya sea en la nube o local.
- **Gobernanza de identidades:** Administra los ciclos de vida de las identidades.
- **Verificación de identidades:** Permite la emisión de credenciales verificables.

**Ejemplo práctico:** Si una empresa necesita gestionar el acceso a sus aplicaciones internas y a servicios en la nube de forma segura, puede utilizar Microsoft Entra para implementar políticas que aseguren que solo los usuarios autorizados puedan acceder a la información, independientemente de dónde estén conectados

## Microsoft Purview

Microsoft Purview es una solución de gobernanza, seguridad y cumplimiento de datos que ayuda a las organizaciones a controlar, proteger y administrar toda su información confidencial en entornos multinube y locales. Proporciona visibilidad integral de los datos y permite clasificarlos inteligentemente, aplicar etiquetas de confidencialidad y cifrado, y establecer políticas para prevenir la pérdida y el uso indebido de datos sensibles.

### Funcionalidades clave de Microsoft Purview

**Gobernanza de datos unificada:**
Permite descubrir, entender y administrar el patrimonio de datos de una organización en un portal unificado.

**Protección de la información**

- **Clasificación inteligente:** Utiliza IA para identificar y clasificar información confidencial en archivos, correos electrónicos y otros datos.
- **Etiquetado de confidencialidad:** Permite aplicar etiquetas con diferentes niveles de seguridad, que pueden restringir el acceso mediante cifrado y agregar marcas de agua a los documentos.
- **Prevención de pérdida de datos (DLP)**: Ayuda a evitar el uso, el intercambio y la transferencia no autorizados de datos confidenciales.

**Administración de riesgos:**
Ofrece herramientas para gestionar riesgos internos y controlar el acceso a los datos.

**Cumplimiento normativo:**
Facilita el cumplimiento de regulaciones de privacidad como el RGPD, gracias a la aplicación de políticas de seguridad.

**Compatibilidad con IA**: Permite bloquear el acceso a aplicaciones de IA no deseadas y controlar la visibilidad y el uso de datos en la era de la inteligencia artificial.

Microsoft Purview es una plataforma integral para la gestión segura y conforme de los datos, diseñada para la complejidad de los entornos modernos.

Microsoft

## Microsoft Security Copilot

Microsoft Security Copilot es una solución de seguridad impulsada por inteligencia artificial generativa que potencia a los profesionales de seguridad y TI para detectar, investigar y responder a ciberamenazas a gran escala.

Utiliza el lenguaje natural para interactuar con las herramientas de seguridad de Microsoft y terceros, ayudando en tareas como la búsqueda de amenazas, la gestión de incidentes y la recopilación de inteligencia de amenazas para mejorar la eficacia y la velocidad de los equipos de seguridad.

Al usar complementos como orígenes de punto de datos, los profesionales de seguridad tienen una visibilidad más amplia de las amenazas y obtienen más contexto.



Security Copilot se centra en facilitar la realización de los siguientes casos de uso: Investigación y corrección de amenazas de seguridad, Creación de consultas de KQL o análisis de scripts sospechosos, Descripción de los riesgos y administración de la posición de seguridad de la organización, Solución de problemas de TI más rápido, Definir y administrar directivas de seguridad, Configuración de flujos de trabajo de ciclo de vida seguro, Desarrollar informes para las partes interesadas, Compilar y agregar agentes

**Security Copilot procesa y organiza iterativamente estos servicios sofisticados para ayudar a generar resultados relevantes para su organización, ya que se basan contextualmente en los datos de la organización.**

## Servicios de Nuvol para Zero Trust con tecnología Microsoft

Nuestros servicios administrados le brindan la tranquilidad de que su seguridad está en manos de profesionistas certificados en Seguridad Microsoft. Ofrecemos:

**Evaluación y planificación**

Analizamos su postura de seguridad actual y diseñamos una estrategia Zero Trust personalizada y gradual, adaptada a sus necesidades y licenciamiento de Microsoft.

**Implementación y configuración:**

Desplegamos y optimizamos las soluciones de ciberseguridad de Microsoft, como Microsoft Defender, Microsoft Entra ID y Microsoft Purview.

## Nuvol + Microsoft
## Su camino hacia Zero Trust

Como socio de servicios administrados de Microsoft, Nuvol aprovecha la tecnología líder del mercado para crear una defensa integral para su negocio.

En Nuvol, nuestro mayor activo es nuestro equipo de especialistas altamente certificados, líderes en el soporte de nivel 3 para tecnologías de Microsoft. No solo conocemos la teoría de Zero Trust; la aplicamos con la experiencia de quien domina la suite de ciberseguridad más completa del mercado. Esta profunda experticia en Microsoft nos permite diseñar, implementar y gestionar una estrategia Zero Trust robusta y eficiente, maximizando el potencial de sus licencias y garantizando una protección inigualable para su organización.

**Capacitación y concienciación**

Formamos a su equipo de TI y a sus usuarios finales para que comprendan y adopten las mejores prácticas de Zero Trust, fortaleciendo la cultura de seguridad de su organización.