El gestor de contraseñas autoalojado de Bitwarden

Gestione de forma segura las credenciales empresariales y las políticas de seguridad personalizadas en su propio servidor mediante el autoalojamiento del gestor de contraseñas Bitwarden.

Obtén la vista interactiva completa en https://bitwarden.com/es-la/self-hosted-password-manager-on-premises/

bitwarden

Aplique su propio modelo de seguridad

Coloque su instalación de Bitwarden detrás de un proxy, cortafuegos y otras protecciones para una mayor seguridad de los datos.

Controle las copias de seguridad y la disponibilidad

Las soluciones basadas en contenedores de Docker o Kubernetes se adaptan a su estrategia existente de alta disponibilidad y recuperación, y dentro de sus procedimientos establecidos.

Personalícelo para adaptarlo a sus necesidades

Cumpla sus requisitos específicos de conformidad y sus políticas internas de residencia de datos con variables de entorno flexibles para necesidades cambiantes.

El gestor de contraseñas de confianza para casa, el trabajo y los desplazamientos

Accesibilidad multiplataforma y dispositivos ilimitados

Acceda a datos críticos en su caja fuerte desde cualquier ubicación, navegador y a través de dispositivos ilimitados

Integre Bitwarden sin problemas

Conecte Bitwarden sin problemas a su pila tecnológica existente con opciones de integración flexibles como proveedores de identidad de inicio de sesión único (SSO) y servicios de directorio, incluido SCIM.

Auditoría de seguridad y cumplimiento

De código abierto, auditado por terceros y cumple con las regulaciones de GDPR, Privacy Shield, HIPAA y CCPA

Sincronización de directorio

Utilice el soporte SCIM o el Conector de Directorio para agilizar la provisión de usuarios y grupos y mantener la sincronización con su servicio de directorio.

Informes de salud de la caja fuerte

Acceda a informes perspicaces para revelar contraseñas débiles, reutilizadas y otras métricas de seguridad útiles.

Soporte siempre activo

Los agentes de Éxito del Cliente están disponibles para apoyarte las 24 horas del día.

Ventajas de los gestores de contraseñas autoalojados

Auténtica soberanía de los datos

Tanto si las preocupaciones provienen de la junta directiva como de sus clientes, con el autoalojamiento, la verdadera soberanía de los datos es una realidad.

Cumplimiento de la normativa

Si su industria, servicio o producto tiene estrictos requisitos de cumplimiento de datos, el autoalojamiento de Bitwarden Password Manager marca una gran casilla de cumplimiento.

Seguridad personalizable

Ajuste la configuración de seguridad según sus necesidades. Adapte todos los aspectos de la seguridad de su organización, desde las variables de entorno de autoalojamiento hasta las políticas internas del producto.

Integración perfecta

Las instalaciones compatibles para Windows, Linux, Docker o Kubernetes se integran con su infraestructura de TI existente. El servidor Bitwarden autoalojado es compatible con todos los clientes finales, incluidas las aplicaciones móviles y de escritorio y las extensiones de navegador. Integración en el producto con su proveedor de identidades, servicios de directorio, etc.

Preparado para auditorías y cumplimiento

Las herramientas SIEM pueden ingerir registros de eventos exhaustivos a través de integraciones o API para realizar un seguimiento de la actividad de los usuarios y garantizar el cumplimiento de sus políticas internas y normativas externas. Los resultados de las auditorías de terceros, los informes SOC 2 y otra información sobre el cumplimiento de la aplicación se publican y actualizan anualmente.

Obtenga una seguridad líder en el sector y un control total de sus datos

Haga que su experiencia en línea sea más segura, más rápida y más agradable mediante el autoalojamiento de Bitwarden Password Manager.

Preguntas frecuentes

Más preguntas frecuentes sobre autoalojamiento aquí

- ¿Cuáles son las ventajas de utilizar un gestor de contraseñas autoalojado?
  1. **Auténtica soberanía de datos**: El autoalojamiento de un gestor de contraseñas te ofrece un control total sobre tus datos. Usted gestiona su propio servidor, asegurándose de que las contraseñas y credenciales confidenciales se almacenan en la infraestructura que usted controla.
  2. **Mayor seguridad**: Con una solución autoalojada, puedes aplicar tu propio modelo de seguridad. Coloque su instalación de gestión de contraseñas detrás de proxies y cortafuegos para una mayor protección.
  3. **Personalización**: Los gestores de contraseñas autoalojados suelen ofrecer variables de entorno flexibles, lo que te permite personalizar la configuración para adaptarla a tus necesidades específicas y a los requisitos de cumplimiento.
  4. **Ventajas del código abierto**: La confianza y la transparencia son esenciales a la hora de elegir qué gestor de contraseñas autoalojar. Dado que Bitwarden es un gestor de contraseñas de código abierto, las medidas de seguridad son autoverificables, y cada línea de código es inspeccionada regularmente por miles de expertos y entusiastas de la seguridad de todo el mundo.
  5. **Cumplimiento normativo**: El autoalojamiento puede ayudar a cumplir con los estrictos requisitos de cumplimiento de datos en varias industrias, ya que tienes control total sobre la residencia y el acceso a los datos.
  6. **Integración con los sistemas existentes**: Las soluciones autoalojadas suelen permitir una integración perfecta con su infraestructura informática actual, incluidos los servicios de directorio y los proveedores de identidad.
  7. **Preparación para auditorías**: Obtenga acceso a registros de eventos detallados para el seguimiento de la actividad de los usuarios, lo que puede ser crucial para las auditorías internas y el mantenimiento del cumplimiento.

- ¿En qué plataformas puedo alojar?

  Los clientes de Bitwarden son multiplataforma, y el servidor puede desplegarse en contenedores Docker en Windows, Linux o en Kubernetes con el uso de una carta Helm.

  Docker Desktop en Windows puede requerir una licencia dependiendo de si su empresa cumple con los requisitos de Docker para las licencias, sin embargo Docker en Linux es gratuito.

  Puede obtener más información sobre Docker y las tecnologías de contenedores en el sitio web de Docker.

- ¿Cómo despliego Bitwarden en AWS, Azure, GCP o VMware vCenter?

  Bitwarden tiene guías detalladas para desplegar instalaciones Docker en la documentación de ayuda. También están disponibles las instrucciones para la instalación en AWS EKS, OpenShift y Azure AKS utilizando Helm. A continuación encontrará recursos recomendados que le ayudarán a empezar:

  - Guías de implantación de Docker
  - Guías de implantación de Helm
  - Cómo autoalojar una organización Bitwarden

- ¿Cómo configuro un gestor de contraseñas de código abierto en mi propio servidor?

  Configurar un gestor de contraseñas de código abierto en su propio servidor suele implicar estos pasos

  1. **Prepare su servidor**: Asegúrate de que tienes un servidor o una máquina virtual preparados. Puede tratarse de hardware local o de un servidor basado en la nube.
  2. **Seleccione el método de instalación**: Muchos gestores de contraseñas autoalojados ofrecen varias opciones de instalación. Las más comunes son:
     - Contenedores Docker
     - Despliegue de Kubernetes
  3. **Instalación**: Explore la documentación detallada de autoalojamiento de Bitwarden para varios tipos de despliegue.
  4. **Configuración**: Establezca variables de entorno y ajuste la configuración para que se adapte a sus requisitos de seguridad y necesidades organizativas.
  5. **Gestión de usuarios**: Establezca cuentas de administrador y configure los derechos de acceso de los usuarios.
  6. **Configuración de clientes**: Instala extensiones de navegador, aplicaciones de escritorio y aplicaciones móviles para tus usuarios, asegurándote de que están configuradas para conectarse a tu servidor autoalojado.
  7. **Pruebas**: Pruebe a fondo la instalación, incluidas funciones como el generador de contraseñas, el uso compartido seguro y la autenticación multifactor.
  8. **Plan de mantenimiento**: Establece procedimientos para realizar copias de seguridad, actualizaciones y auditorías de seguridad periódicas para mantener tu gestor de contraseñas autoalojado seguro y actualizado.

  Recuerde que, aunque el autoalojamiento ofrece muchas ventajas, también requiere un mantenimiento continuo y vigilancia de la seguridad. Asegúrese de que dispone de los recursos y la experiencia necesarios para gestionar eficazmente una solución autoalojada.