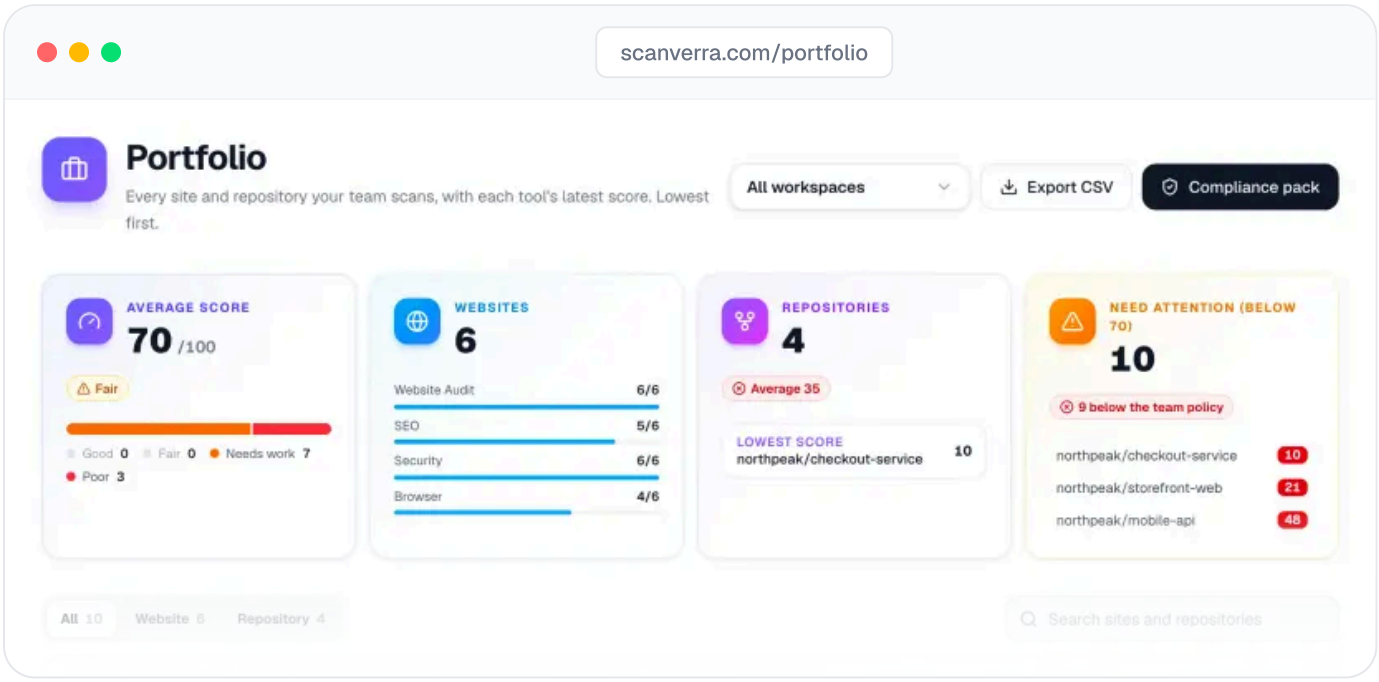
SCANVERRA
Detect • Analyze • Protect

SCANVERRA ENTERPRISE

Resumen de Scanverra Enterprise

Portafolio, cumplimiento, remediación y controles de acceso para todos tus sitios y repositorios.



6	7	12 meses	100
herramientas en un portafolio	marcos de cumplimiento mapeados	de registro de auditoría	páginas por rastreo del sitio

- ✓ SAML SSO y SCIM
- ✓ OWASP, PCI DSS, WCAG, SOC 2, RGPD
- ✓ Registro de auditoría de 12 meses
- ✓ Slack, Teams y webhooks

CONTENIDO

01 Verlo todo
02 Demostrar cumplimiento
03 Corregir antes
04 Controlar el acceso
05 Vigilar los cambios

Las pantallas de esta página muestran una empresa de demostración con datos inventados.

01 · VERLO TODO

Todos tus sitios y repositorios a la vez

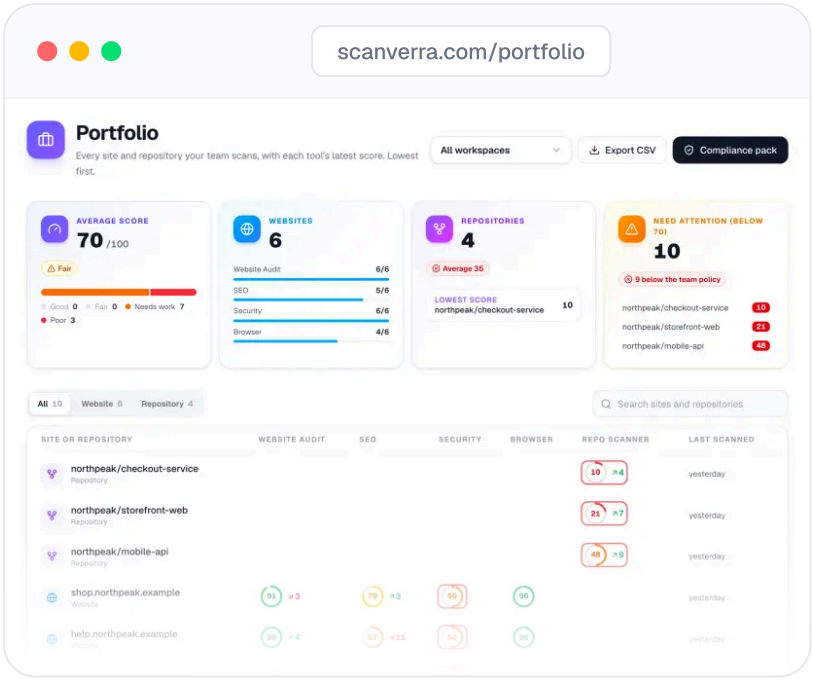
Una vista de todo lo que gestionan tus equipos y un resumen semanal para quien solo necesita lo esencial.

Team y Enterprise

Un portafolio de todos tus sitios y repositorios

Cada objetivo que escanea tu equipo, con la última puntuación de cada herramienta y el cambio desde el escaneo anterior, del peor al mejor. Fíltralo por espacio de trabajo, expórtalo o abre el informe detrás de cada cifra.

- Puntuaciones de Auditoría web, SEO, Seguridad, Auditoría de navegador y Analizador de repos lado a lado
- Un anillo rojo en todo lo que queda por debajo de la política de tu equipo
- Código y sitio en producción: dependencias vulnerables que de verdad están desplegadas
- IA en tu código: proveedores, modelos y servidores MCP en todos los repositorios

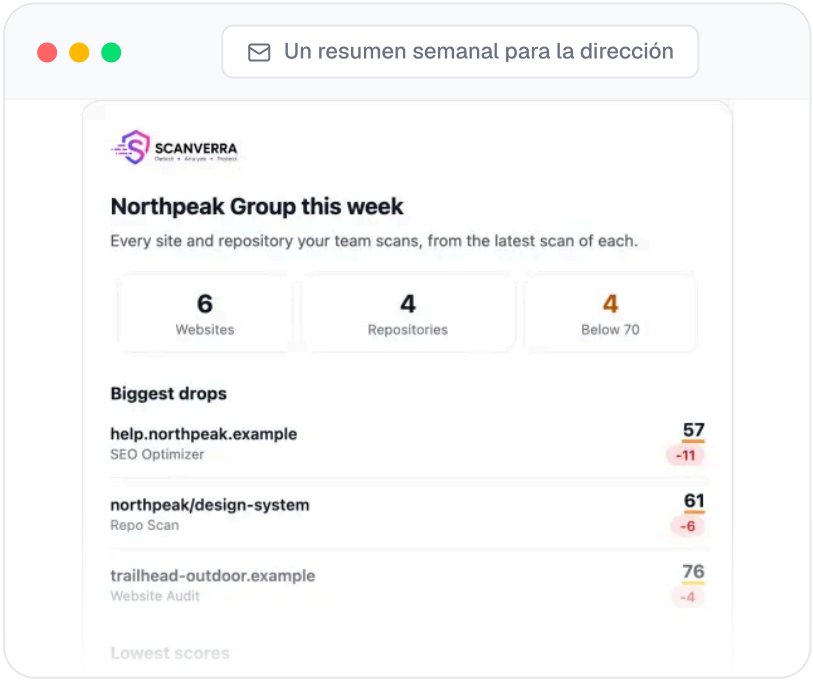


Enterprise

Un resumen semanal para la dirección

Cada lunes, los propietarios y administradores reciben un correo con las puntuaciones más bajas, las mayores caídas y los repositorios que usan IA sin una política. Cada persona puede darse de baja por su cuenta.

- Puntuaciones más bajas y mayores caídas de todo el portafolio
- Huecos de política de IA según los últimos escaneos de repositorios
- Un enlace de vuelta al portafolio para ver el detalle



02 · DEMOSTRAR CUMPLIMIENTO

Evidencias con las que tu auditor puede trabajar

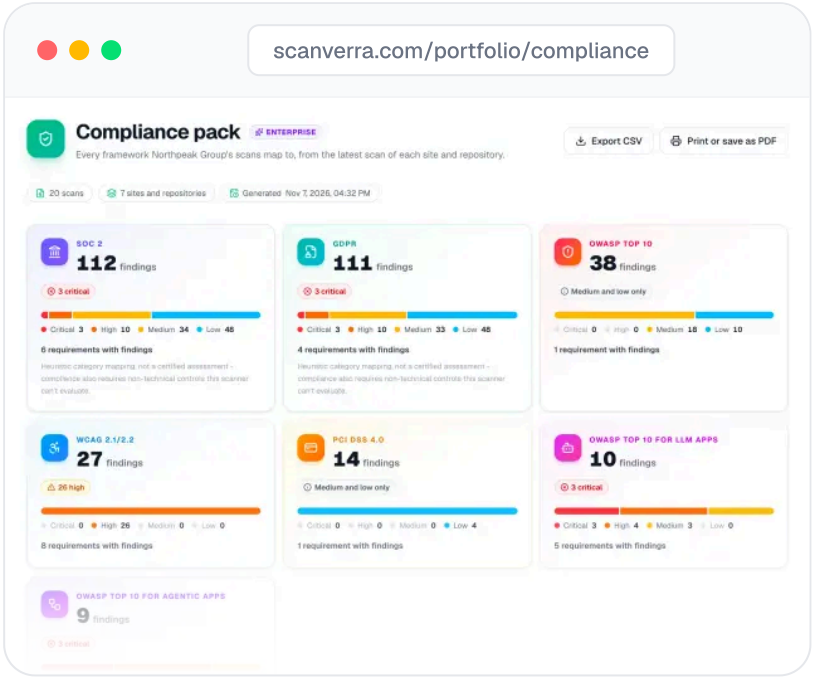
Resultados por marco a partir de tus escaneos reales y la monitorización del checkout que exige PCI DSS 4.0.

Enterprise

Un paquete de cumplimiento creado a partir de tus escaneos reales

OWASP Top 10, PCI DSS 4.0, WCAG 2.1 y 2.2, SOC 2, RGPD y las listas de OWASP para apps de LLM y agentes, requisito por requisito, con los sitios y repositorios afectados. Es una evidencia con la que trabajar, no una certificación.

- ✓ Cada requisito con sus hallazgos, su gravedad y los objetivos afectados
- ✓ Exporta a CSV o guárdalo como PDF para el expediente de auditoría
- ✓ Descargas de SBOM en CycloneDX 1.5 y SPDX 2.3
- ✓ Filtra por espacio de trabajo para dar a cada unidad de negocio su propio paquete

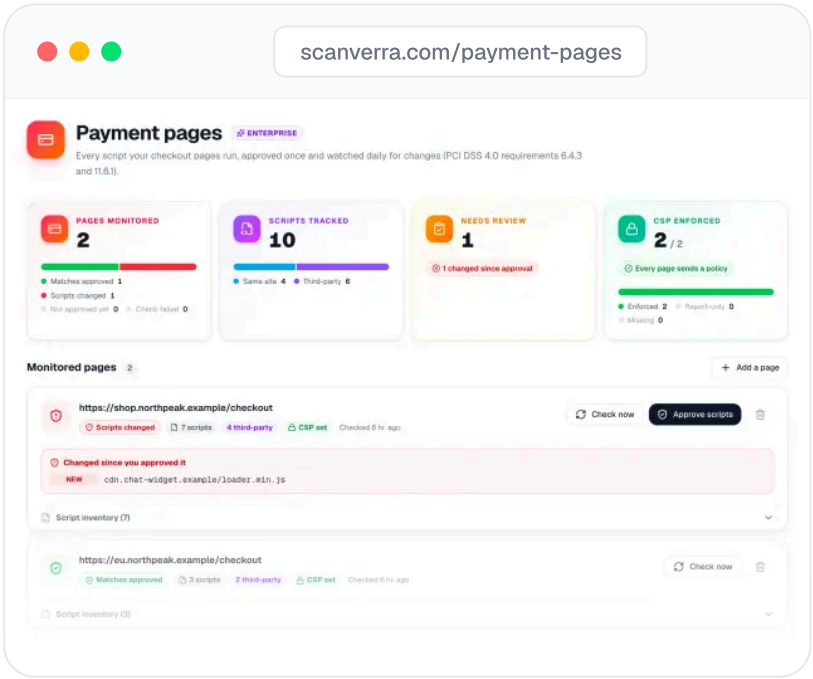


Enterprise

Monitorización de scripts PCI DSS 4.0 para páginas de pago

Cada script que ejecutan tus páginas de pago se registra en un navegador real, con su hash SHA-256 y tu Content-Security-Policy. Aprueba la lista una vez y cualquier script nuevo o modificado se señala al día siguiente.

- ✓ Pensado para los requisitos 6.4.3 y 11.6.1
- ✓ Scripts de terceros e inline, cada uno con su hash
- ✓ Páginas de pago tras un inicio de sesión, con un acceso guardado
- ✓ Alertas por correo, Slack, Microsoft Teams o tu webhook



03 · CORREGIR ANTES

Del hallazgo a la corrección, con un responsable

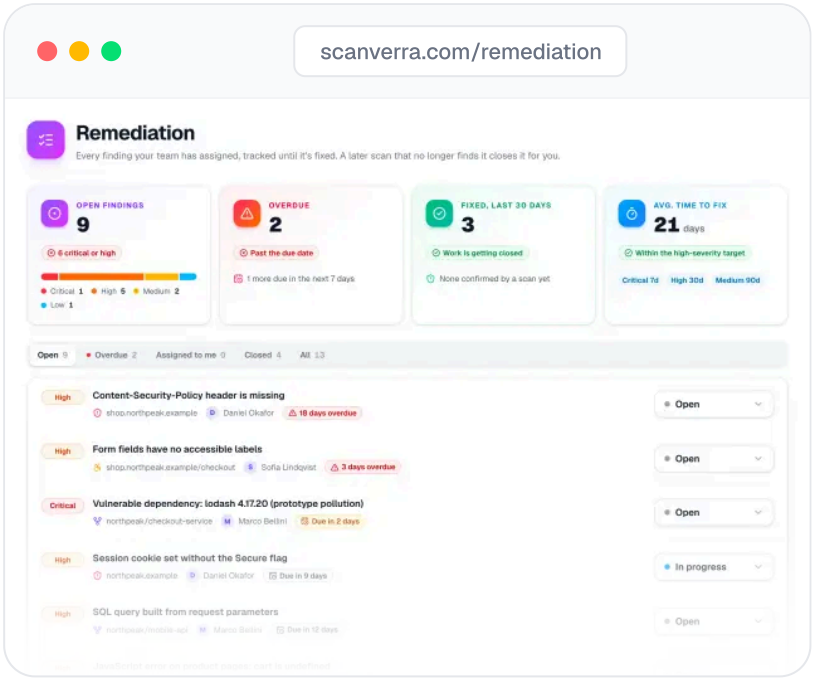
Cada hallazgo tiene una persona y un plazo, y una política decide qué es suficiente para publicar.

Team y Enterprise

Los hallazgos se convierten en tareas con responsables y plazos

Asigna cualquier hallazgo de cualquier herramienta a un compañero. El plazo depende de la gravedad, la persona asignada recibe un correo y un escaneo posterior que ya no encuentra el problema cierra la tarea por ti.

- Plazos por gravedad: crítico 7 días, alto 30, medio 90, bajo 180
- Abiertos, vencidos, corregidos y tiempo de corrección de un vistazo
- Cada tarea abre el hallazgo exacto en su informe
- Se cierra solo cuando un escaneo lo confirma, para las comprobaciones que ejecutó ese escaneo

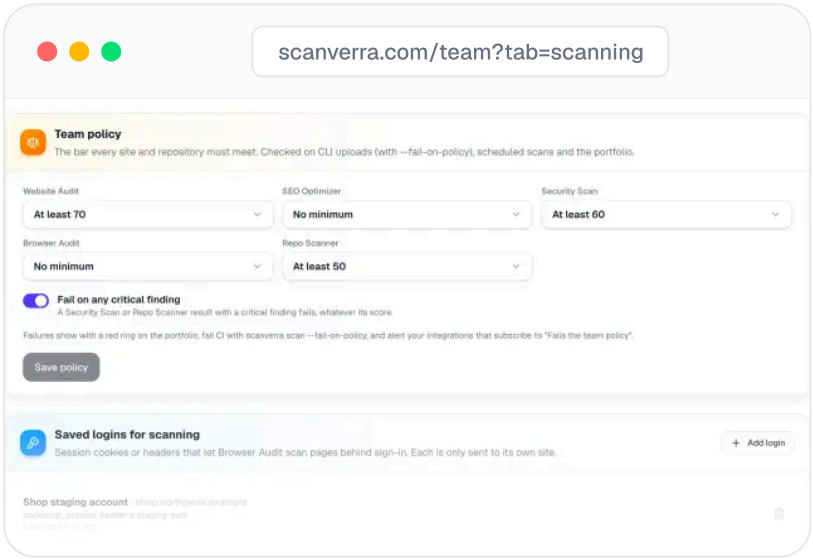


Enterprise

Un mismo listón para cada sitio y repositorio

Define la puntuación mínima de cada herramienta y suspende directamente ante cualquier hallazgo crítico. La misma política se comprueba en las subidas de la CLI en CI, en los escaneos programados y en el portafolio.

- Una puntuación mínima por herramienta
- Haz fallar la compilación con scanverra scan --fail-on-policy
- Una alerta cuando un escaneo programado no cumple la política
- Accesos guardados para que la Auditoría de navegador escanee páginas tras un inicio de sesión



04 · CONTROLAR EL ACCESO

Los controles que pide el área de compras

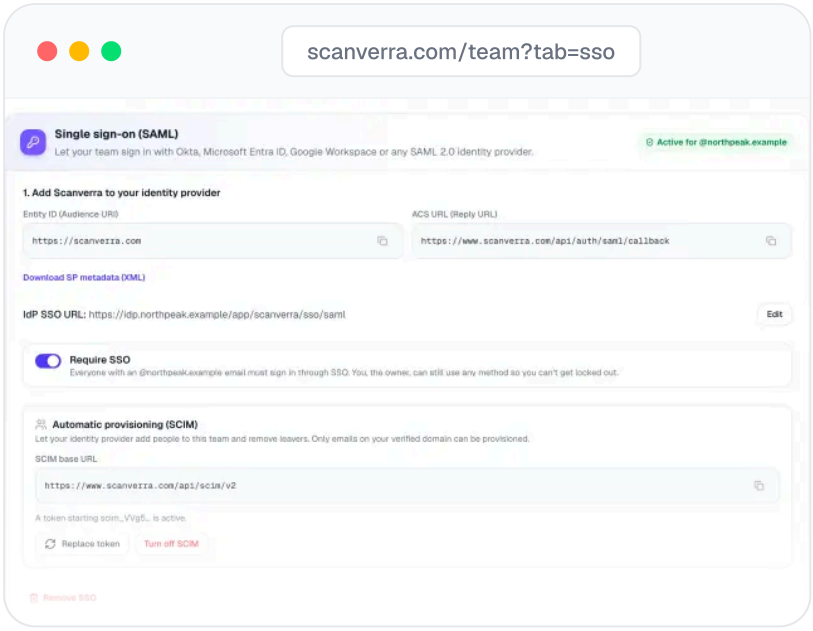
Inicio de sesión único, aprovisionamiento, roles, espacios de trabajo y un registro de quién hizo qué.

Enterprise

Inicio de sesión único y aprovisionamiento que configuras tú

Conecta Okta, Microsoft Entra ID, Google Workspace o cualquier proveedor de identidad SAML 2.0 desde la página del equipo. Demuestra que el dominio es tuyo con un registro DNS y exige SSO a todos los que lo usan.

- Exige SSO, con un acceso de respaldo para el propietario para que nunca te quedes fuera
- SCIM 2.0 añade y elimina miembros desde tu proveedor de identidad
- Solo se pueden aprovisionar correos de tu dominio verificado
- Cada respuesta SAML se acepta una sola vez y solo para su propio dominio

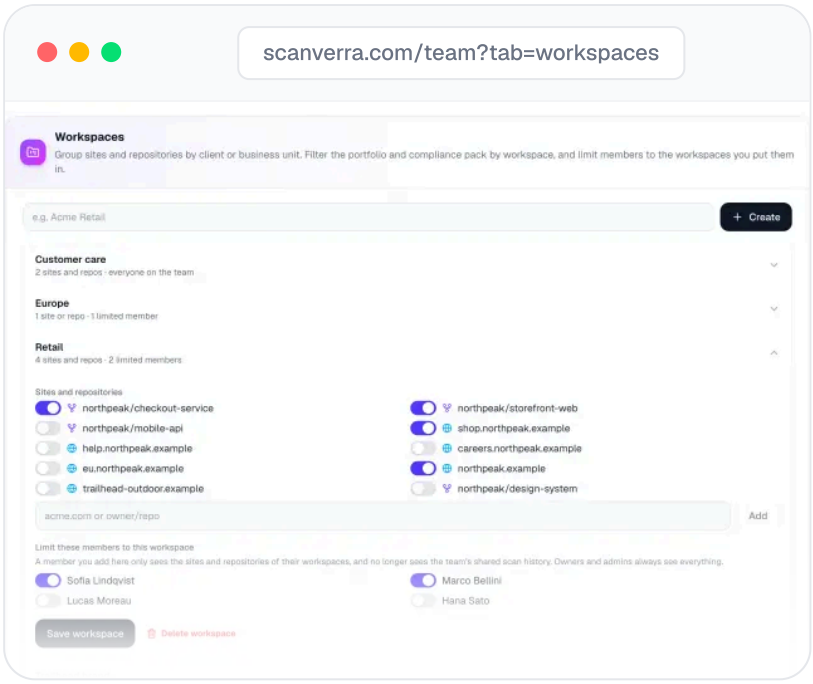


Enterprise

Espacios de trabajo y roles que encajan con tu organigrama

Agrupa sitios y repositorios por unidad de negocio, marca o cliente, y da acceso de Administrador, Miembro o Lector. Quien está limitado a un espacio de trabajo solo ve sus sitios y repositorios.

- Los espacios de trabajo filtran el portafolio, el paquete de cumplimiento y la exportación de datos
- Los lectores ven todos los informes, pero no pueden lanzar escaneos de pago ni cambiar ajustes
- Claves de API del equipo que siguen funcionando cuando su creador se va
- Claves de solo lectura y fechas de caducidad para pipelines y herramientas de BI

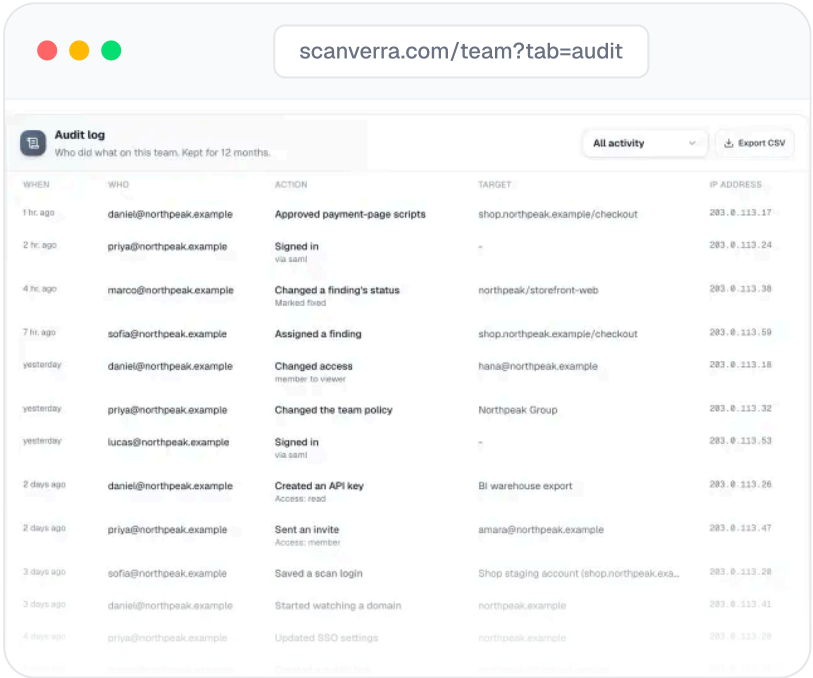


Enterprise

Un registro de auditoría de todo lo que importa

Inicios de sesión, invitaciones, cambios de acceso, claves de API, enlaces compartidos, escaneos eliminados, cambios en hallazgos, programaciones y cambios de SSO, con quién lo hizo, cuándo y desde dónde. Se conserva 12 meses.

- Filtra por tipo de actividad
- Exporta a CSV para tus registros
- Léelo desde tu SIEM con una clave de API
- Dirección IP y navegador en cada evento



05 · VIGILAR LOS CAMBIOS

Entérate cuando aparece algo nuevo

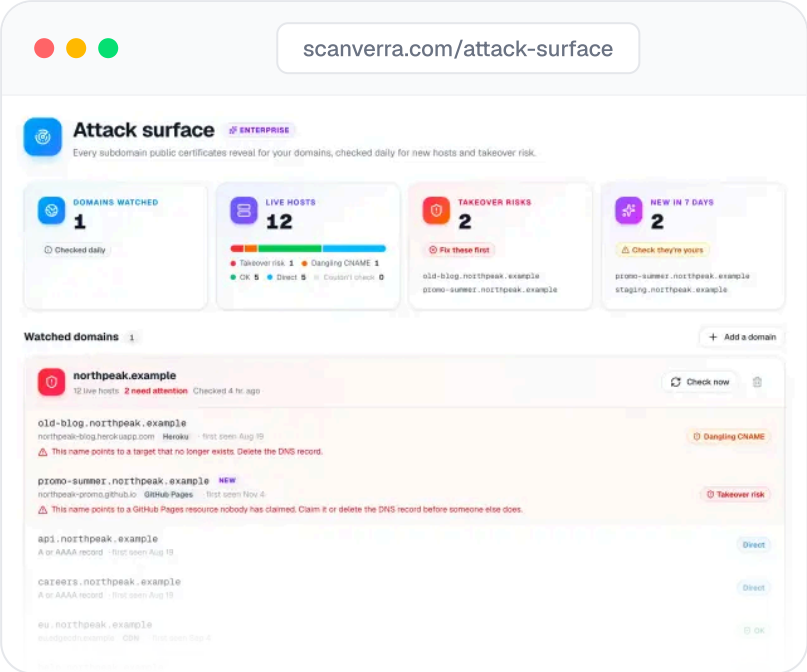
Comprobaciones diarias de subdominios olvidados y semanales de cómo hablan los asistentes de IA de tus marcas.

Enterprise

Encuentra los subdominios que habías olvidado

Scanverra lee cada día los registros públicos de certificados de tus dominios, comprueba en cada subdominio el riesgo de toma de control y los DNS colgantes, y te avisa cuando aparece un host nuevo.

- ✓ Comprobación de toma de control para servicios como GitHub Pages y Heroku
- ✓ Registros CNAME colgantes señalados, con qué hacer al respecto
- ✓ Alertas de hosts nuevos y de riesgos nuevos
- ✓ Los hosts que salieron del DNS se conservan como historial

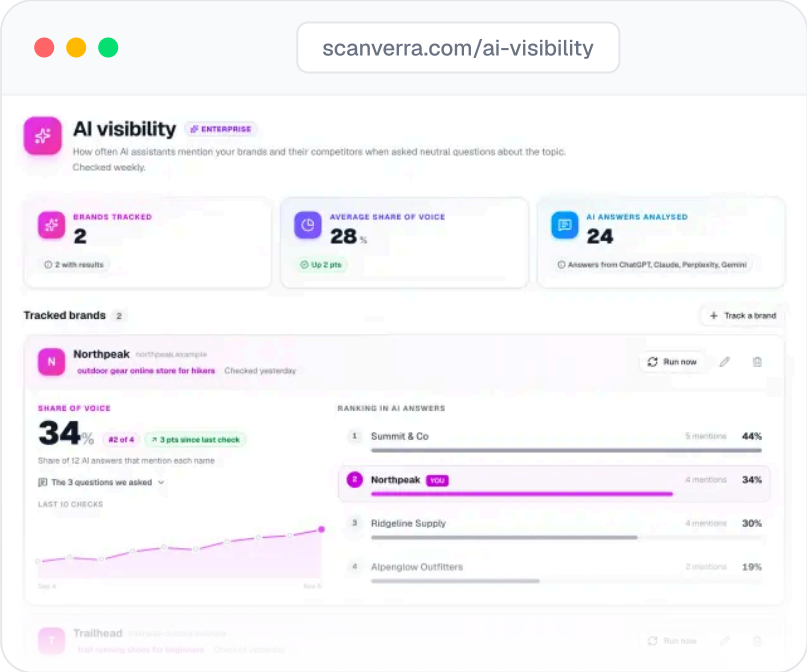


Enterprise

Tu cuota de voz en las respuestas de la IA

Sigue con qué frecuencia los asistentes de IA nombran tus marcas y a tus competidores cuando los compradores hacen preguntas neutrales sobre tu mercado. Cada marca se comprueba cada semana, con su evolución y su posición.

- ✓ Varias marcas, cada una con su propio tema y hasta 5 competidores
- ✓ Preguntas neutrales, como las de un comprador, que nunca te mencionan
- ✓ Clasificación frente a los competidores a partir de las mismas respuestas
- ✓ Las preguntas formuladas, junto a cada resultado



Y todo lo demás que necesita un equipo grande

Slack, Microsoft Teams y webhooks

Caídas de puntuación, incumplimientos de política, cambios en páginas de pago y hosts nuevos, enviados donde tu equipo ya trabaja. Los webhooks se firman con HMAC-SHA256.

Controles de datos

Desactiva los enlaces públicos a informes, apaga la IA para todo el equipo para que ningún dato de escaneo llegue a un modelo y conserva el historial 30, 90, 180 o 365 días.

Informes de marca blanca

Tu nombre, logotipo y color en los informes PDF y en los enlaces compartidos a informes de sitios web, con la mención a Scanverra opcional.

Claves de API del equipo y exportación de datos

Claves propiedad del equipo, con permisos de solo lectura y fechas de caducidad, y un feed CSV, NDJSON o JSON de cada escaneo para tu almacén de datos.

GitLab, también autogestionado

Escanea repositorios de gitlab.com y de GitLab autogestionado y abre merge requests con correcciones, junto a GitHub, Bitbucket y Azure DevOps.

Monitorización de todo el sitio

Rastreos SEO programados de hasta 100 páginas por sitio, puntuados y con alertas como cualquier escaneo programado.

10 plazas, más bajo petición

Acceso de Administrador, Miembro y Lector para todo el equipo, un gestor de cuenta asignado y soporte prioritario.

Escaneos programados ilimitados

Escaneos diarios, semanales o mensuales de cada sitio y repositorio, con una alerta cuando baja una puntuación.

Lo que suelen preguntar los compradores

¿Qué incluye Enterprise?

Todo lo de Team, más SSO y SCIM, el registro de auditoría, los espacios de trabajo, el paquete de cumplimiento, la política del equipo, los controles de datos, los informes de marca blanca, la monitorización de la superficie de ataque y de las páginas de pago, la visibilidad en IA para varias marcas, las claves de API del equipo y el resumen ejecutivo semanal.

¿Cómo se factura Enterprise?

Enterprise es un contrato a medida con precios por volumen. Cuéntanos cuántos sitios, repositorios y personas tienes y te enviaremos un presupuesto.

¿Qué proveedores de identidad funcionan con SSO?

Cualquier proveedor de identidad SAML 2.0, incluidos Okta, Microsoft Entra ID y Google Workspace. El aprovisionamiento SCIM 2.0 funciona con Okta y Microsoft Entra ID.

¿El paquete de cumplimiento es una certificación?

No. Relaciona los hallazgos automáticos con los requisitos de cada marco para que tengas evidencias con las que trabajar. Una certificación también necesita controles de procesos y políticas que ningún escáner puede comprobar.

¿Podemos mantener nuestros datos lejos de los modelos de IA?

Sí. Con la IA desactivada para el equipo, ningún dato de escaneo se envía a un modelo de IA. Las puntuaciones y los hallazgos siguen funcionando; los resúmenes, las correcciones y el chat con IA se desactivan.

¿Podéis escanear páginas tras un inicio de sesión o sitios en una red privada?

La Auditoría de navegador y las comprobaciones de páginas de pago pueden usar un acceso guardado para páginas tras un inicio de sesión. Los sitios que solo son accesibles dentro de tu propia red todavía no se pueden escanear.

Habla con nosotros

Cuéntanos sobre tus sitios, repositorios y equipo, y volveremos con un plan y un presupuesto.

CORREO
support@scanverra.com

WEB
www.scanverra.com/es/enterprise