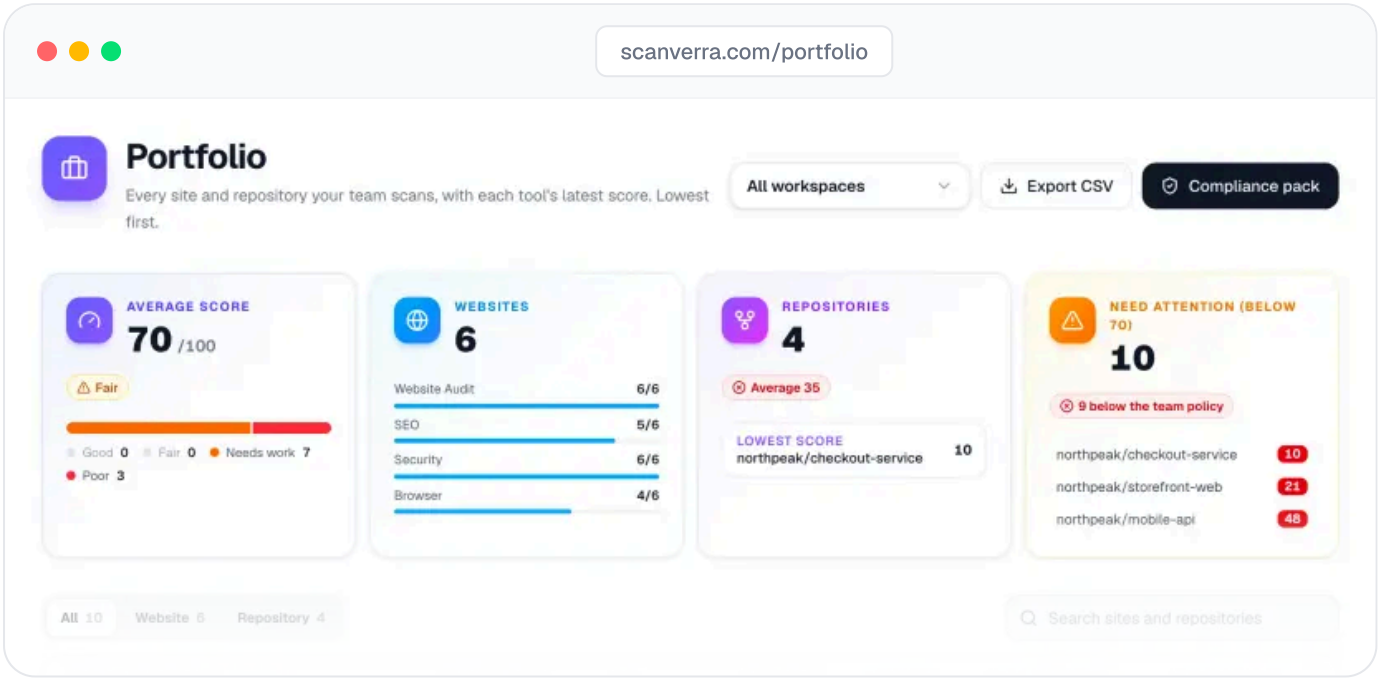
SCANVERRA

SCANVERRA ENTERPRISE

Présentation de Scanverra Enterprise

Portefeuille, conformité, remédiation et contrôle des accès pour tous vos sites et dépôts.



6	7	12 mois	100
outils dans un portefeuille	référentiels de conformité couverts	de journal d'audit	pages par exploration de site

- ✓ SSO SAML et SCIM
- ✓ OWASP, PCI DSS, WCAG, SOC 2, RGPD
- ✓ Journal d'audit sur 12 mois
- ✓ Slack, Teams et webhooks

SOMMAIRE

01 Tout voir
02 Prouver la conformité
03 Corriger plus vite
04 Maîtriser les accès
05 Surveiller les changements

Les écrans de cette page montrent une entreprise de démonstration avec des données fictives.

01 · TOUT VOIR

Tous vos sites et dépôts d'un seul coup d'œil

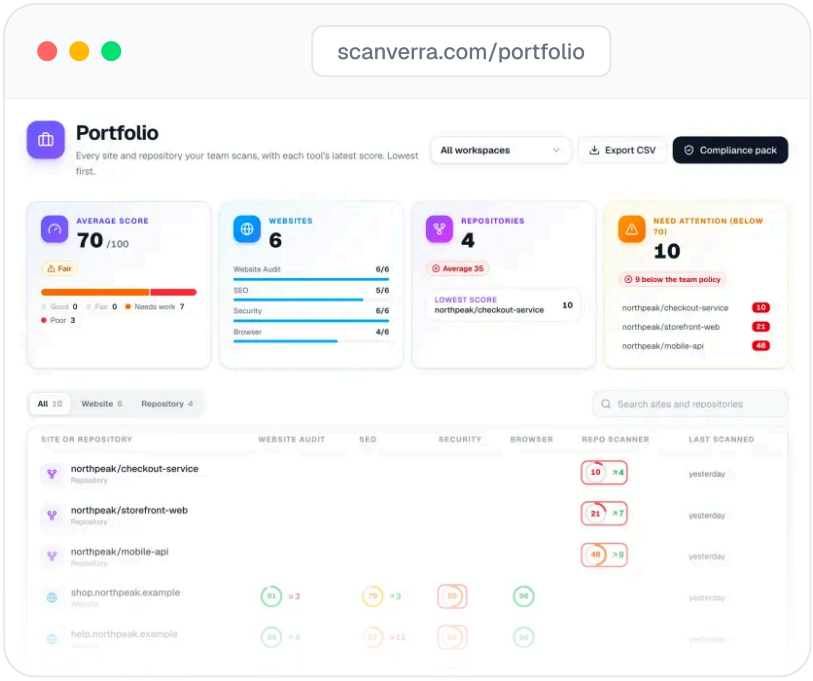
Une vue de tout ce que gèrent vos équipes, et un résumé hebdomadaire pour ceux qui veulent l'essentiel.

Team et Enterprise

Un portefeuille de tous vos sites et dépôts

Chaque cible scannée par votre équipe, avec le dernier score de chaque outil et l'évolution depuis le scan précédent, du plus faible au meilleur. Filtrez-le par espace de travail, exportez-le ou ouvrez le rapport derrière chaque chiffre.

- Les scores Audit de site, SEO, Sécurité, Audit navigateur et Analyseur de dépôts côte à côte
- Un anneau rouge sur tout ce qui est sous la politique de votre équipe
- Code et site en production : les dépendances vulnérables réellement déployées
- L'IA dans votre code : fournisseurs, modèles et serveurs MCP dans tous les dépôts

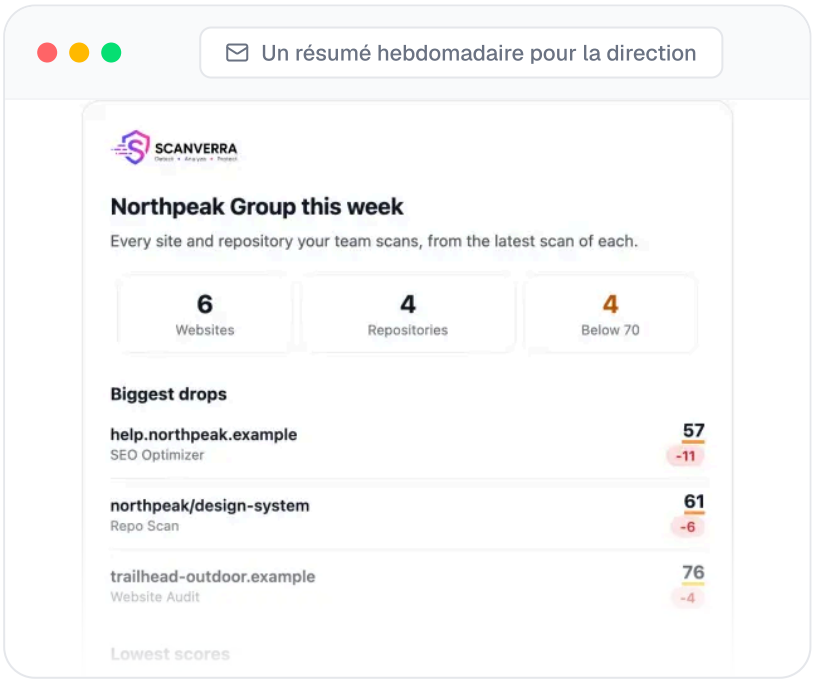


Enterprise

Un résumé hebdomadaire pour la direction

Chaque lundi, les propriétaires et administrateurs reçoivent un e-mail avec les scores les plus bas, les plus fortes baisses et les dépôts qui utilisent l'IA sans politique. Chacun peut se désabonner individuellement.

- Les scores les plus bas et les plus fortes baisses de tout le portefeuille
- Les lacunes de politique IA issues des derniers scans de dépôts
- Un lien vers le portefeuille pour le détail



02 · PROUVER LA CONFORMITÉ

Des éléments de preuve exploitables par votre auditeur

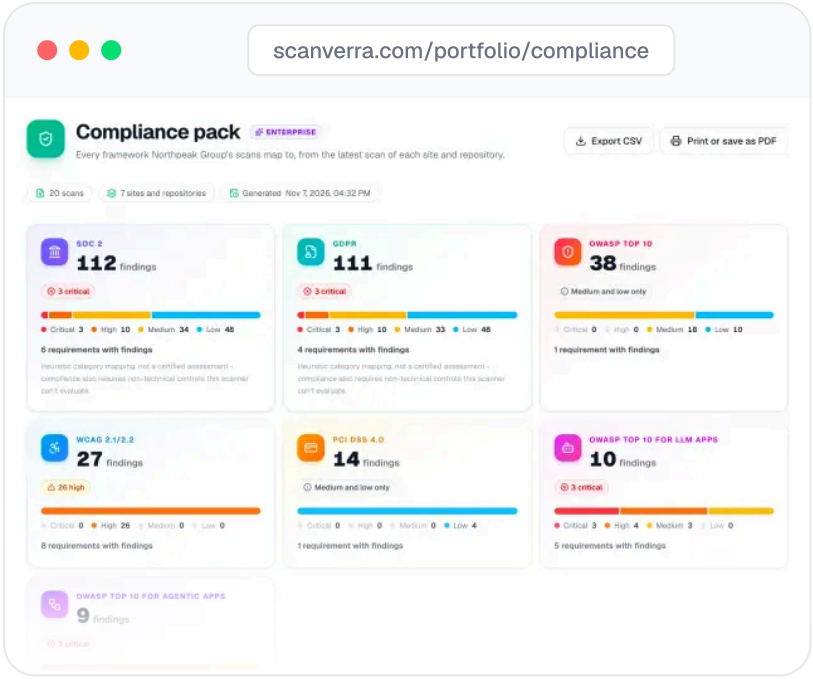
Des résultats par référentiel issus de vos vrais scans, et la surveillance des pages de paiement exigée par PCI DSS 4.0.

Enterprise

Un pack de conformité construit à partir de vos vrais scans

OWASP Top 10, PCI DSS 4.0, WCAG 2.1 et 2.2, SOC 2, RGPD et les listes OWASP pour les applications LLM et agentiques, exigence par exigence, avec les sites et dépôts concernés. C'est une base de travail, pas une certification.

- Chaque exigence avec ses constats, sa gravité et les cibles concernées
- Export en CSV, ou enregistrement en PDF pour le dossier d'audit
- Téléchargements SBOM en CycloneDX 1.5 et SPDX 2.3
- Filtrez par espace de travail pour donner à chaque entité son propre pack

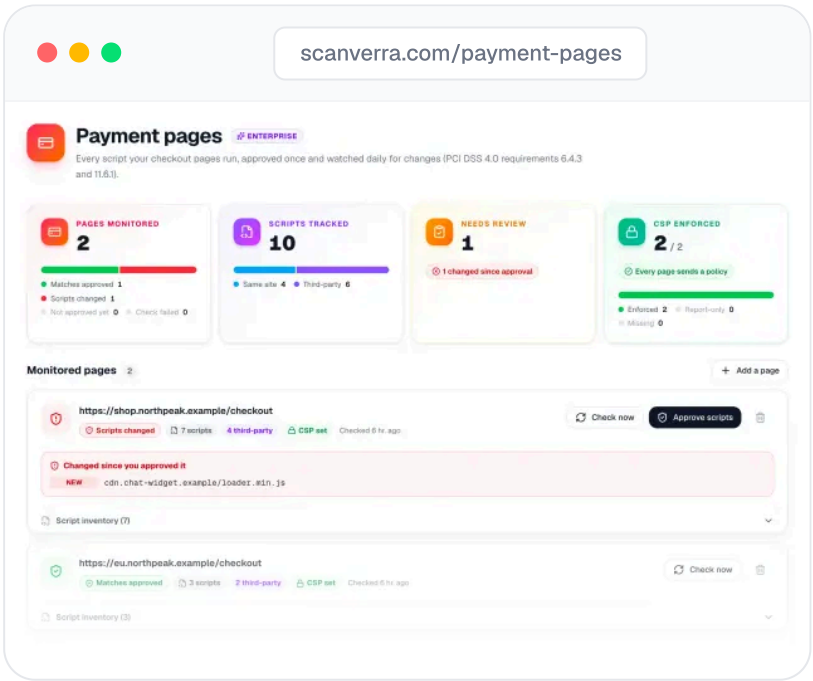


Enterprise

Surveillance des scripts PCI DSS 4.0 pour les pages de paiement

Chaque script exécuté par vos pages de paiement est enregistré dans un vrai navigateur, avec son empreinte SHA-256 et votre Content-Security-Policy. Validez la liste une fois, et tout script nouveau ou modifié est signalé le lendemain.

- Conçu pour les exigences 6.4.3 et 11.6.1
- Scripts tiers et inline, chacun avec son empreinte
- Pages de paiement derrière une connexion, avec un identifiant enregistré
- Alertes par e-mail, Slack, Microsoft Teams ou votre webhook



03 · CORRIGER PLUS VITE

Du constat à la correction, avec un responsable

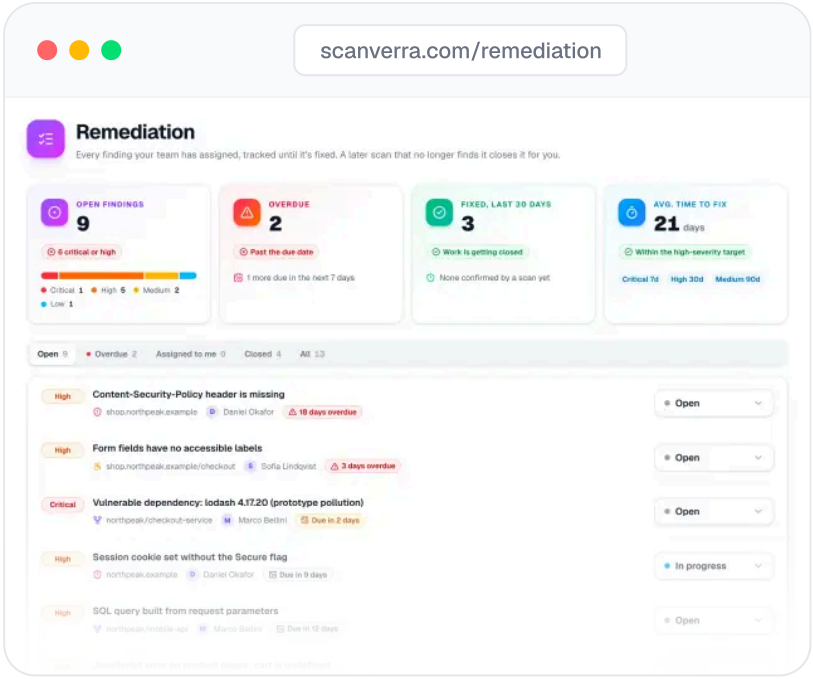
Chaque constat a une personne et une échéance, et une politique décide de ce qui est assez bon pour être livré.

Team et Enterprise

Les constats deviennent des tâches avec responsables et échéances

Attribuez n'importe quel constat de n'importe quel outil à un collègue. L'échéance dépend de la gravité, la personne reçoit un e-mail, et un scan ultérieur qui ne trouve plus le problème clôt la tâche pour vous.

- Échéances par gravité : critique 7 jours, élevée 30, moyenne 90, faible 180
- Ouverts, en retard, corrigés et délai de correction en un coup d'œil
- Chaque tâche ouvre le constat exact dans son rapport
- Clos uniquement quand un scan le confirme, pour les vérifications effectuées par ce scan

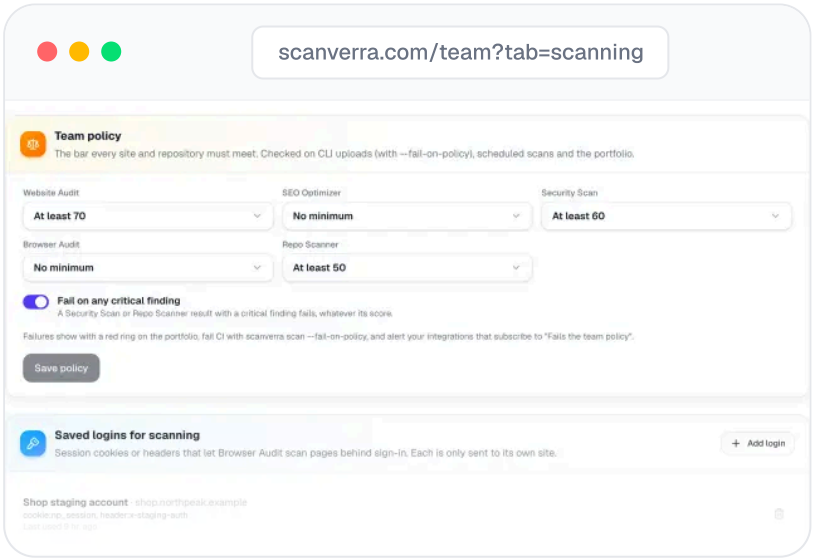


Enterprise

Une même exigence pour chaque site et dépôt

Fixez le score minimum de chaque outil et faites échouer tout constat critique. La même politique est vérifiée sur les envois de la CLI en CI, sur les scans planifiés et dans le portefeuille.

- Un score minimum par outil
- Faites échouer le build avec scanverra scan --fail-on-policy
- Une alerte quand un scan planifié ne respecte pas la politique
- Des identifiants enregistrés pour que l'Audit navigateur scanne les pages derrière une connexion



04 · MAÎTRISER LES ACCÈS

Les contrôles que demandent les achats

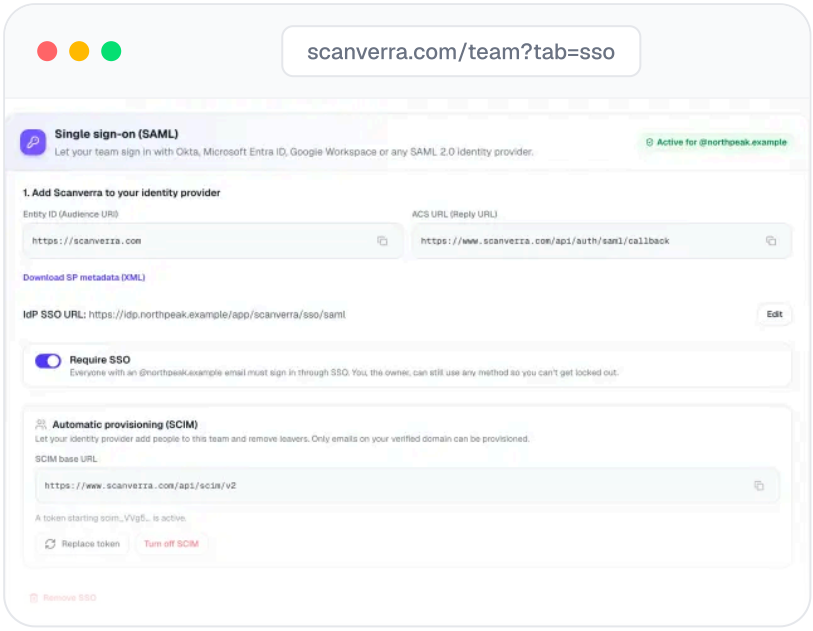
Authentification unique, provisionnement, rôles, espaces de travail et une trace de qui a fait quoi.

Enterprise

Authentification unique et provisionnement, configurés par vous

Connectez Okta, Microsoft Entra ID, Google Workspace ou tout fournisseur d'identité SAML 2.0 depuis la page Équipe. Prouvez que le domaine vous appartient avec un enregistrement DNS, puis imposez le SSO à tous ses utilisateurs.

- Imposez le SSO, avec un accès de secours pour le propriétaire afin de ne jamais être bloqué
- SCIM 2.0 ajoute et retire des membres depuis votre fournisseur d'identité
- Seuls les e-mails de votre domaine vérifié peuvent être provisionnés
- Chaque réponse SAML n'est acceptée qu'une fois, et uniquement pour son propre domaine

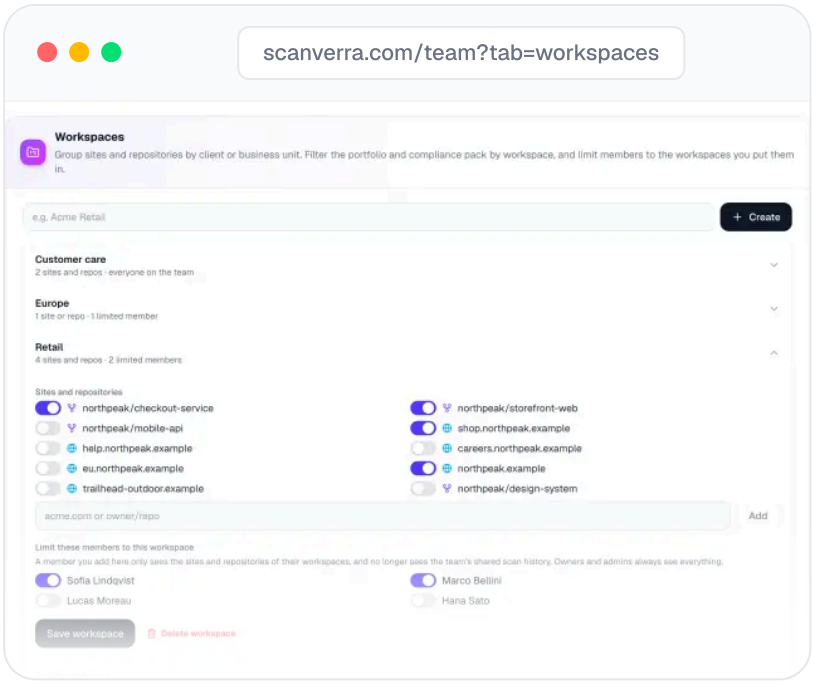


Enterprise

Des espaces de travail et des rôles calqués sur votre organisation

Regroupez sites et dépôts par entité, marque ou client, et donnez un accès Administrateur, Membre ou Lecteur. Une personne limitée à un espace de travail ne voit que ses sites et dépôts.

- Les espaces de travail filtrent le portefeuille, le pack de conformité et l'export de données
- Les lecteurs consultent tous les rapports mais ne peuvent ni lancer de scans payants ni modifier les réglages
- Des clés d'API d'équipe qui continuent de fonctionner après le départ de leur créateur
- Des clés en lecture seule et des dates d'expiration pour les pipelines et les outils BI

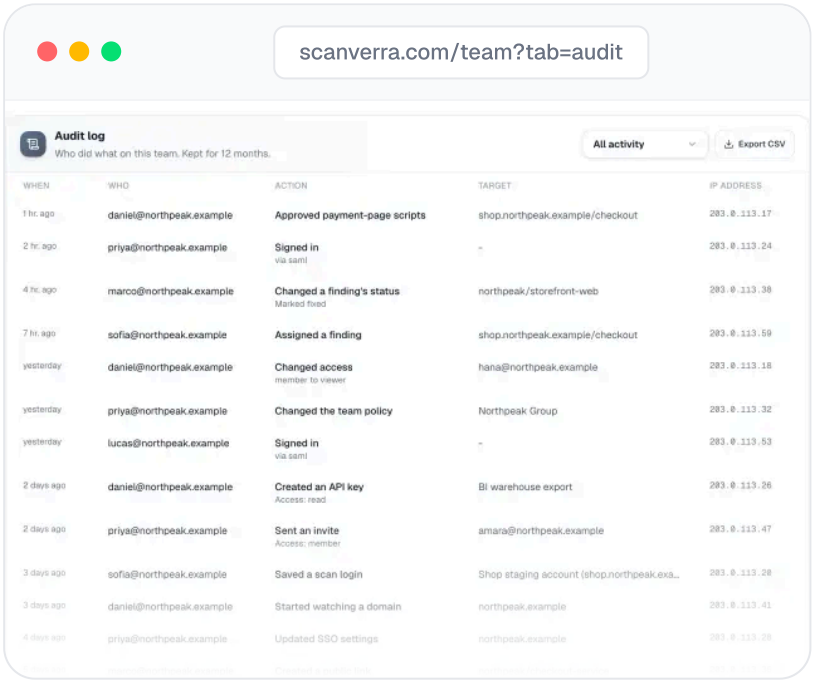


Enterprise

Un journal d'audit pour tout ce qui compte

Connexions, invitations, changements d'accès, clés d'API, liens de partage, scans supprimés, mises à jour de constats, planifications et changements de SSO, avec qui, quand et d'où. Conservé 12 mois.

- Filtre par type d'activité
- Export en CSV pour vos archives
- Lecture depuis votre SIEM avec une clé d'API
- Adresse IP et navigateur pour chaque événement



05 · SURVEILLER LES CHANGEMENTS

Savoir quand quelque chose de nouveau apparaît

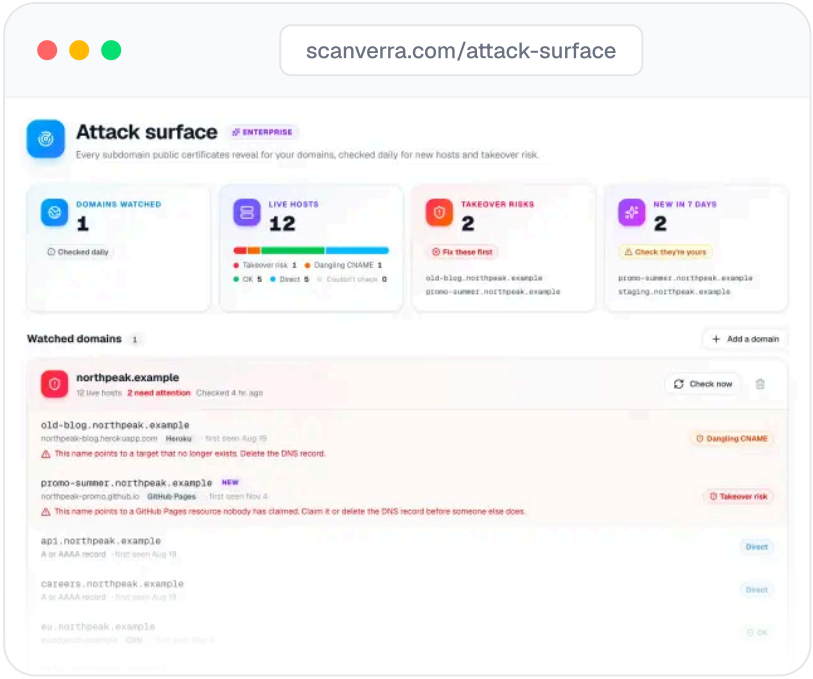
Des vérifications quotidiennes des sous-domaines oubliés, et hebdomadaires de la façon dont les assistants IA parlent de vos marques.

Enterprise

Retrouvez les sous-domaines oubliés

Scanverra lit chaque jour les journaux publics de certificats de vos domaines, vérifie le risque de prise de contrôle et les DNS orphelins de chaque sous-domaine, et vous prévient quand un nouvel hôte apparaît.

- Vérification de prise de contrôle pour des hébergeurs comme GitHub Pages et Heroku
- Enregistrements CNAME orphelins signalés, avec la marche à suivre
- Alertes pour les nouveaux hôtes et les nouveaux risques
- Les hôtes sortis du DNS sont conservés en historique

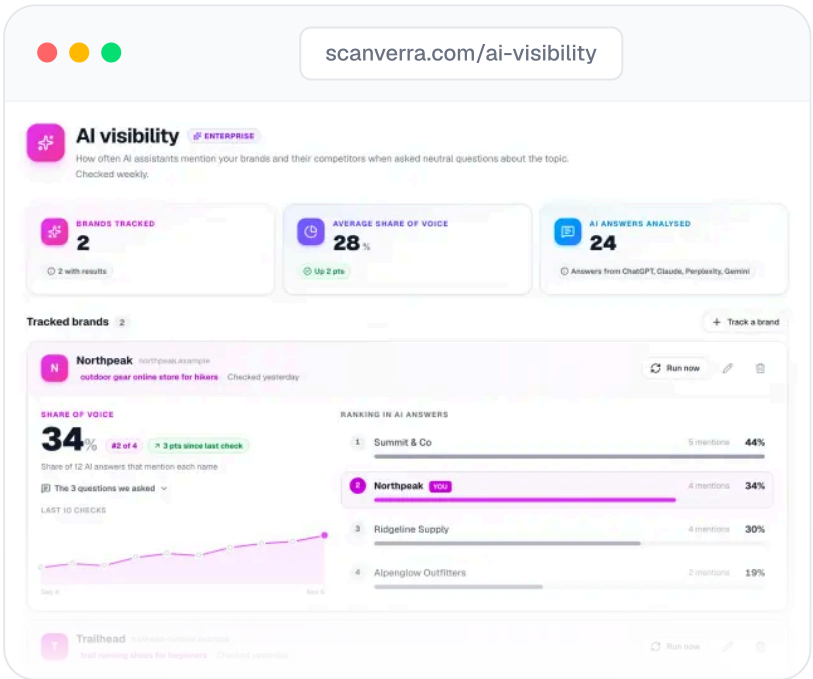


Enterprise

Votre part de voix dans les réponses de l'IA

Suivez la fréquence à laquelle les assistants IA citent vos marques et vos concurrents quand des acheteurs posent des questions neutres sur votre marché. Chaque marque est vérifiée chaque semaine, avec son évolution et son classement.

- Plusieurs marques, chacune avec son sujet et jusqu'à 5 concurrents
- Des questions neutres, comme celles d'un acheteur, qui ne vous citent jamais
- Classement face aux concurrents à partir des mêmes réponses
- Les questions posées, affichées à côté de chaque résultat



Et tout le reste dont une grande équipe a besoin

Slack, Microsoft Teams et webhooks

Baisses de score, non-respects de la politique, changements sur les pages de paiement et nouveaux hôtes, envoyés là où votre équipe travaille déjà. Les webhooks sont signés en HMAC-SHA256.

Contrôle des données

Désactivez les liens publics vers les rapports, coupez l'IA pour toute l'équipe afin qu'aucune donnée de scan n'atteigne un modèle, et conservez l'historique 30, 90, 180 ou 365 jours.

Rapports en marque blanche

Votre nom, votre logo et votre couleur sur les rapports PDF et sur les liens partagés vers les rapports de sites, la mention Scanverra étant facultative.

Clés d'API d'équipe et export de données

Des clés appartenant à l'équipe, avec des droits en lecture seule et des dates d'expiration, et un flux CSV, NDJSON ou JSON de chaque scan pour votre entrepôt de données.

GitLab, y compris auto-hébergé

Scannez les dépôts gitlab.com et GitLab auto-hébergés et ouvrez des merge requests de correction, aux côtés de GitHub, Bitbucket et Azure DevOps.

Surveillance de tout le site

Des explorations SEO planifiées jusqu'à 100 pages par site, notées et signalées comme tout scan planifié.

10 places, davantage sur demande

Accès Administrateur, Membre et Lecteur pour toute l'équipe, un responsable de compte dédié et un support prioritaire.

Scans planifiés illimités

Des scans quotidiens, hebdomadaires ou mensuels de chaque site et dépôt, avec une alerte quand un score baisse.

Ce que demandent souvent les acheteurs

Que comprend Enterprise ?

Tout ce qui est dans Team, plus le SSO et SCIM, le journal d'audit, les espaces de travail, le pack de conformité, la politique d'équipe, le contrôle des données, les rapports en marque blanche, la surveillance de la surface d'attaque et des pages de paiement, la visibilité IA multimarque, les clés d'API d'équipe et le résumé hebdomadaire pour la direction.

Comment Enterprise est-il facturé ?

Enterprise est un contrat sur mesure avec une tarification au volume. Indiquez-nous combien de sites, de dépôts et de personnes vous avez, et nous vous enverrons un devis.

Quels fournisseurs d'identité fonctionnent avec le SSO ?

Tout fournisseur d'identité SAML 2.0, dont Okta, Microsoft Entra ID et Google Workspace. Le provisionnement SCIM 2.0 fonctionne avec Okta et Microsoft Entra ID.

Le pack de conformité est-il une certification ?

Non. Il rapproche les constats automatiques des exigences de chaque référentiel, pour vous donner une base de travail. Une certification exige aussi des contrôles de processus et de politique qu'aucun scanner ne peut vérifier.

Pouvons-nous tenir nos données à l'écart des modèles d'IA ?

Oui. Avec l'IA désactivée pour l'équipe, aucune donnée de scan n'est envoyée à un modèle d'IA. Les scores et les constats fonctionnent toujours ; les résumés, corrections et le chat IA sont désactivés.

Pouvez-vous scanner des pages derrière une connexion ou des sites sur un réseau privé ?

L'Audit navigateur et les vérifications de pages de paiement peuvent utiliser un identifiant enregistré pour les pages derrière une connexion. Les sites accessibles uniquement depuis votre propre réseau ne peuvent pas encore être scannés.

Parlons-en

Parlez-nous de vos sites, de vos dépôts et de votre équipe, et nous reviendrons vers vous avec un plan et un devis.

E-MAIL
support@scanverra.com

WEB
www.scanverra.com/fr/enterprise