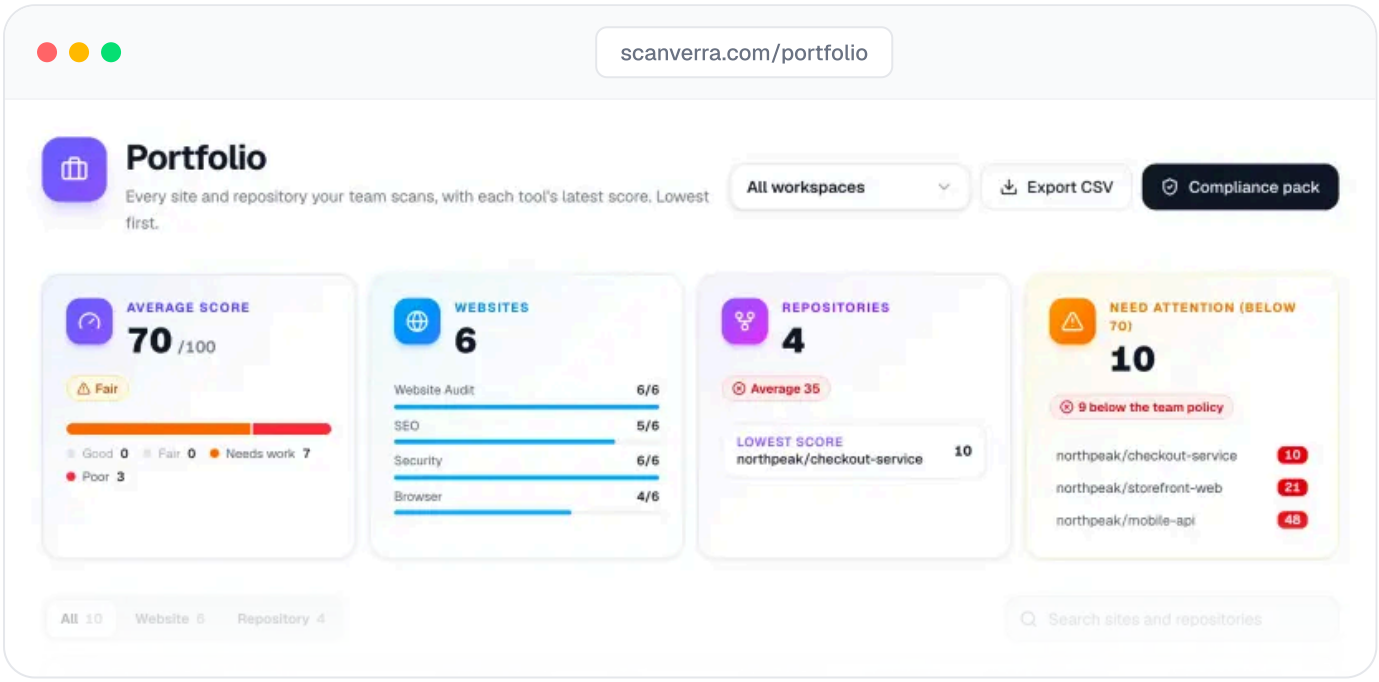
SCANVERRA ENTERPRISE

Scanverra Enterprise im Überblick

Portfolio, Compliance, Behebung und Zugriffskontrollen für alle Ihre Websites und Repositories.



6	7	12 Monate	100
Tools in einem Portfolio	zugeordnete Compliance-Frameworks	Audit-Log	Seiten pro Website-Crawl

- ✓ SAML-SSO und SCIM
- ✓ OWASP, PCI DSS, WCAG, SOC 2, DSGVO
- ✓ Audit-Log für 12 Monate
- ✓ Slack, Teams und Webhooks

INHALT

01 Alles im Blick
02 Compliance belegen
03 Schneller beheben
04 Zugriff steuern
05 Änderungen erkennen

Die Ansichten auf dieser Seite zeigen ein Demo-Unternehmen mit erfundenen Daten.

01 · ALLES IM BLICK

Alle Websites und Repositories auf einen Blick

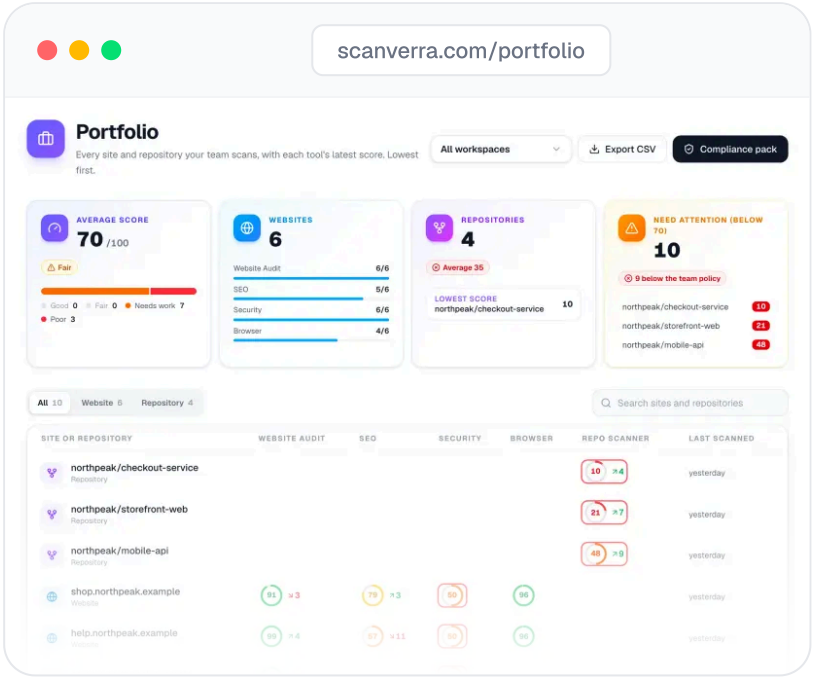
Eine Ansicht von allem, was Ihre Teams betreiben, und eine wöchentliche Zusammenfassung für alle, die nur die Kernaussage brauchen.

Team und Enterprise

Ein Portfolio aller Websites und Repositories

Jedes Ziel, das Ihr Team scannt, mit dem neuesten Wert jedes Tools und der Veränderung seit dem letzten Scan, das schwächste zuerst. Nach Workspace filtern, exportieren oder den Bericht hinter jeder Zahl öffnen.

- Werte aus Website-Audit, SEO, Sicherheit, Browser-Audit und Repo-Scanner nebeneinander
- Ein roter Ring bei allem, was unter der Richtlinie Ihres Teams liegt
- Code und Live-Website: verwundbare Abhängigkeiten, die tatsächlich ausgeliefert sind
- KI in Ihrem Code: Anbieter, Modelle und MCP-Server über alle Repositories

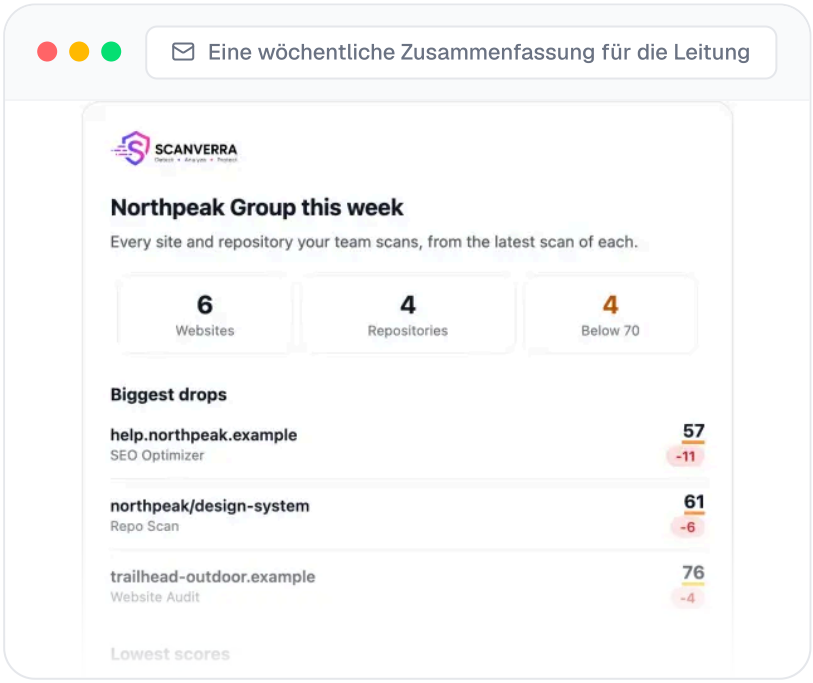


Enterprise

Eine wöchentliche Zusammenfassung für die Leitung

Jeden Montag erhalten Inhaber und Admins eine E-Mail mit den niedrigsten Werten, den größten Rückgängen und den Repositories, die KI ohne Richtlinie nutzen. Jede Person kann sich selbst abmelden.

- Niedrigste Werte und größte Rückgänge im gesamten Portfolio
- Lücken bei KI-Richtlinien aus den neuesten Repository-Scans
- Ein Link zurück ins Portfolio für die Details



02 · COMPLIANCE BELEGEN

Nachweise, mit denen Ihre Prüfer arbeiten können

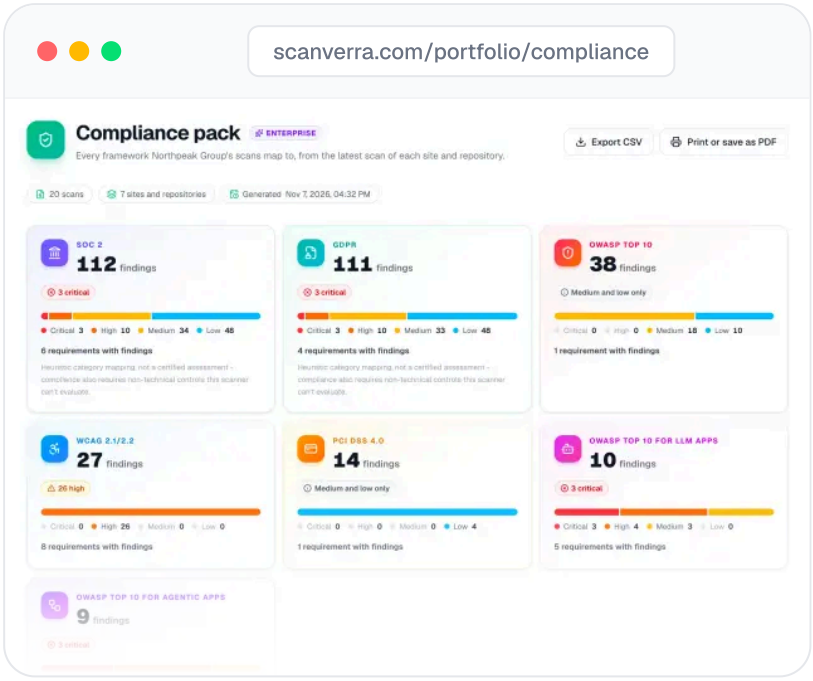
Ergebnisse je Framework aus Ihren echten Scans und das Checkout-Monitoring, das PCI DSS 4.0 verlangt.

Enterprise

Ein Compliance-Paket aus Ihren echten Scans

OWASP Top 10, PCI DSS 4.0, WCAG 2.1 und 2.2, SOC 2, DSGVO und die OWASP-Listen für LLM- und Agenten-Apps, Anforderung für Anforderung, mit den betroffenen Websites und Repositories. Es ist eine Arbeitsgrundlage, keine Zertifizierung.

- ✓ Jede Anforderung mit ihren Befunden, ihrem Schweregrad und den betroffenen Zielen
- ✓ Export als CSV oder als PDF für die Prüfakte
- ✓ SBOM-Downloads in CycloneDX 1.5 und SPDX 2.3
- ✓ Nach Workspace filtern, damit jede Geschäftseinheit ihr eigenes Paket bekommt

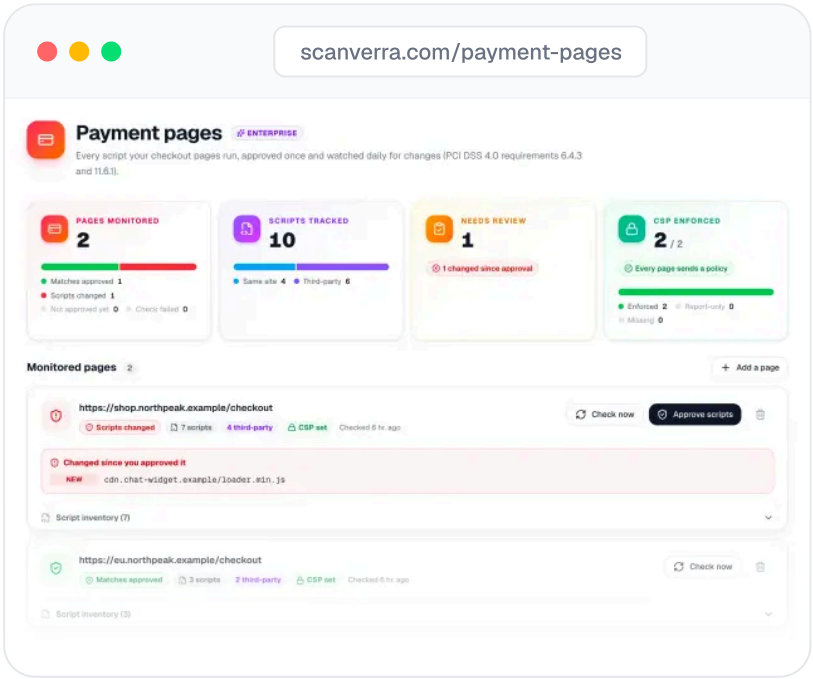


Enterprise

PCI-DSS-4.0-Skriptmonitoring für Checkout-Seiten

Jedes Skript, das Ihre Zahlungsseiten ausführen, wird in einem echten Browser erfasst, mit seinem SHA-256-Hash und Ihrer Content-Security-Policy. Geben Sie die Liste einmal frei, und jedes neue oder geänderte Skript wird am nächsten Tag gemeldet.

- ✓ Entwickelt für die Anforderungen 6.4.3 und 11.6.1
- ✓ Drittanbieter- und Inline-Skripte, jeweils mit Hash
- ✓ Checkout-Seiten hinter einer Anmeldung, mit einem gespeicherten Login
- ✓ Benachrichtigungen per E-Mail, Slack, Microsoft Teams oder Webhook



03 · SCHNELLER BEHEBEN

Vom Befund zur Behebung, mit klarer Verantwortung

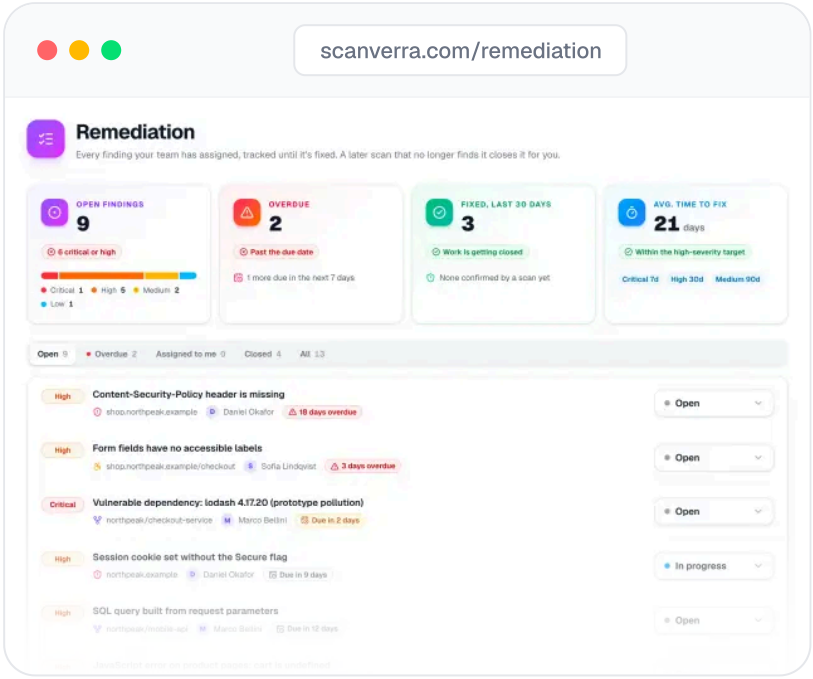
Jeder Befund bekommt eine Person und eine Frist, und eine Richtlinie legt fest, was gut genug zum Ausliefern ist.

Team und Enterprise

Aus Befunden werden Aufgaben mit Verantwortlichen und Fristen

Weisen Sie jeden Befund aus jedem Tool einer Person im Team zu. Die Frist richtet sich nach dem Schweregrad, die Person erhält eine E-Mail, und ein späterer Scan, der das Problem nicht mehr findet, schließt die Aufgabe automatisch.

- ✓ Fristen nach Schweregrad: kritisch 7 Tage, hoch 30, mittel 90, niedrig 180
- ✓ Offen, überfällig, behoben und Zeit bis zur Behebung auf einen Blick
- ✓ Jede Aufgabe öffnet den genauen Befund in seinem Bericht
- ✓ Geschlossen nur, wenn ein Scan es bestätigt, für die Prüfungen, die dieser Scan ausgeführt hat

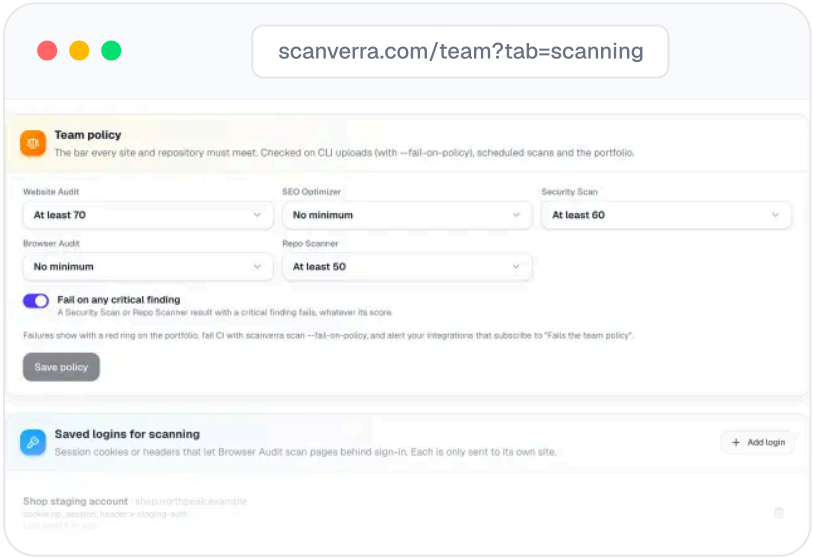


Enterprise

Ein Maßstab für jede Website und jedes Repository

Legen Sie den niedrigsten zulässigen Wert je Tool fest und lassen Sie jeden kritischen Befund sofort durchfallen. Dieselbe Richtlinie wird bei CLI-Uploads in der CI, bei geplanten Scans und im Portfolio geprüft.

- ✓ Ein Mindestwert je Tool
- ✓ Den Build mit scanverra scan --fail-on-policy abbrechen
- ✓ Eine Benachrichtigung, wenn ein geplanter Scan die Richtlinie verfehlt
- ✓ Gespeicherte Logins, damit das Browser-Audit Seiten hinter einer Anmeldung scannen kann



04 · ZUGRIFF STEUERN

Die Kontrollen, nach denen der Einkauf fragt

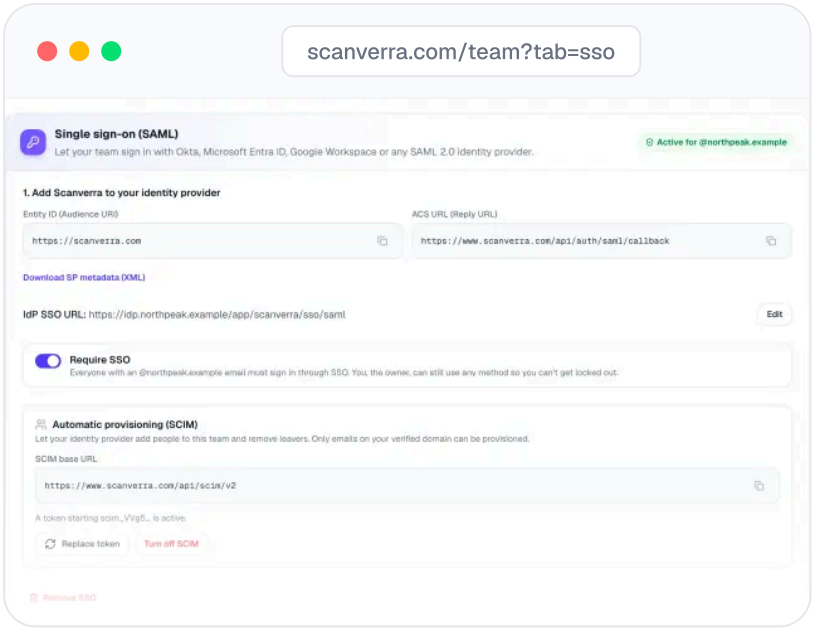
Single Sign-on, Provisionierung, Rollen, Workspaces und ein Protokoll darüber, wer was getan hat.

Enterprise

Single Sign-on und Provisionierung, selbst eingerichtet

Verbinden Sie Okta, Microsoft Entra ID, Google Workspace oder einen anderen SAML-2.0-Identitätsanbieter auf der Team-Seite. Belegen Sie mit einem DNS-Eintrag, dass Ihnen die Domain gehört, und schreiben Sie SSO für alle darauf vor.

- ✓ SSO vorschreiben, mit einem Zugang für den Inhaber, damit Sie sich nie aussperren
- ✓ SCIM 2.0 fügt Mitglieder aus Ihrem Identitätsanbieter hinzu und entfernt sie
- ✓ Nur E-Mails auf Ihrer verifizierten Domain können provisioniert werden
- ✓ Jede SAML-Antwort wird nur einmal und nur für ihre eigene Domain akzeptiert

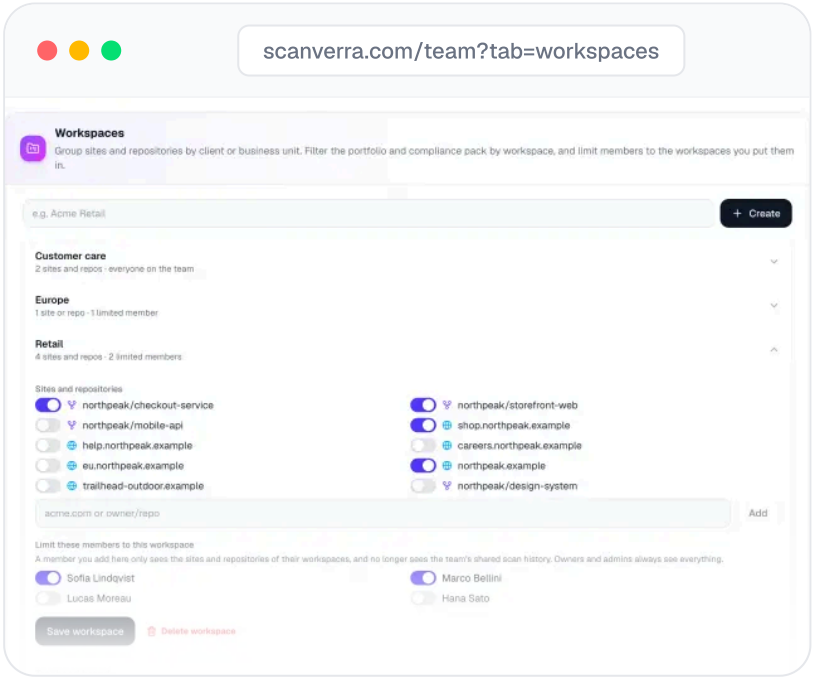


Enterprise

Workspaces und Rollen passend zu Ihrem Organigramm

Gruppieren Sie Websites und Repositories nach Geschäftseinheit, Marke oder Kunde und vergeben Sie Admin-, Mitglieds- oder Betrachterzugriff. Wer auf einen Workspace beschränkt ist, sieht nur dessen Websites und Repositories.

- ✓ Workspaces filtern Portfolio, Compliance-Paket und Datenexport
- ✓ Betrachter lesen jeden Bericht, können aber keine kostenpflichtigen Scans starten oder Einstellungen ändern
- ✓ Team-API-Schlüssel, die weiter funktionieren, wenn ihr Ersteller geht
- ✓ Schreibgeschützte Schlüssel und Ablaufdaten für Pipelines und BI-Tools

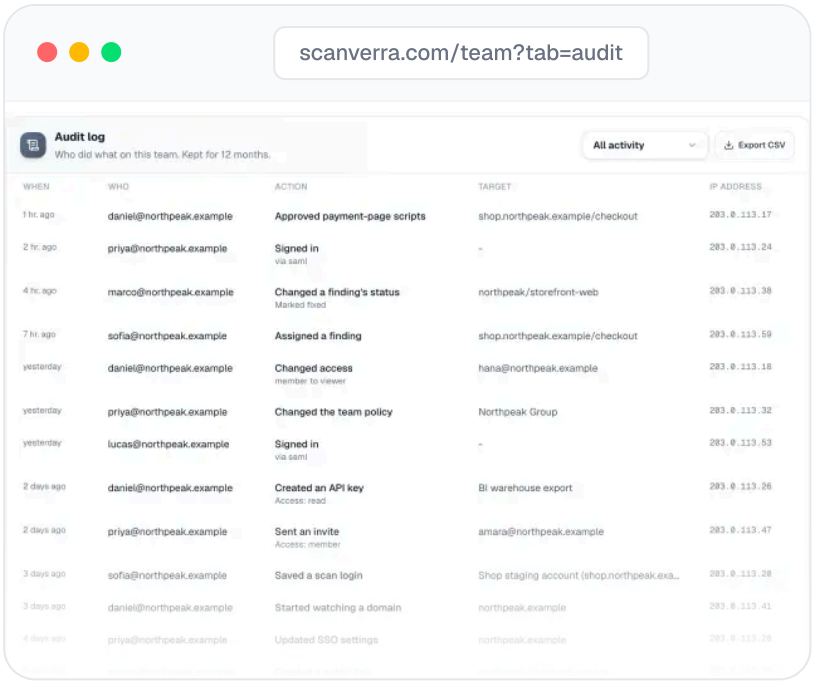


Enterprise

Ein Audit-Log für alles, was zählt

Anmeldungen, Einladungen, Zugriffsänderungen, API-Schlüssel, Freigabelinks, gelöschte Scans, Befund-Updates, Zeitpläne und SSO-Änderungen, mit wer, wann und von wo. 12 Monate aufbewahrt.

- Nach Art der Aktivität filtern
- Als CSV für Ihre Unterlagen exportieren
- Mit einem API-Schlüssel aus Ihrem SIEM abrufen
- IP-Adresse und Browser bei jedem Ereignis



05 · ÄNDERUNGEN ERKENNEN

Erfahren, wenn etwas Neues auftaucht

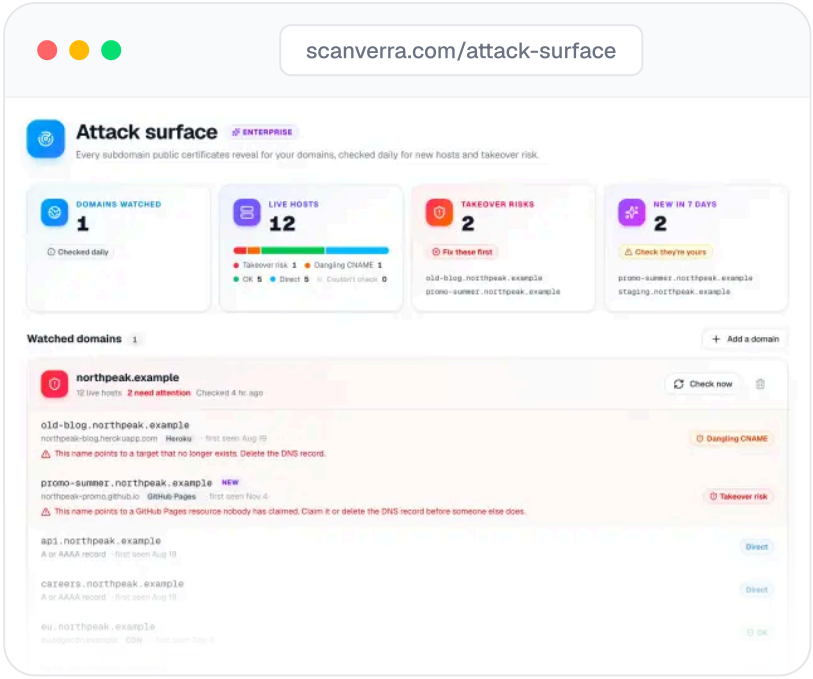
Tägliche Prüfungen auf vergessene Subdomains, wöchentliche Prüfungen, wie KI-Assistenten über Ihre Marken sprechen.

Enterprise

Finden Sie die Subdomains, die Sie vergessen haben

Scanverra liest täglich die öffentlichen Zertifikatslogs Ihrer Domains, prüft jede Subdomain auf Übernahmerisiko und verwaiste DNS-Einträge und meldet, wenn ein neuer Host auftaucht.

- ✓ Übernahmeprüfungen für Hosting-Dienste wie GitHub Pages und Heroku
- ✓ Verwaiste CNAME-Einträge markiert, mit dem, was zu tun ist
- ✓ Benachrichtigungen bei neuen Hosts und neuen Risiken
- ✓ Hosts, die nicht mehr im DNS sind, bleiben als Verlauf erhalten

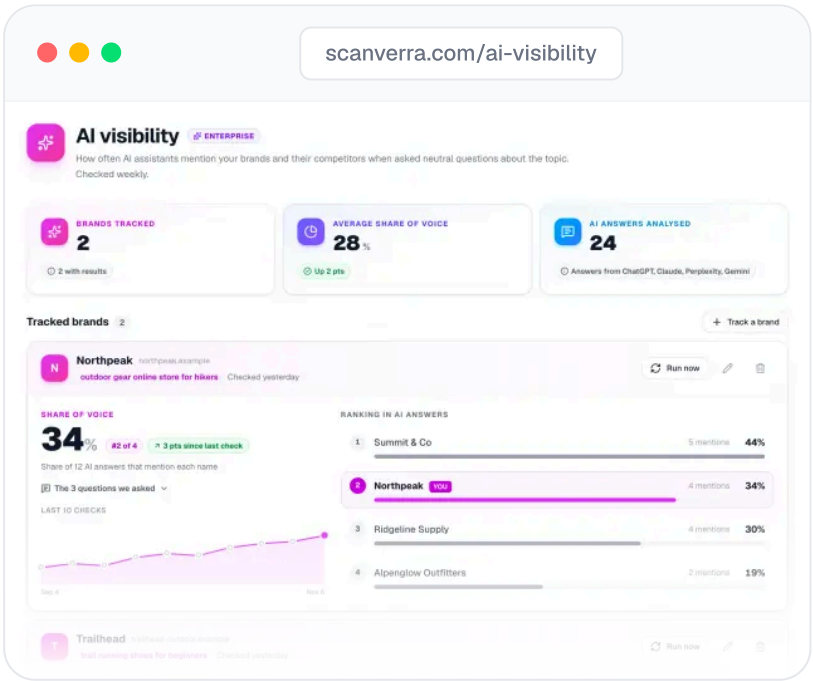


Enterprise

Ihr Anteil an KI-Antworten

Verfolgen Sie, wie oft KI-Assistenten Ihre Marken und Ihre Wettbewerber nennen, wenn Käufer neutrale Fragen zu Ihrem Markt stellen. Jede Marke wird wöchentlich geprüft, mit Verlauf und Rangfolge.

- ✓ Mehrere Marken, jede mit eigenem Thema und bis zu 5 Wettbewerbern
- ✓ Neutrale Fragen wie von Käufern, die Sie nie erwähnen
- ✓ Rangfolge gegenüber Wettbewerbern aus denselben Antworten
- ✓ Die gestellten Fragen, neben jedem Ergebnis angezeigt



Und alles andere, was ein größeres Team braucht

Slack, Microsoft Teams und Webhooks

Wertverluste, Richtlinienverstöße, Änderungen an Zahlungsseiten und neue Hosts, dorthin geschickt, wo Ihr Team schon arbeitet. Webhooks werden mit HMAC-SHA256 signiert.

Datenkontrollen

Öffentliche Berichtslinks abschalten, KI für das ganze Team ausschalten, damit keine Scandaten ein Modell erreichen, und den Scanverlauf 30, 90, 180 oder 365 Tage aufbewahren.

White-Label-Berichte

Ihr Name, Logo und Ihre Farbe auf PDF-Berichten und auf geteilten Links zu Website-Berichten, der Scanverra-Hinweis ist optional.

Team-API-Schlüssel und Datenexport

Schlüssel im Besitz des Teams, mit schreibgeschützten Bereichen und Ablaufdaten, und ein CSV-, NDJSON- oder JSON-Feed aller Scans für Ihr Data Warehouse.

GitLab, auch selbst gehostet

gitlab.com und selbst gehostete GitLab-Repositories scannen und Merge Requests mit Korrekturen öffnen, neben GitHub, Bitbucket und Azure DevOps.

Website-weites Monitoring

Geplante SEO-Crawls mit bis zu 100 Seiten pro Website, bewertet und gemeldet wie jeder geplante Scan.

10 Plätze, mehr auf Anfrage

Admin-, Mitglieds- und Betrachterzugriff für alle im Team, ein fester Ansprechpartner und bevorzugter Support.

Unbegrenzte geplante Scans

Tägliche, wöchentliche oder monatliche Scans jeder Website und jedes Repositorys, mit einer Benachrichtigung, wenn ein Wert sinkt.

Was Käufer meist fragen

Was ist in Enterprise enthalten?

Alles aus Team, dazu SSO und SCIM, das Audit-Log, Workspaces, das Compliance-Paket, die Team-Richtlinie, Datenkontrollen, White-Label-Berichte, Monitoring von Angriffsfläche und Zahlungsseiten, KI-Sichtbarkeit für mehrere Marken, Team-API-Schlüssel und die wöchentliche Zusammenfassung für die Leitung.

Wie wird Enterprise abgerechnet?

Enterprise ist ein individueller Vertrag mit Mengenpreisen. Sagen Sie uns, wie viele Websites, Repositories und Personen Sie haben, und wir schicken Ihnen ein Angebot.

Welche Identitätsanbieter funktionieren mit SSO?

Jeder SAML-2.0-Identitätsanbieter, darunter Okta, Microsoft Entra ID und Google Workspace. SCIM-2.0-Provisionierung funktioniert mit Okta und Microsoft Entra ID.

Ist das Compliance-Paket eine Zertifizierung?

Nein. Es ordnet automatisierte Befunde den Anforderungen jedes Frameworks zu, damit Sie eine Arbeitsgrundlage haben. Eine Zertifizierung braucht außerdem Prozess- und Richtlinienkontrollen, die kein Scanner prüfen kann.

Können wir unsere Daten von KI-Modellen fernhalten?

Ja. Wenn KI für das Team ausgeschaltet ist, werden keine Scandaten an ein KI-Modell gesendet. Werte und Befunde funktionieren weiter; KI-Zusammenfassungen, Korrekturen und Chat sind abgeschaltet.

Können Sie Seiten hinter einer Anmeldung oder Websites in einem privaten Netzwerk scannen?

Browser-Audit und Prüfungen von Zahlungsseiten können einen gespeicherten Login für Seiten hinter einer Anmeldung verwenden. Websites, die nur in Ihrem eigenen Netzwerk erreichbar sind, können noch nicht gescannt werden.

Sprechen Sie mit uns

Erzählen Sie uns von Ihren Websites, Repositories und Ihrem Team, und wir melden uns mit einem Plan und einem Angebot.

E-MAIL
support@scanverra.com

WEB
www.scanverra.com/de/enterprise