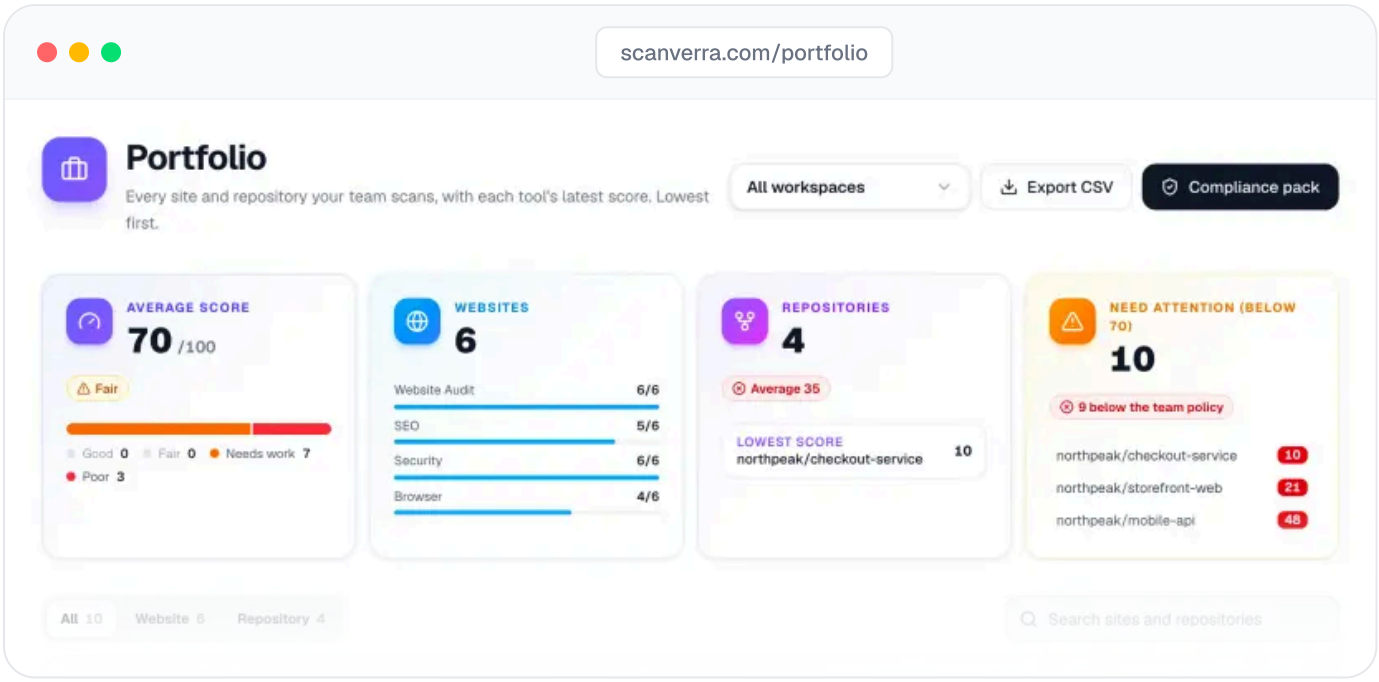
SCANVERRA ENTERPRISE

Scanverra Enterprise の概要

保有するすべてのサイトとリポジトリのための、ポートフォリオ、コンプライアンス、是正、アクセス管理。



6	7	12 か月	100
ツールをひとつのポートフォリオで	対応するコンプライアンスフレームワーク	監査ログを保存	ページまでのサイト全体クロール

- ✓ SAML SSO と SCIM
- ✓ OWASP、PCI DSS、WCAG、SOC 2、GDPR
- ✓ 12 か月の監査ログ
- ✓ Slack、Teams、Webhook

目次

01 すべてを見渡す
02 コンプライアンスを示す
03 速く直す
04 アクセスを管理する
05 変化を見逃さない

このページの画面は、架空のデータを使ったデモ企業のものです。

01 · すべてを見渡す

すべてのサイトとリポジトリを一度に

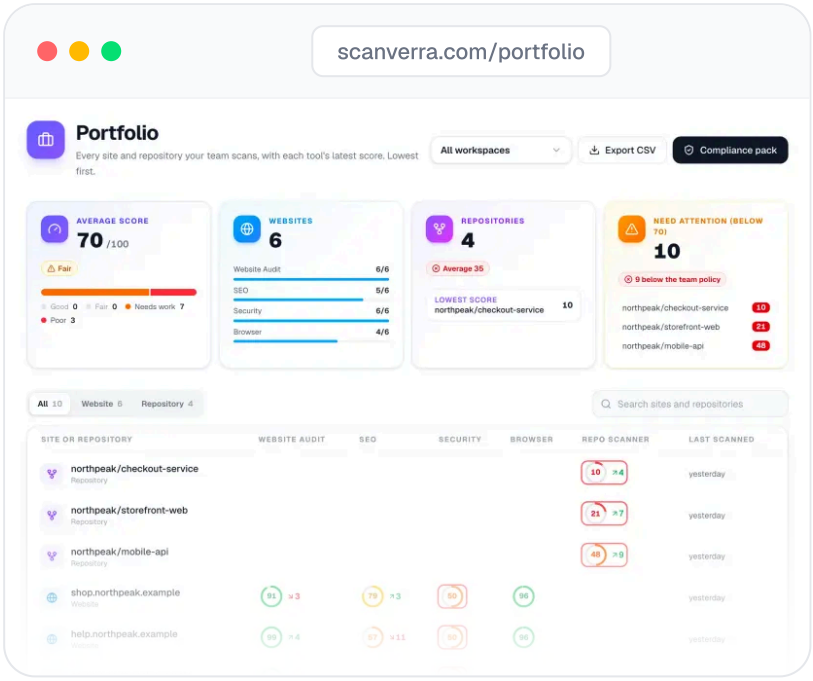
チームが運用するすべてをひとつのビューで。要点だけ知りたい人には週次のサマリーを。

Team と Enterprise

すべてのサイトとリポジトリのポートフォリオ

チームがスキャンするすべての対象を、各ツールの最新スコアと前回からの変化とともに、低い順に表示します。ワークスペースで絞り込んだり、エクスポートしたり、どの数値からでもレポートを開けます。

- ウェブサイト監査、SEO、セキュリティ、ブラウザ監査、リポジトリスキャナーのスコアを並べて表示
- チームのポリシーを下回るものには赤いリング
- コードと本番サイト:実際にデプロイされている脆弱な依存関係
- コード内の AI:全リポジトリのプロバイダー、モデル、MCP サーバー

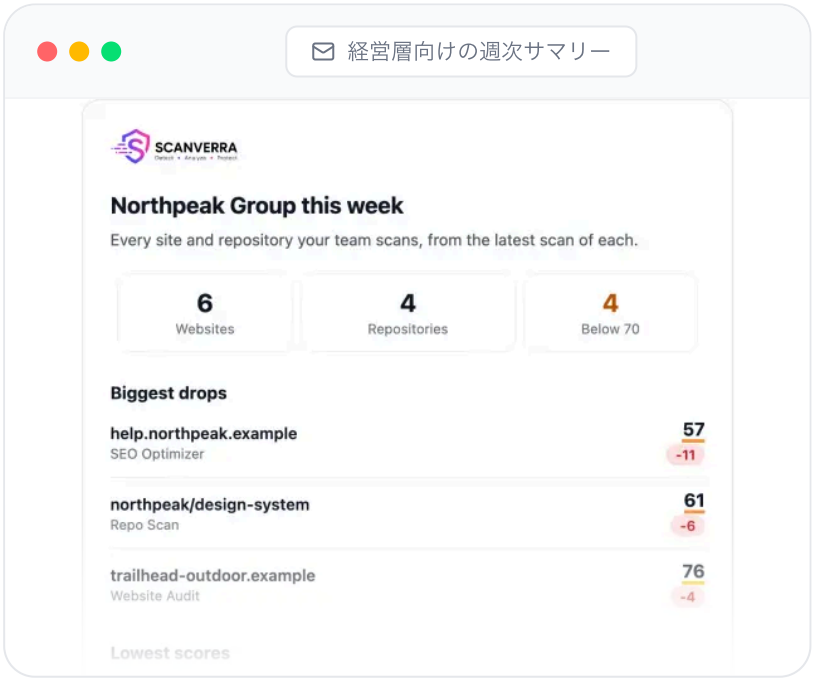


Enterprise

経営層向けの週次サマリー

毎週月曜日、オーナーと管理者に、最も低いスコア、最も大きな低下、ポリシーなしで AI を使っているリポジトリをまとめたメールが届きます。配信停止は一人ずつ設定できます。

- ポートフォリオ全体で最も低いスコアと最も大きな低下
- 最新のリポジトリスキャンから見た AI ポリシーの不足
- 詳細はポートフォリオへのリンクひとつで



02 · コンプライアンスを示す

監査担当者がそのまま使える根拠

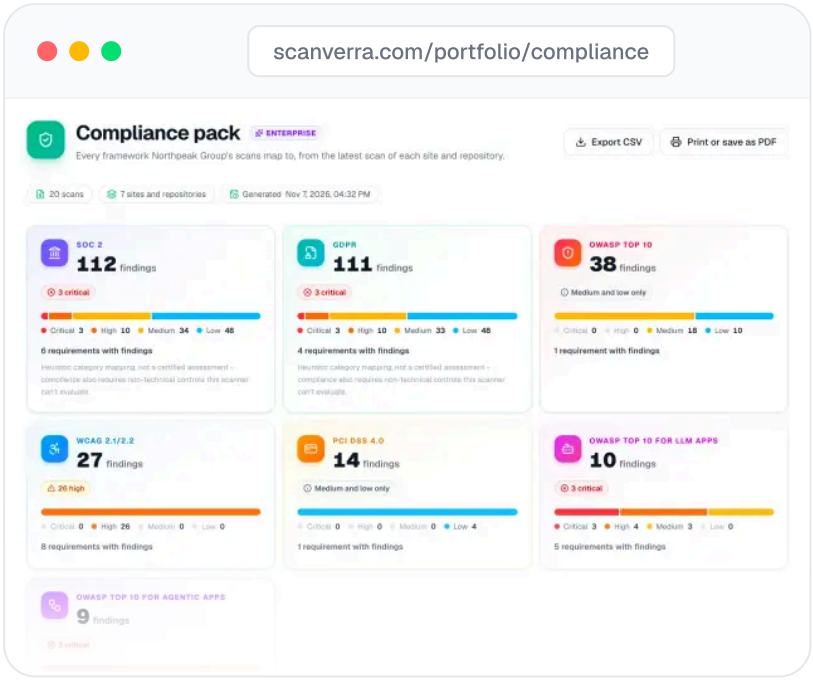
実際のスキャンから得たフレームワーク別の結果と、PCI DSS 4.0 が求めるチェックアウトの監視。

Enterprise

実際のスキャンから作るコンプライアンスパック

OWASP Top 10、PCI DSS 4.0、WCAG 2.1 と 2.2、SOC 2、GDPR、そして LLM・エージェント向けアプリの OWASP リストを、要件ごとに、影響するサイトとリポジトリとともに示します。認証ではなく、作業の根拠となる資料です。

- ✓ 各要件の検出内容、重大度、影響する対象
- ✓ CSV で書き出すか、監査資料用に PDF で保存
- ✓ CycloneDX 1.5 と SPDX 2.3 の SBOM をダウンロード
- ✓ ワークスペースで絞り込み、事業部門ごとのパックに

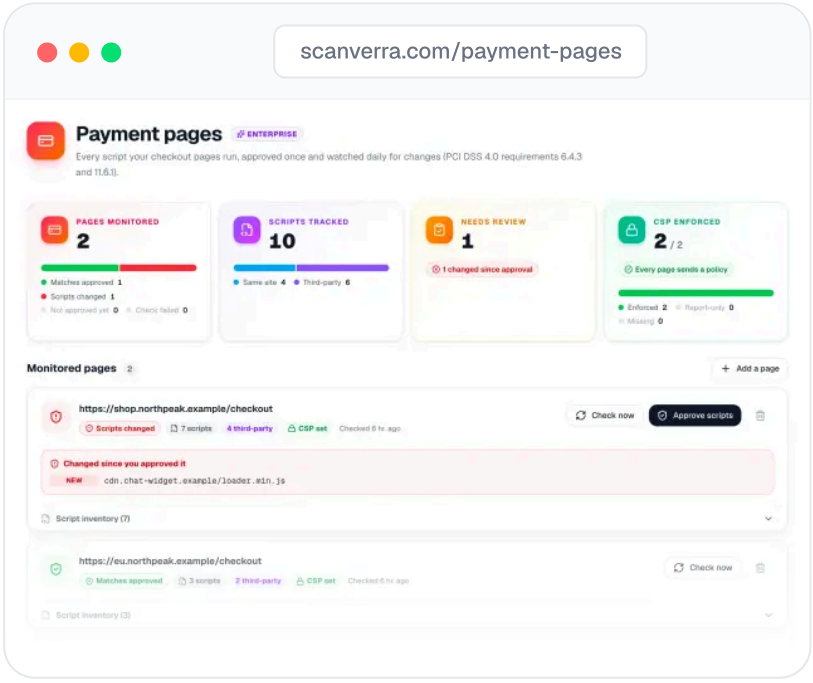


Enterprise

チェックアウトページの PCI DSS 4.0 スクリプト監視

決済ページが実行するすべてのスクリプトを実際のブラウザで記録し、SHA-256 ハッシュと Content-Security-Policy を保存します。一度承認すれば、新しいスクリプトや変更されたスクリプトは翌日に通知されます。

- ✓ 要件 6.4.3 と 11.6.1 に対応
- ✓ サードパーティとインラインのスクリプトを、それぞれハッシュ付きで
- ✓ 保存したログイン情報で、サインインが必要なチェックアウトページにも対応
- ✓ メール、Slack、Microsoft Teams、Webhook で通知



03 · 速く直す

検出から修正まで、担当者付きで

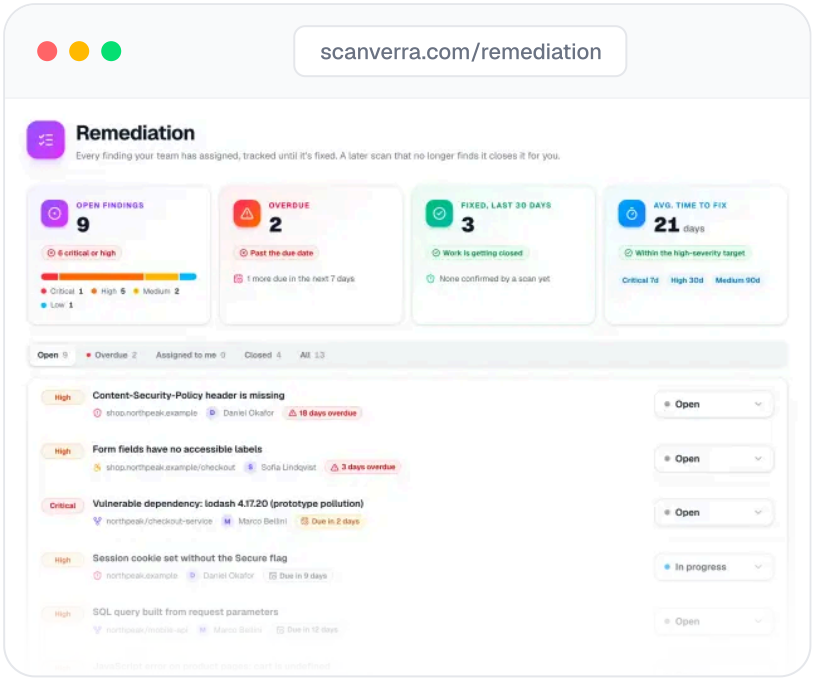
すべての検出に担当者と期限を。リリースしてよい水準はひとつのポリシーで決めます。

Team と Enterprise

検出が担当者と期限付きのタスクに

どのツールの検出でもチームメンバーに割り当てられます。期限は重大度に応じて決まり、担当者にはメールが届き、後のスキャンで問題が見つからなくなればタスクは自動で閉じます。

- 重大度別の期限:致命的 7 日、高 30 日、中 90 日、低 180 日
- 未対応、期限超過、修正済み、修正までの時間がひと目でわかる
- 各タスクからレポート内の該当する検出を直接開ける
- そのスキャンが実行したチェックで確認された場合にのみ閉じる

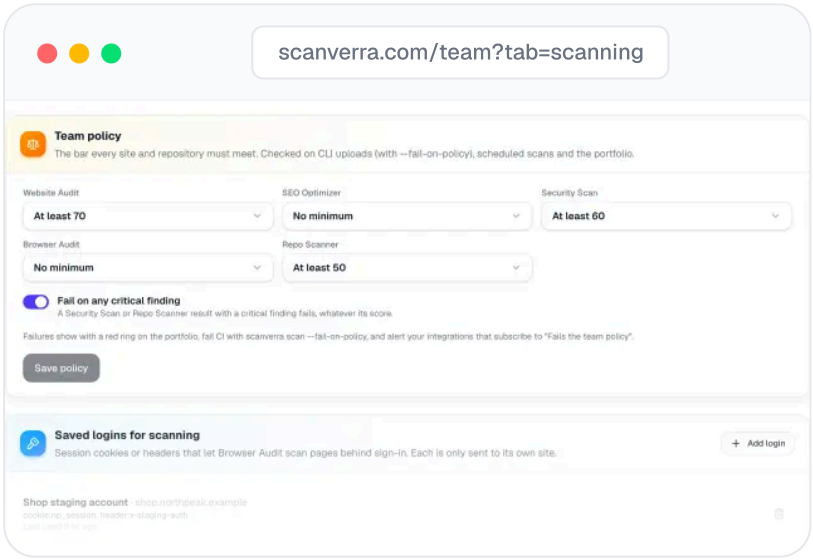


Enterprise

すべてのサイトとリポジトリにひとつの基準

ツールごとの最低スコアを設定し、致命的な検出が 1 つでもあれば不合格にできます。同じポリシーが CI での CLI アップロード、定期スキャン、ポートフォリオで確認されます。

- ツールごとの最低スコア
- scanverra scan --fail-on-policy でビルドを失敗させる
- 定期スキャンがポリシーを満たさないときに通知
- 保存したログイン情報で、ブラウザ監査がサインイン後のページもスキャン



04 · アクセスを管理する

購買部門が求める管理機能

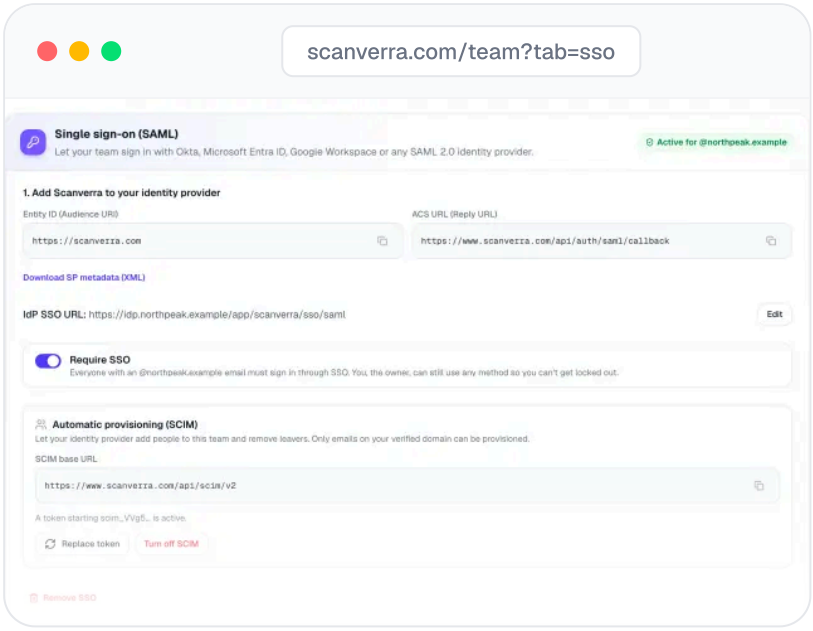
シングルサインオン、プロビジョニング、ロール、ワークスペース、そして誰が何をしたかの記録。

Enterprise

自分で設定できるシングルサインオンとプロビジョニング

Okta、Microsoft Entra ID、Google Workspace などの SAML 2.0 ID プロバイダーを、チームページから接続できます。DNS レコードでドメインの所有を証明し、そのドメインの全員に SSO を必須にできます。

- SSO を必須にしても、オーナー用の代替手段があるので締め出されない
- SCIM 2.0 で ID プロバイダーからメンバーを追加・削除
- プロビジョニングできるのは検証済みドメインのメールだけ
- SAML レスポンスは一度だけ、そのドメインに対してのみ受け付ける

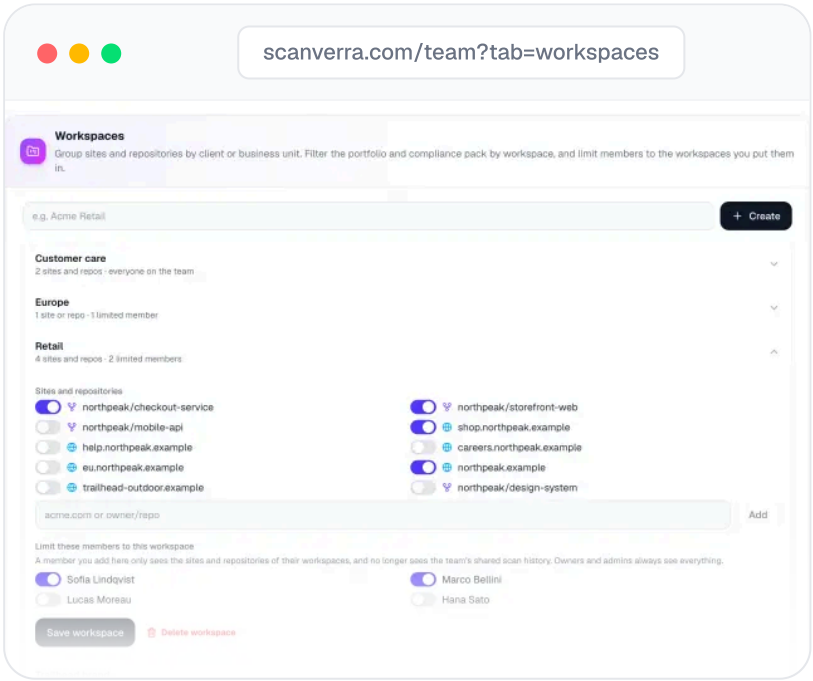


Enterprise

組織図に合わせたワークスペースとロール

サイトとリポジトリを事業部門、ブランド、顧客ごとにまとめ、管理者・メンバー・閲覧者のアクセス権を付与できます。ワークスペースに限定された人は、そのサイトとリポジトリだけを見られます。

- ワークスペースでポートフォリオ、コンプライアンスパック、データエクスポートを絞り込み
- 閲覧者はすべてのレポートを読めるが、有料スキャンの開始や設定変更はできない
- 作成者が退職しても使い続けられるチームの API キー
- パイプラインや BI ツール向けの読み取り専用キーと有効期限

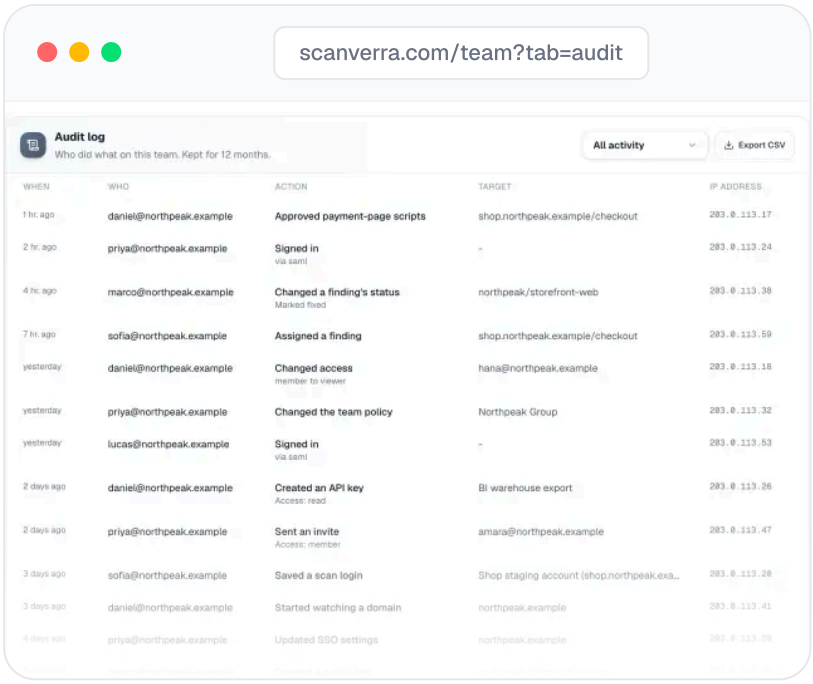


Enterprise

重要な操作をすべて記録する監査ログ

サインイン、招待、アクセス権の変更、API キー、共有リンク、削除されたスキャン、検出の更新、スケジュール、SSO の変更を、誰が、いつ、どこから行ったかとともに記録します。保存期間は 12 か月です。

- アクティビティの種類で絞り込み
- 記録用に CSV でエクスポート
- API キーを使って SIEM から読み取り
- すべてのイベントに IP アドレスとブラウザ



05 · 変化を見逃さない

新しいものが現れたらすぐわかる

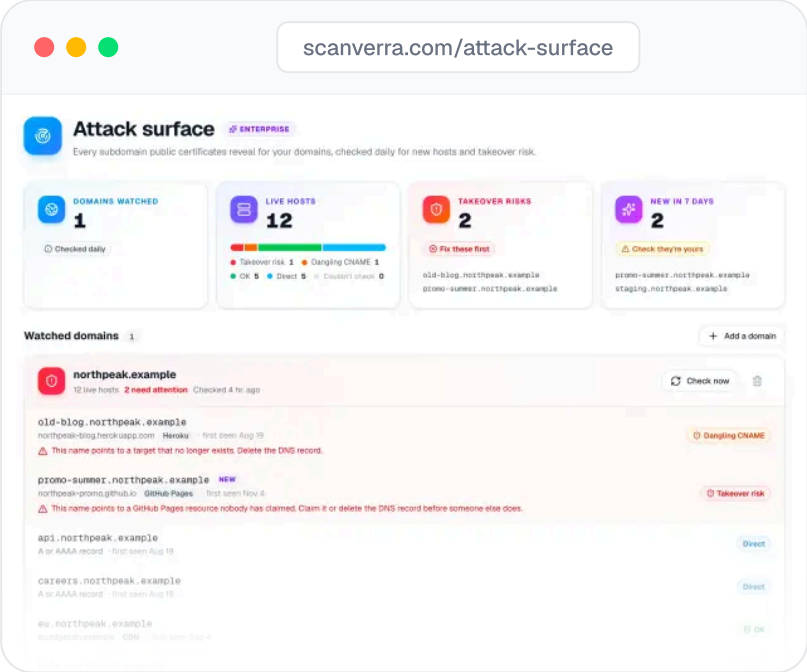
忘れられたサブドメインを毎日、AI アシスタントがブランドをどう語るかを毎週チェックします。

Enterprise

忘れていたサブドメインを見つける

Scanverra はドメインの公開証明書ログを毎日読み取り、各サブドメインの乗っ取りリスクと宙に浮いた DNS をチェックし、新しいホストが現れたら知らせます。

- GitHub Pages や Heroku などのホスティングサービスの乗っ取りチェック
- 宙に浮いた CNAME レコードを、対処方法とともに警告
- 新しいホストと新しいリスクの通知
- DNS から消えたホストも履歴として保持

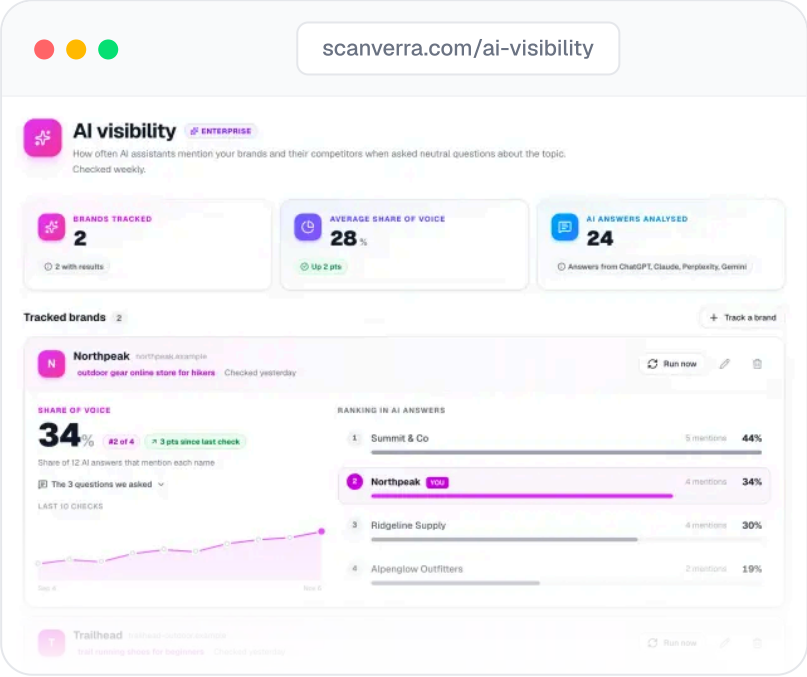


Enterprise

AI の回答におけるシェア・オブ・ボイス

購入を検討する人が市場について中立的な質問をしたとき、AI アシスタントが自社ブランドと競合をどれだけ挙げるかを追跡します。各ブランドは毎週チェックされ、推移と順位がわかります。

- 複数のブランドを、それぞれのトピックと最大 5 社の競合とともに
- あなたに一切触れない、購入者目線の中立的な質問
- 同じ回答から競合と比べた順位
- 実際に尋ねた質問を、各結果の横に表示



大きなチームに必要なその他の機能

Slack、Microsoft Teams、Webhook

スコアの低下、ポリシー違反、決済ページの変更、新しいホストを、チームがすでに使っている場所へ送ります。Webhook は HMAC-SHA256 で署名されます。

データ管理

公開レポートリンクを無効にし、チーム全体で AI をオフにしてスキャンデータがモデルに届かないようにし、スキャン履歴の保存期間を 30・90・180・365 日から選べます。

ホワイトラベルのレポート

PDF レポートと、Web サイトのレポートの共有リンクに、自社の名前・ロゴ・色を表示。Scanverra の表記は任意です。

チームの API キーとデータエクスポート

チームが所有するキーに読み取り専用の権限と有効期限を設定でき、すべてのスキャンを CSV・NDJSON・JSON でデータウェアハウスに取り込めます。

セルフマネージドの GitLab にも対応

gitlab.com とセルフマネージドの GitLab のリポジトリをスキャンし、修正のマージリクエストを作成できます。GitHub、Bitbucket、Azure DevOps にも対応しています。

サイト全体の監視

1 サイトあたり最大 100 ページの定期 SEO クロールを、ほかの定期スキャンと同じくスコア化して通知します。

10 シート、追加はご相談ください

チーム全員に管理者・メンバー・閲覧者のアクセス権、専任のアカウントマネージャー、優先サポート。

定期スキャンは無制限

すべてのサイトとリポジトリを毎日・毎週・毎月スキャンし、スコアが下がったら通知します。

導入検討時によくいただく質問

Enterprise には何が含まれますか?

Team のすべての機能に加えて、SSO と SCIM、監査ログ、ワークスペース、コンプライアンスパック、チームポリシー、データ管理、ホワイトラベルのレポート、アタックサーフェスと決済ページの監視、複数ブランドの AI での可視性、チームの API キー、週次のエグゼクティブサマリーが含まれます。

Enterprise の料金はどう決まりますか?

Enterprise はボリューム価格によるカスタム契約です。サイト、リポジトリ、利用人数をお知らせいただければ、お見積もりをお送りします。

SSO に対応している ID プロバイダーは?

Okta、Microsoft Entra ID、Google Workspace を含む、あらゆる SAML 2.0 ID プロバイダーに対応しています。SCIM 2.0 のプロビジョニングは Okta と Microsoft Entra ID で使えます。

コンプライアンスパックは認証ですか?

いいえ。自動検出の結果を各フレームワークの要件に対応付け、作業の根拠となる資料を提供します。認証には、スキャナーでは確認できないプロセスやポリシーの管理も必要です。

データを AI モデルに送らないようにできますか?

はい。チームで AI をオフにすると、スキャンデータは AI モデルに送信されません。スコアと検出結果はそのまま使え、AI による要約、修正、チャットはオフになります。

サインインが必要なページや、プライベートネットワーク上のサイトもスキャンできますか?

ブラウザ監査と決済ページのチェックでは、保存したログイン情報を使ってサインイン後のページをスキャンできます。社内ネットワークからしかアクセスできないサイトは、まだスキャンできません。

お問い合わせ

サイト、リポジトリ、チームについてお聞かせください。プランとお見積もりをご連絡します。

メール
support@scanverra.com

WEB
www.scanverra.com/ja/enterprise