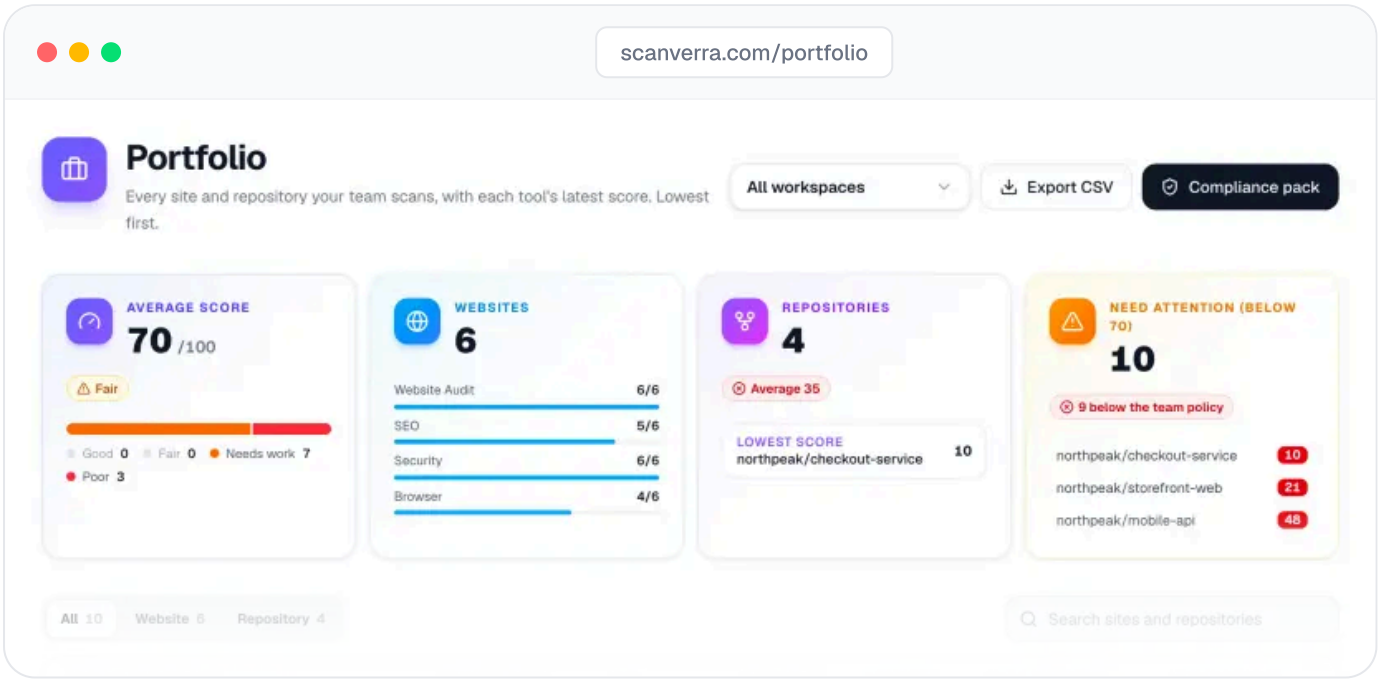
SCANVERRA
Detect • Analyze • Protect

SCANVERRA ENTERPRISE

Apresentação do Scanverra Enterprise

Portfólio, conformidade, correções e controles de acesso para todos os seus sites e repositórios.



6	7	12 meses	100
ferramentas em um portfólio	frameworks de conformidade mapeados	de log de auditoria	páginas por rastreamento do site

- ✓ SAML SSO e SCIM
- ✓ OWASP, PCI DSS, WCAG, SOC 2, GDPR
- ✓ Log de auditoria de 12 meses
- ✓ Slack, Teams e webhooks

CONTEÚDO

01 Ver tudo
02 Comprovar conformidade
03 Corrigir mais rápido
04 Controlar o acesso
05 Acompanhar mudanças

As telas desta página mostram uma empresa de demonstração com dados fictícios.

01 · VER TUDO

Todos os seus sites e repositórios de uma vez

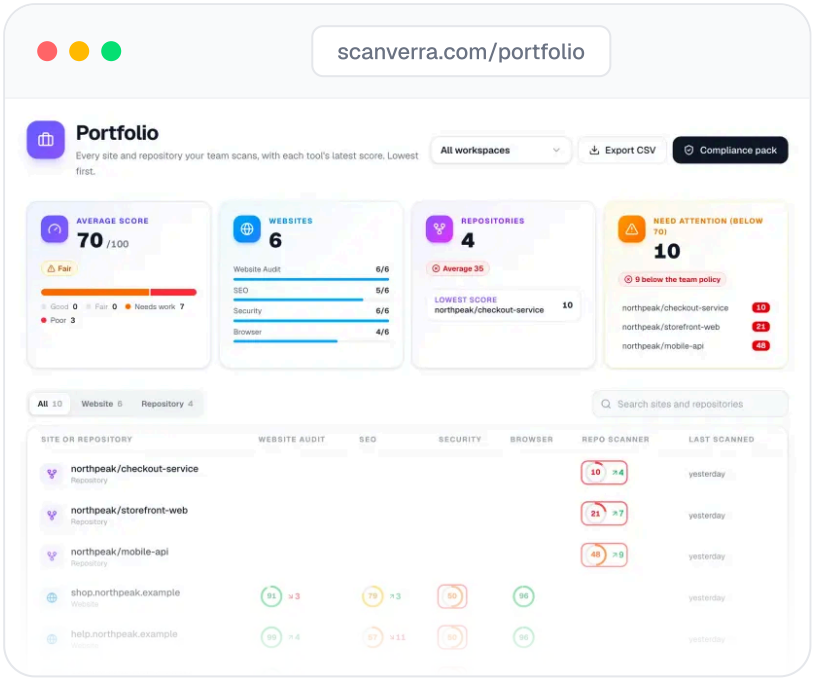
Uma visão de tudo o que suas equipes mantêm, e um resumo semanal para quem só precisa do essencial.

Team e Enterprise

Um portfólio de todos os seus sites e repositórios

Cada alvo que sua equipe varre, com a pontuação mais recente de cada ferramenta e a variação desde a última varredura, do pior para o melhor. Filtre por workspace, exporte ou abra o relatório por trás de cada número.

- Pontuações de Auditoria de site, SEO, Segurança, Auditoria de navegador e Scanner de repositório lado a lado
- Um anel vermelho em tudo o que está abaixo da política da sua equipe
- Código e site no ar: dependências vulneráveis que estão de fato implantadas
- IA no seu código: provedores, modelos e servidores MCP em todos os repositórios

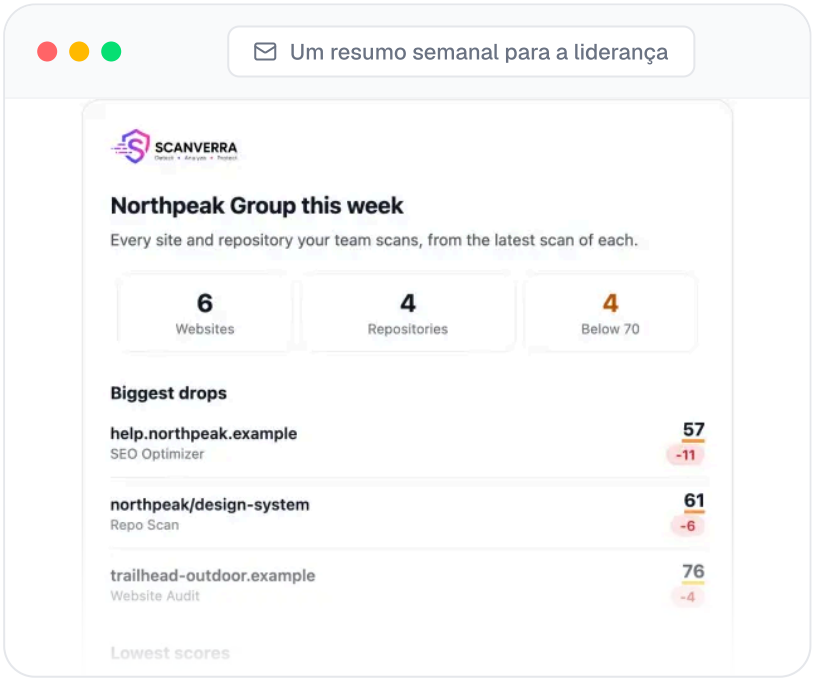


Enterprise

Um resumo semanal para a liderança

Toda segunda-feira, proprietários e administradores recebem um e-mail com as menores pontuações, as maiores quedas e os repositórios que usam IA sem uma política. Cada pessoa pode cancelar a inscrição por conta própria.

- Menores pontuações e maiores quedas em todo o portfólio
- Lacunas de política de IA a partir das últimas varreduras de repositórios
- Um link de volta ao portfólio para ver os detalhes



02 · COMPROVAR CONFORMIDADE

Evidências com que seu auditor pode trabalhar

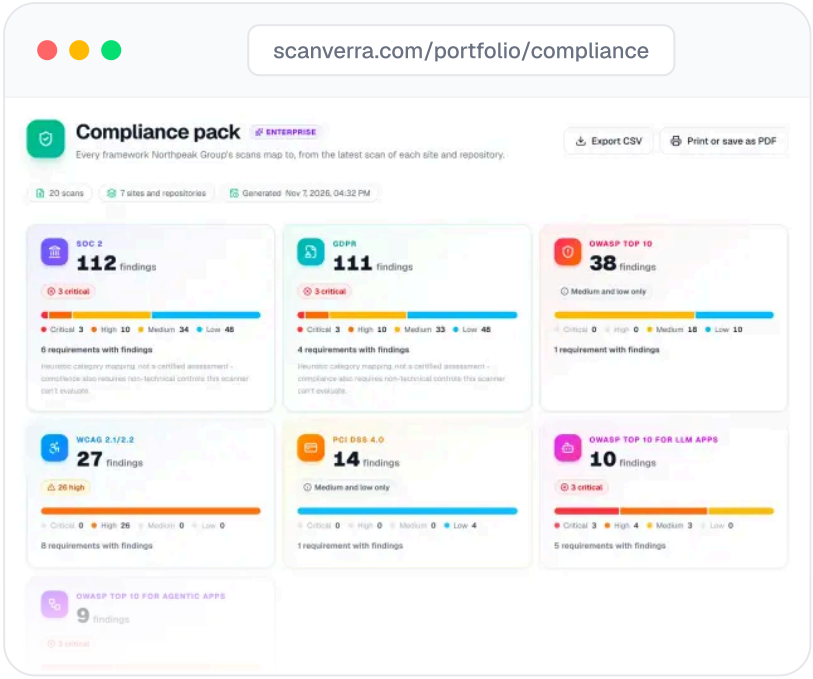
Resultados por framework a partir das suas varreduras reais, e o monitoramento do checkout que o PCI DSS 4.0 exige.

Enterprise

Um pacote de conformidade feito a partir das suas varreduras reais

OWASP Top 10, PCI DSS 4.0, WCAG 2.1 e 2.2, SOC 2, GDPR e as listas da OWASP para apps de LLM e agentes, requisito por requisito, com os sites e repositórios afetados. É uma evidência para trabalhar, não uma certificação.

- Cada requisito com seus achados, sua gravidade e os alvos afetados
- Exporte para CSV ou salve como PDF para o dossiê de auditoria
- Downloads de SBOM em CycloneDX 1.5 e SPDX 2.3
- Filtre por workspace para dar a cada unidade de negócio seu próprio pacote

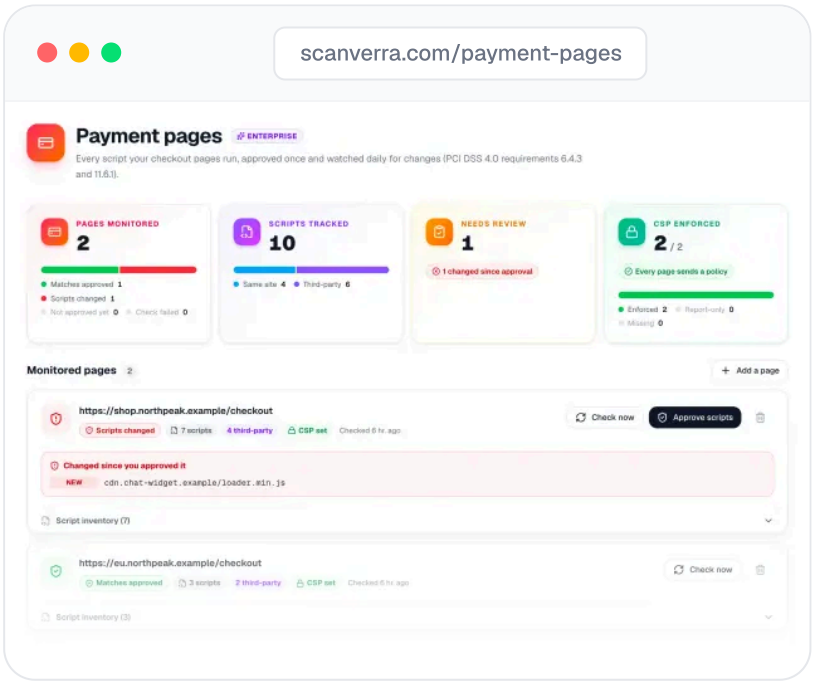


Enterprise

Monitoramento de scripts PCI DSS 4.0 para páginas de checkout

Cada script que suas páginas de pagamento executam é registrado em um navegador real, com seu hash SHA-256 e sua Content-Security-Policy. Aprove a lista uma vez, e qualquer script novo ou alterado é sinalizado no dia seguinte.

- Feito para os requisitos 6.4.3 e 11.6.1
- Scripts de terceiros e inline, cada um com seu hash
- Páginas de checkout que exigem login, com um acesso salvo
- Alertas por e-mail, Slack, Microsoft Teams ou seu webhook



03 · CORRIGIR MAIS RÁPIDO

Do achado à correção, com um responsável

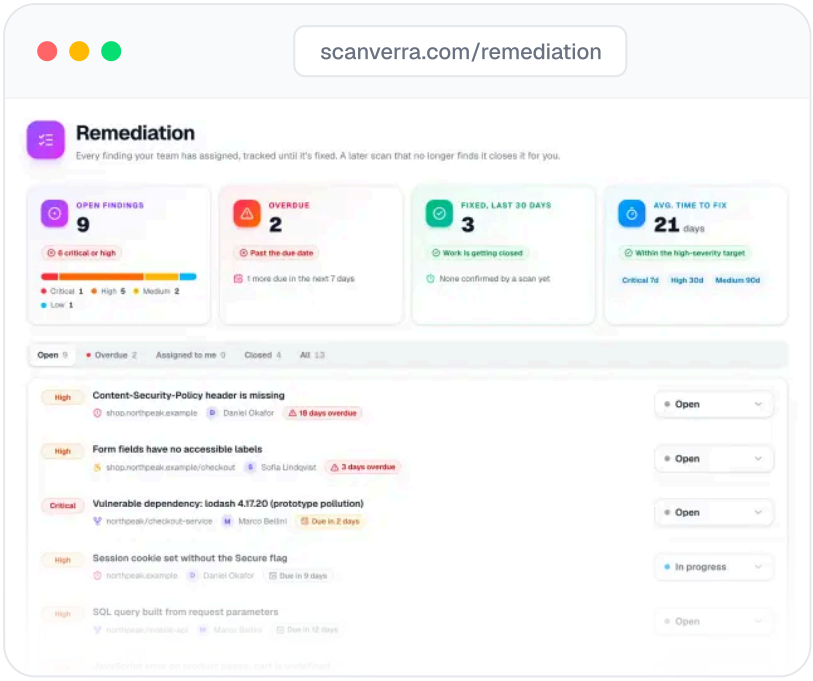
Cada achado tem uma pessoa e um prazo, e uma política decide o que está bom o bastante para ir ao ar.

Team e Enterprise

Achados viram tarefas com responsáveis e prazos

Atribua qualquer achado de qualquer ferramenta a um colega. O prazo segue a gravidade, a pessoa recebe um e-mail e uma varredura posterior que não encontra mais o problema encerra a tarefa para você.

- Prazos por gravidade: crítico 7 dias, alto 30, médio 90, baixo 180
- Abertos, atrasados, corrigidos e tempo de correção num relance
- Cada tarefa abre o achado exato no seu relatório
- Encerrada só quando uma varredura confirma, para as verificações que ela executou

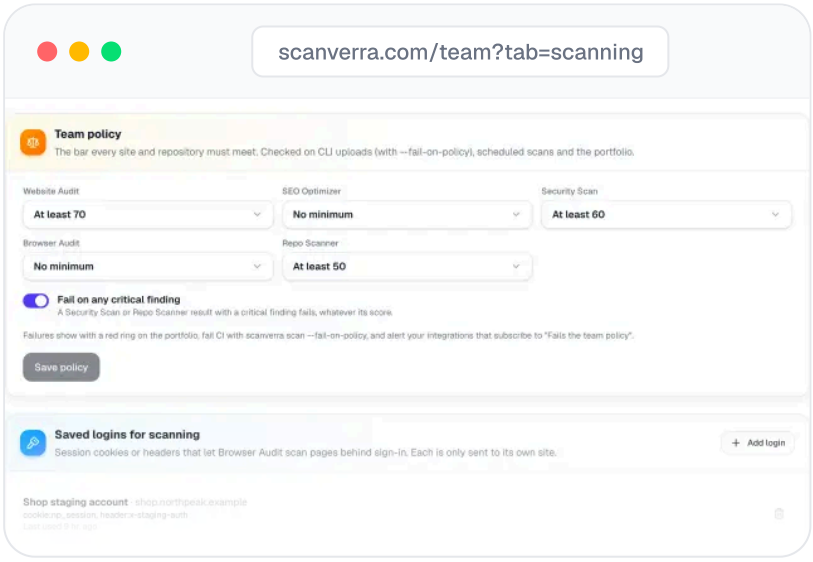


Enterprise

Uma régua para cada site e repositório

Defina a pontuação mínima de cada ferramenta e reprove direto qualquer achado crítico. A mesma política é verificada nos envios da CLI em CI, nas varreduras agendadas e no portfólio.

- Uma pontuação mínima por ferramenta
- Faça o build falhar com scanverra scan --fail-on-policy
- Um alerta quando uma varredura agendada não cumpre a política
- Acessos salvos para a Auditoria de navegador varrer páginas que exigem login



04 · CONTROLAR O ACESSO

Os controles que o setor de compras pede

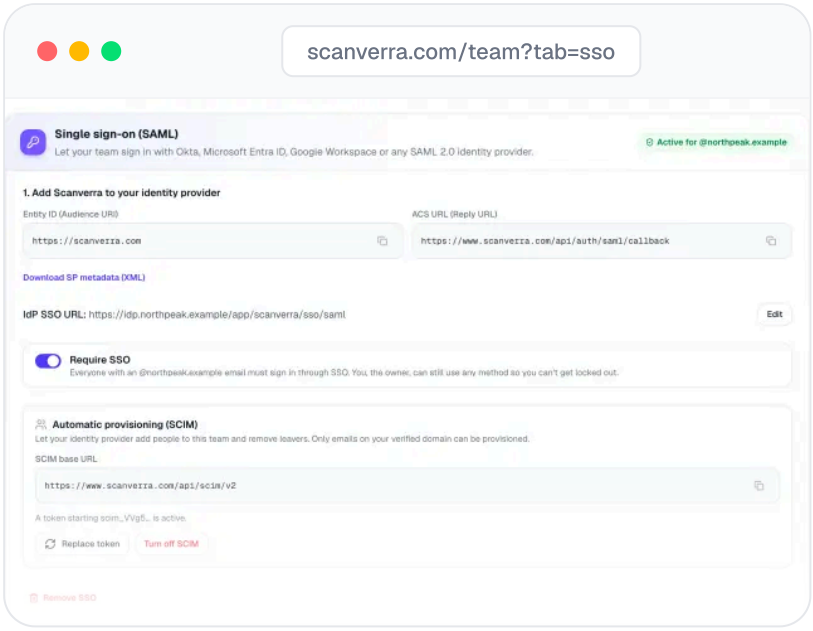
Login único, provisionamento, papéis, workspaces e um registro de quem fez o quê.

Enterprise

Login único e provisionamento configurados por você

Conecte Okta, Microsoft Entra ID, Google Workspace ou qualquer provedor de identidade SAML 2.0 pela página da equipe. Comprove que o domínio é seu com um registro DNS e exija SSO de todos que o usam.

- Exija SSO, com um acesso de reserva para o proprietário para você nunca ficar trancado do lado de fora
- O SCIM 2.0 adiciona e remove membros a partir do seu provedor de identidade
- Só e-mails do seu domínio verificado podem ser provisionados
- Cada resposta SAML é aceita uma única vez e só para o próprio domínio

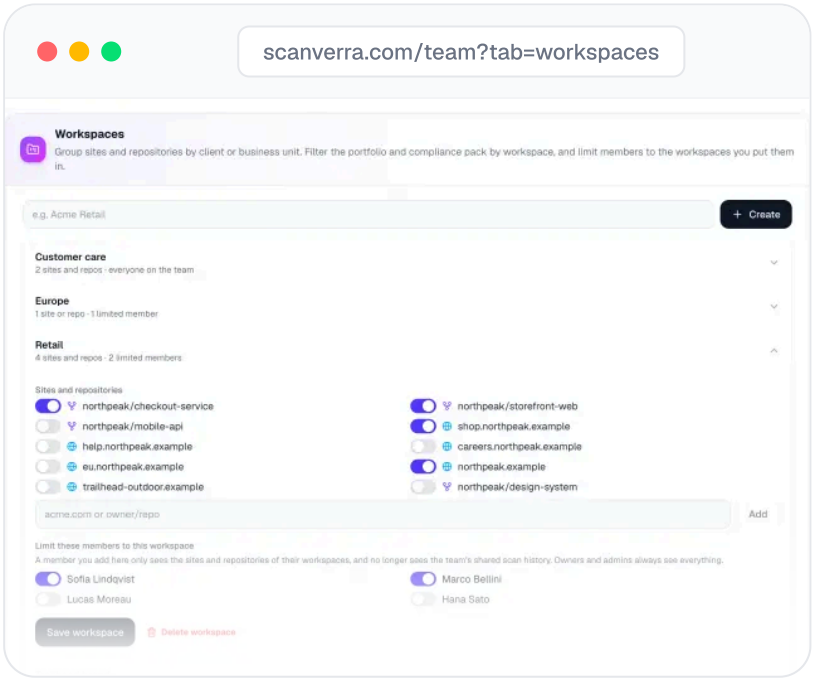


Enterprise

Workspaces e papéis que seguem seu organograma

Agrupe sites e repositórios por unidade de negócio, marca ou cliente, e dê acesso de Administrador, Membro ou Leitor. Quem está limitado a um workspace vê só os sites e repositórios dele.

- Workspaces filtram o portfólio, o pacote de conformidade e a exportação de dados
- Leitores veem todos os relatórios, mas não iniciam varreduras pagas nem mudam configurações
- Chaves de API da equipe que continuam funcionando quando quem as criou sai
- Chaves somente leitura e datas de expiração para pipelines e ferramentas de BI

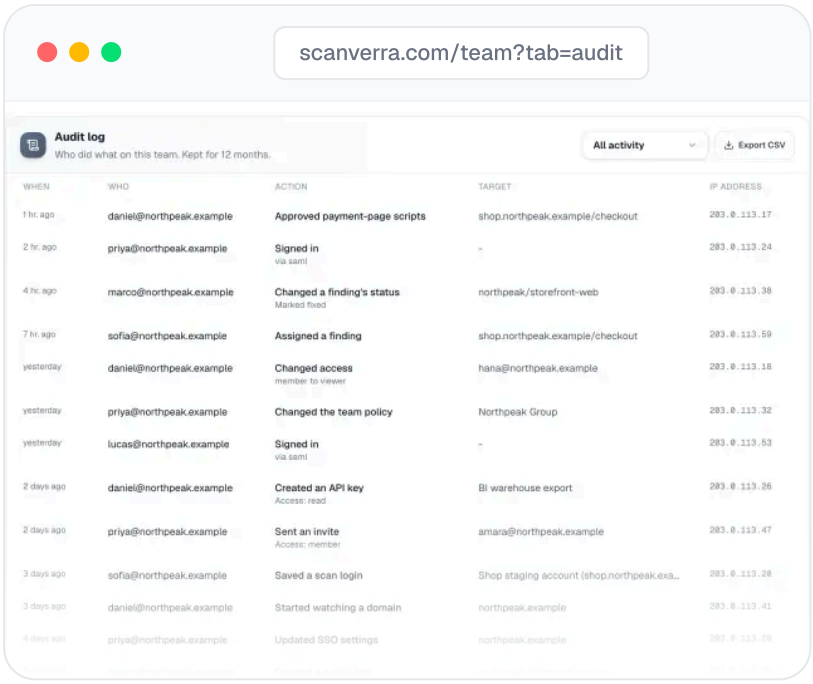


Enterprise

Um log de auditoria para tudo o que importa

Logins, convites, mudanças de acesso, chaves de API, links compartilhados, varreduras excluídas, atualizações de achados, agendamentos e mudanças de SSO, com quem fez, quando e de onde. Guardado por 12 meses.

- Filtre por tipo de atividade
- Exporte para CSV para seus registros
- Leia a partir do seu SIEM com uma chave de API
- Endereço IP e navegador em cada evento



05 · ACOMPANHAR MUDANÇAS

Saiba quando algo novo aparece

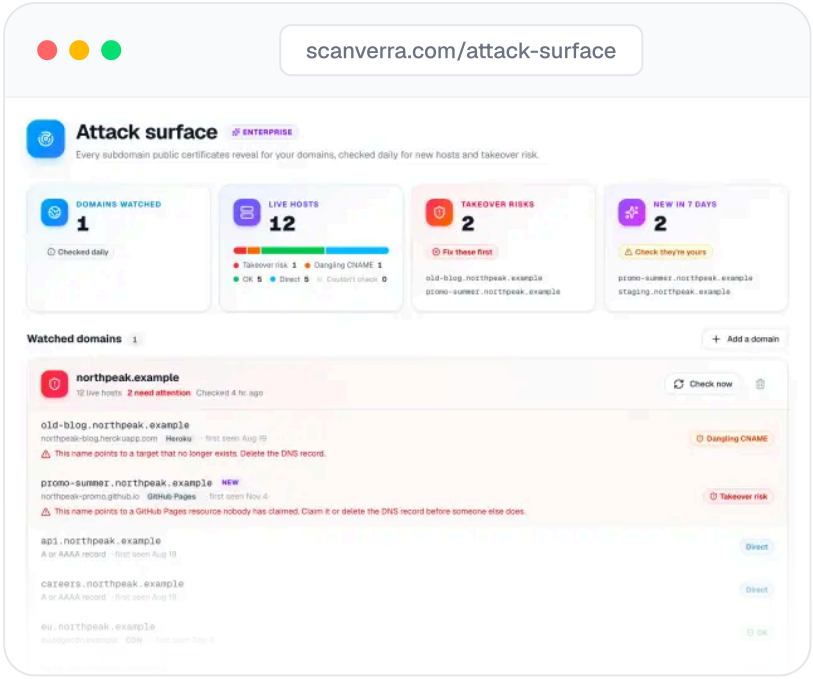
Verificações diárias de subdomínios esquecidos e semanais de como os assistentes de IA falam das suas marcas.

Enterprise

Encontre os subdomínios que você esqueceu

A Scanverra lê todo dia os logs públicos de certificados dos seus domínios, verifica em cada subdomínio o risco de sequestro e DNS pendente, e avisa quando aparece um host novo.

- Verificação de sequestro para serviços de hospedagem como GitHub Pages e Heroku
- Registros CNAME pendentes sinalizados, com o que fazer
- Alertas de hosts novos e de novos riscos
- Hosts que saíram do DNS ficam guardados como histórico

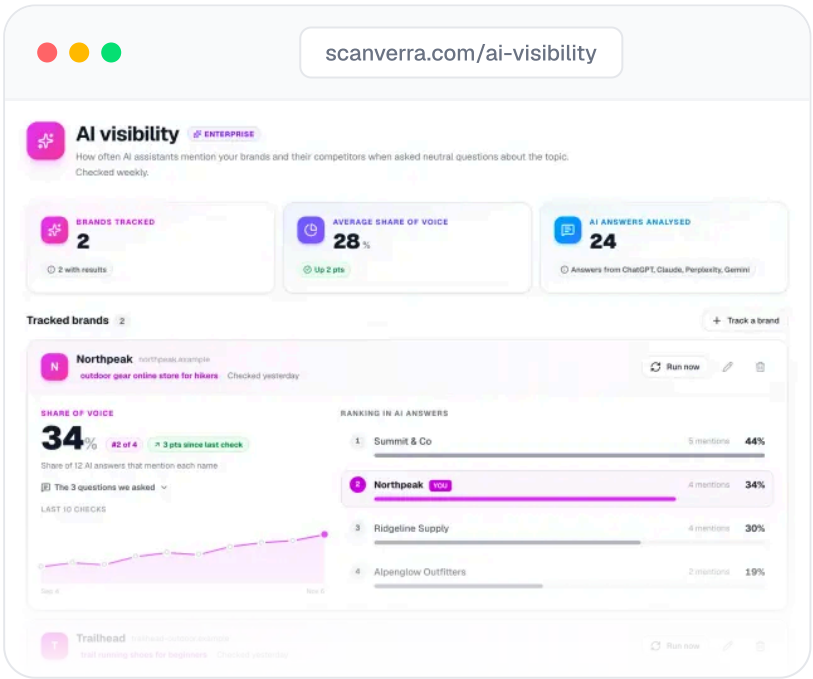


Enterprise

Sua participação nas respostas da IA

Acompanhe com que frequência os assistentes de IA citam suas marcas e seus concorrentes quando compradores fazem perguntas neutras sobre o seu mercado. Cada marca é verificada toda semana, com tendência e posição.

- Várias marcas, cada uma com seu tema e até 5 concorrentes
- Perguntas neutras, como as de um comprador, que nunca citam você
- Posição frente aos concorrentes a partir das mesmas respostas
- As perguntas feitas, exibidas ao lado de cada resultado



E tudo o mais que uma equipe maior precisa

Slack, Microsoft Teams e webhooks

Quedas de pontuação, falhas de política, mudanças em páginas de pagamento e hosts novos, enviados para onde sua equipe já trabalha. Os webhooks são assinados com HMAC-SHA256.

Controles de dados

Desative links públicos de relatórios, desligue a IA para toda a equipe para que nenhum dado de varredura chegue a um modelo e guarde o histórico por 30, 90, 180 ou 365 dias.

Relatórios white-label

Seu nome, logotipo e cor nos relatórios em PDF e nos links compartilhados de relatórios de sites, com o crédito da Scanverra opcional.

Chaves de API da equipe e exportação de dados

Chaves que pertencem à equipe, com escopo somente leitura e datas de expiração, e um feed em CSV, NDJSON ou JSON de cada varredura para seu data warehouse.

GitLab, inclusive autogerenciado

Varra repositórios do gitlab.com e de GitLab autogerenciado e abra merge requests com correções, junto com GitHub, Bitbucket e Azure DevOps.

Monitoramento do site inteiro

Rastreamentos de SEO agendados de até 100 páginas por site, pontuados e com alertas como qualquer varredura agendada.

10 assentos, mais sob consulta

Acesso de Administrador, Membro e Leitor para toda a equipe, um gerente de conta dedicado e suporte prioritário.

Varreduras agendadas ilimitadas

Varreduras diárias, semanais ou mensais de cada site e repositório, com um alerta quando uma pontuação cai.

O que os compradores costumam perguntar

O que o Enterprise inclui?

Tudo do Team, mais SSO e SCIM, o log de auditoria, workspaces, o pacote de conformidade, a política da equipe, controles de dados, relatórios white-label, monitoramento da superfície de ataque e das páginas de pagamento, visibilidade em IA para várias marcas, chaves de API da equipe e o resumo executivo semanal.

Como o Enterprise é cobrado?

O Enterprise é um contrato sob medida com preços por volume. Conte quantos sites, repositórios e pessoas você tem, e enviaremos uma proposta.

Quais provedores de identidade funcionam com SSO?

Qualquer provedor de identidade SAML 2.0, incluindo Okta, Microsoft Entra ID e Google Workspace. O provisionamento SCIM 2.0 funciona com Okta e Microsoft Entra ID.

O pacote de conformidade é uma certificação?

Não. Ele relaciona achados automáticos aos requisitos de cada framework, para você ter evidências com que trabalhar. Uma certificação também exige controles de processo e de política que nenhum scanner consegue verificar.

Podemos manter nossos dados longe de modelos de IA?

Sim. Com a IA desligada para a equipe, nenhum dado de varredura é enviado a um modelo de IA. Pontuações e achados continuam funcionando; resumos, correções e chat com IA ficam desligados.

Vocês varrem páginas que exigem login ou sites em uma rede privada?

A Auditoria de navegador e as verificações de páginas de pagamento podem usar um acesso salvo para páginas que exigem login. Sites acessíveis só dentro da sua própria rede ainda não podem ser varridos.

Fale com a gente

Conte sobre seus sites, repositórios e equipe, e voltaremos com um plano e uma proposta.

E-MAIL
support@scanverra.com

SITE
www.scanverra.com/pt/enterprise