DATASHEET

AI APPGEN SECURITY: SECURE THE APPS THAT SKIP YOUR PIPELINE

AI AppGen covers the apps published outside your pipeline: no ticket, no code review, no CI gate, no security sign-off. A prompt in Base44 or a deploy to Vercel comes with a database, a secret store and a public URL. Orca connects the platform the app runs on, the data behind it and the cloud account under it, so your team fixes the exposed app that actually reaches customer data, without adding another point tool.

Key challenges

AI turned every employee into a builder, and the platforms they ship on sit outside the controls security owns. Verizon's 2026 DBIR ranks shadow AI as the third most common non-malicious insider action, up 4x in a year (Verizon, 2026).

Apps ship with no record anywhere. A builder prompts an app and hits publish, and no step creates an inventory entry. One scan found 380,000 public assets on Lovable, Base44, Replit and Netlify, about 5,000 of them holding sensitive corporate data (RedAccess, 2026).

Generators pick insecure defaults. New apps, preview URLs and production deployments are often public without login. In Orca's testing, a new Base44 workspace makes every new app public by default.

The database sits open behind a public key. Generated apps ship the backend's client key in the browser and skip row-level security. In CVE-2025-48757, 303 endpoints across 170 Lovable projects exposed names, emails, payment data and API keys to anyone (Superblocks, 2025).

Platform settings grant more than anyone reviewed. SSO is configured but not enforced, owner roles pile up, tokens never expire and contractors get added by hand. None of it shows up in your identity provider's access reviews.

One app spans five vendors. The model, the AppGen platform, the backend, the hosting platform and the cloud account each have a different owner, and none of them is security.

Point tools see one fragment. SSE and browser tools see who opened the AI platform, not what they published. Agent and platform security tools see the app, not the cloud account, identity and data underneath it.

Benefits at a glance

- **Find shadow AppGen:** see which AppGen platforms, hosting and backend services your teams use, including ones nobody approved
- **Posture where AppGen risk starts:** identity, exposure and data-handling misconfigurations on AppGen platforms like Base44, Vercel, Claude Enterprise and ChatGPT Enterprise
- **Context, not just findings:** know whether an exposed app is public, holds plaintext secrets, or keeps prompts and files indefinitely
- **One place for AppGen, cloud, and code security:** AppGen findings join your code and cloud environments in the Unified Data Model and existing workflows
- **Builders keep building:** discover AppGen services in your code and cloud environments, then secure each platform without disrupting builders
- **A named owner on every app:** each finding is tied to the person and workspace that created it

> ***Many organizations still struggle to discover what's been built and where it runs. Now that building is no longer confined to engineering, discovery has to start from what these AI-generated apps leave behind in the environment, not from the builder declaring anything."***

GRACE TRINIDAD
Research Director, IDC

©2026 ORCA SECURITY. ALL RIGHTS RESERVED.

Make AI AppGen security actionable with Orca

See what builders shipped, without chasing them. Every project, deployment, domain, token and member on connected platforms, tied to the person who built it.

Find the app that's open to the internet. Orca classifies each Vercel project as public-facing, restricted or closed, without being fooled by login pages.

Catch secrets before someone else does. Plaintext secret-like environment variables, unprotected source maps and fork builds that can read project secrets.

Close the identity gaps on AI platforms. Unenforced SSO, excess owners, stale or non-expiring tokens, and users added outside SCIM.

Control where prompts and files go. Alerts on indefinite retention, disabled redaction, training opt-in and org-wide public projects in Claude Enterprise.

Fix the risky app first. AppGen findings are scored with the same risk model as the rest of your cloud.

One platform, one data model. AppGen findings share the Unified Data Model with your cloud and flow into the alerts, ticketing and compliance reports you already use.

Approve apps instead of blocking them. Security gets enough context to say yes, and builders keep the tools they picked.

Orca capabilities

Orca covers the five parts every AI-generated app has: the model, the AppGen platform, the backend, the hosting platform and the cloud account. All five land in one Unified Data Model.

MODELS	**Claude Enterprise posture** Catch owner sprawl, unenforced SSO, indefinite retention, training opt-in and public projects	**ChatGPT Enterprise posture** Inventory users, groups and service accounts, and flag excess owners, non-expiring credentials and users added outside SCIM	**DSPM for AI platforms** Find sensitive data in Claude Enterprise and ChatGPT Enterprise projects and files
APPGEN PLATFORMS	**Shadow AppGen discovery** Discover AppGen platforms like Lovable, v0 and Base44 from the traces they leave in your code and cloud	**Base44 posture** Flag public apps, anonymous data access, admins without MFA and weak workspace guardrails	
BACKEND AND HOSTING	**Supabase posture** Check row-level security coverage, exposed service-role keys and auth settings on the databases AppGen tools create	**Vercel posture** Inventory teams, tokens, projects, deployments and domains, and catch edge, identity and data risks	**Internet-exposure analysis** Classify each Vercel project as public-facing, internet-facing (restricted) or closed
CLOUD	**AI security posture** Find the cloud AI services AppGen apps call and flag exposure and over-privileged roles	**AI secrets detection** Find OpenAI, Anthropic and other AI provider keys across repositories, including code AppGen tools sync to GitHub	

Specifications

Area	Supported
Enterprise AI assistants	Claude Enterprise, ChatGPT Enterprise
AppGen platforms and hosting	Lovable, v0, Bolt, Base44, Replit, Vercel, Netlify, Supabase
Cloud providers	AWS, Azure, Google Cloud, Oracle Cloud, Alibaba Cloud and Tencent Cloud
Managed AI services	Amazon Bedrock, Amazon SageMaker, Azure OpenAI, Azure AI Foundry and Google Vertex AI
Source code management	GitHub, GitLab, Azure DevOps and Bitbucket
Deployment	Agentless and read-only: API connections to each AI platform, AppGen platform and hosting provider, plus SideScanning™ with read-only cloud access, in SaaS, in-account or private mode
Security and data handling	Certifications, data handling and privacy practices are published in the Orca Trust Center

About Orca

Orca Security delivers security for the companies that build. As cloud, code, AI and app generation expand the attack surface, Orca transforms security risk into the context teams need to act. The Orca Platform provides complete visibility across cloud, AI, and application environments, correlates risk across every layer, and prioritizes the exposures that matter most so organizations can remediate faster and innovate with confidence. Trusted by hundreds of organizations, including SAP, Autodesk, Gannett, Lemonade, and Digital Turbine, Orca is backed by leading investors including Temasek, CapitalG, ICONIQ Capital, and Redpoint Ventures. Learn more at orca.security and book a personalized demo.

Ready to see what your builders shipped?
Sign up for a demo. Visit orca.security/demo

©2026 ORCA SECURITY. ALL RIGHTS RESERVED.