SIX SENSE SOLUTIONS

The security primitives API for teams that get audited

hello@sixsensesolutions.net
www.sixsensesolutions.net
(202) 531-0660

If it is not captured at creation time, it does not exist for auditors.

THE PROBLEM

Most teams generate credentials correctly. They use the right functions, enforce complexity, rotate on schedule. But when an auditor asks for proof of what was true at the moment a specific credential was created, they have nothing.

Manual reconstruction of credential evidence fails under audit. Auditors want proof of what happened, not an explanation of what you think happened.

OUR SOLUTION

Six Sense Solutions generates cryptographically secure credentials and produces machine-readable audit evidence in the same API call. The evidence exists at creation time, automatically, with no additional documentation step.

FOUR ENDPOINTS. ONE INTEGRATION.

POST /v1/generate

Cryptographically secure credentials with entropy bits, compliance profile, and generation timestamp in every response. NIST, SOC2, and HIPAA profiles available.

POST /v1/validate

Score credential strength against configurable compliance policies. Returns pass/fail per policy check with detailed analysis auditors can verify.

POST /v1/breach-check

Check credentials against 850 million known breached passwords using k-anonymity. The plaintext credential never leaves your environment.

GET /v1/audit-log

Tamper-evident log of all generation and validation events. Query by date range. The output compliance teams hand directly to auditors.

FRAMEWORK ALIGNMENT

SOC2 Type II	Credential controls, audit logging, encryption at rest
HIPAA Security Rule	Access control documentation, ePHI credential chain of custody
NIST 800-63B	Entropy documentation, character requirements, ambiguous exclusion
CMMC 2.0	IA.L1-3.5.1 access control, credential generation evidence

WHO WE SERVE

Managed Service Providers
Consistent cryptographic standards and per-call audit proof across every client account. One API key covers all environments.

Compliance Consultants
Give your clients audit-ready credential documentation from day one. Spend less time reconstructing evidence and more time closing engagements.

Mid-Market IT Teams
Replace ad-hoc credential generation with a single auditable API that satisfies SOC2 requirements automatically.

Healthcare IT
HIPAA-aligned credential generation with chain of custody logging. Documentation ties credential issuance to user roles and ePHI access rights.

PRICING

Free	**$0/month**
300 calls/month. Generate, validate, breach check. No credit card.	
Pro	**$29/month**
50,000 calls/month. All four endpoints including audit log. Email support.	
Business	**$149/month**
500,000 calls/month. Compliance documentation package. Priority support.	
Enterprise	**Custom**
Unlimited calls. Custom profiles. FedRAMP roadmap. Dedicated support.	

PARTNER PROGRAM

We work with compliance consultants and MSPs who want to give their clients automated credential audit documentation.

- ✓ Referral partnership: recurring monthly fee per client referred
- ✓ White-label: bundle under your brand as part of your SOC2 package
- ✓ Consulting partner: 90-day Pro access at no cost to evaluate on a real engagement

SECURITY POSTURE

- ✓ Zero credential storage. Generated credentials never written to any log or database.
- ✓ crypto.randomInt() exclusively. Math.random() does not exist in our codebase.
- ✓ K-anonymity breach detection. Plaintext credential never transmitted externally.
- ✓ Infrastructure as code. Every resource managed via Terraform. Fully auditable.
- ✓ AWS encryption at rest. DynamoDB with AWS managed keys and point-in-time recovery.