Product specification

# Smart Contract Guard 360

Smart contract assurance for institutions that must evidence control over on-chain systems. This specification sets out the six diligence artifacts a reviewer receives, grouped by what each one proves.

Version 1.0 | September 26, 2026 | Confidential, provided under NDA

Architecture

**Proprietary detection model at the core, with a rules engine applying control frameworks**

Coverage

**EVM including Hyperledger Besu, Solana, and Move-based chains**

Compliance mapping

**NIST CSF, ISO 27001, DORA and MiCA, plus the client's own control framework**

## What a reviewer can prove

### 01
### The architecture
Where every component runs, what crosses the trust boundary, and what each chain supports.

Page 2

### 02
### The findings
That every verdict is evidence a third party can reproduce from pinned inputs.

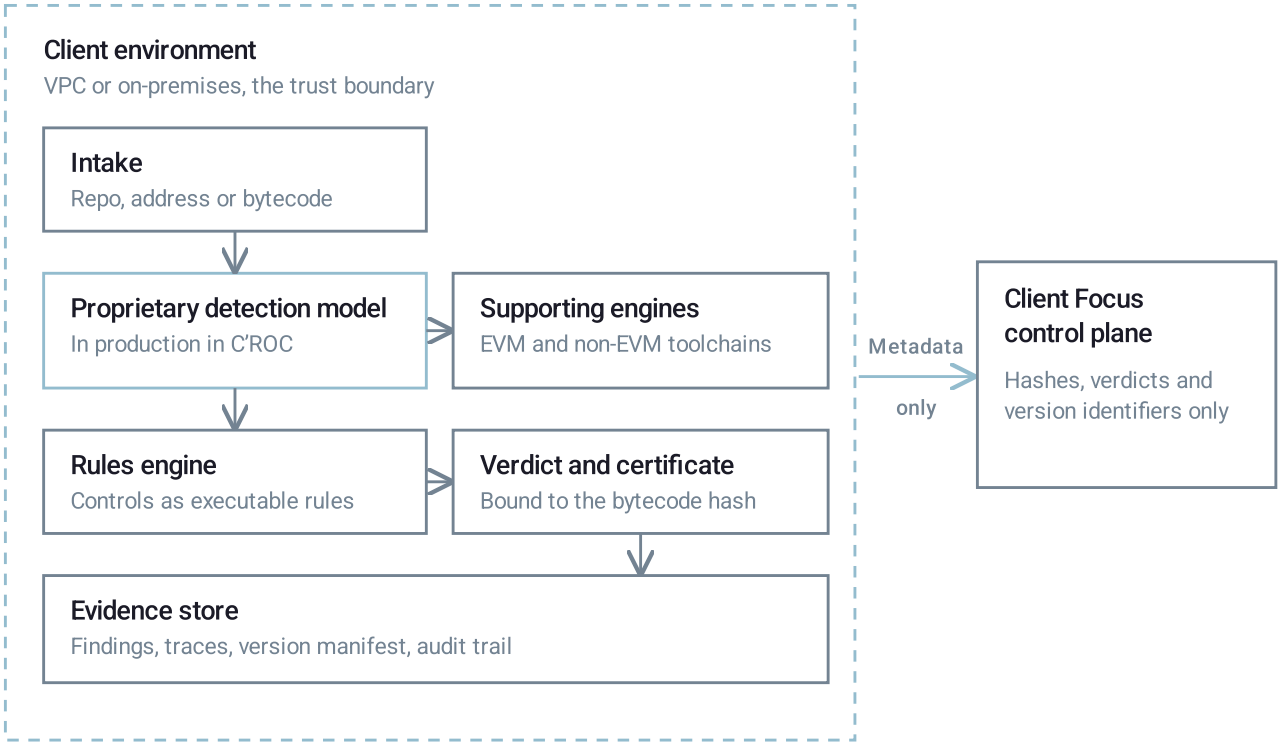
Page 3

### 03
### The operation
That assurance continues after release and the platform is ready for vendor onboarding.

Page 4

# 01 Prove the architecture

How the system is built, and where the trust boundary sits




## Reference architecture and data-flow diagram

Available

Where every component runs, what crosses the trust boundary, how signing works, and how the system behaves when the control plane is unreachable.

## Versioned chain-support matrix

Available

Production capability per chain with pinned tool editions, known limits and validation status. EVM including Hyperledger Besu, Solana (Rust and Anchor), and Move-based chains such as Aptos and Sui.

— Contract source, bytecode and model inference never leave the client boundary.

# 02 Prove the findings

That every verdict is evidence a third party can reproduce

### Redacted assessment and signed attestation

Per engagement or at go-live

A representative finding with reproducible evidence bound to the bytecode hash, the tested scope and exclusions, the rule-based verdict, and the steps to reproduce it.

### Benchmark report with baseline comparisons

At go-live

Incremental value over the supporting engines, false positives, misses with the critical class reported separately, and per-chain coverage. Figures come from the go-live test against a defined corpus.

## How a reviewer reproduces a verdict

**Step 1 — Pin the inputs**
Bytecode hash, engine and ruleset versions recorded

**Step 2 — Re-run**
The client's own team runs the pinned toolchain

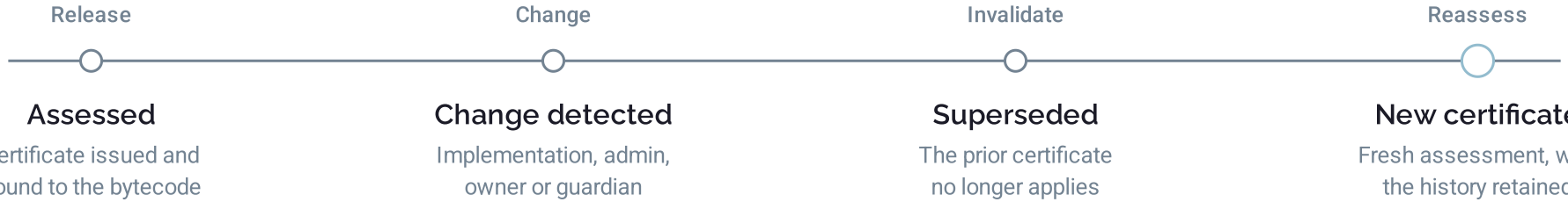
**Step 3 — Compare**
The rule-based verdict matches the certificate

**Step 4 — Confirm status**
Valid, superseded or withdrawn in the registry

Rules decide the verdict. AI informs the investigation, and a candidate becomes a finding only on deterministic confirmation.

# 03 Prove the operation

That assurance continues after release, and the platform is ready for onboarding




### End-to-end lifecycle example

Available

One contract followed from release through a detected change, invalidation of the prior certificate, and reassessment, with the full history retained as evidence.

### Enterprise readiness pack

Available | SOC 2 Type II planned

SSO and directory integration, role-based access and audit trail, service levels, penetration-test scope, continuity and evidence portability, with ISO 27001 status.

## Requesting these artifacts

Artifacts marked Available are provided on request under NDA. The others are produced from the client's own environment and benchmark corpus during delivery and at go-live acceptance, with a stated measurement date and pinned toolchain version.

info@clientfocusllc.com
+1 (888) 613-7190
clientfocusllc.com/solutions/scg360

ASHBURN, VIRGINIA
44355 Premier Plaza, Suite 110
Ashburn, VA 20147
United States

HYDERABAD, INDIA
Mazhar Estates, Sector 3, HUDA Techno Enclave
HITEC City Phase 2, Madhapur
Hyderabad, Telangana 500081

CONTACT
+1 (888) 613-7190
info@clientfocusllc.com
clientfocusllc.com