30-minute diligence script

SE runbook for live security review calls

Trustholm 30-Minute Diligence Script (SE Runbook)

Use during live security review calls with screen share in trial tenant.

Before call (5 min)

- - Confirm trial tenant provisioned
- - One agent installed and heartbeating
- - Signing certificate staged in test tenant

Minute 0–5: Security Center posture

Navigate to /security (Security Center). Capture: MFA status, SSO mode, audit logging toggle, script signing flags. Say: "This is posture summary—not a substitute for your ISMS."

Minute 5–15: Dual-custody + signing

1. Submit script for approval as User A

```
2. Attempt self-approve as User A → expect disabled Approve / ERR_DUAL_CUSTODY_VIOLATION
3. Approve as User B
4. Queue signed execution to pilot agent
```

Minute 15–25: Audit export

1. Open /audit or GET /api/audit/export with category + datetime window

```
2. Show publish → approve → execute correlation
3. Hash file live if GRC process requires
```

Minute 25–30: Isolation + limitations

- - Explain schema-per-tenant + JWT binding (403 demo if time)
- - State gaps honestly: WORM immutability backlog, vendor SOC 2 observation in progress
- - Mention Event Hub/DCR sink if Sentinel buyer

Artifacts to email post-call

- - Redacted export CSV
- - Security Center screenshot
- - Link to trust hub Shipped/Gap table
