HX-AEIR
AGENT EVALUATION INCIDENT RECONSTRUCTION

Security and Key Custody Guide

Customer-controlled trust boundaries, signing identity, network posture, and operations.

Document ID	HX-AEIR-DOC-002
Version	1.0
Published	August 26, 2026
Audience	Security architects, cloud administrators, risk teams, and incident-response stakeholders
Publisher	Tigantic Holdings, LLC dba HolonomiX

Marketplace documentation | Customer-facing reference

Contents

1. Security model

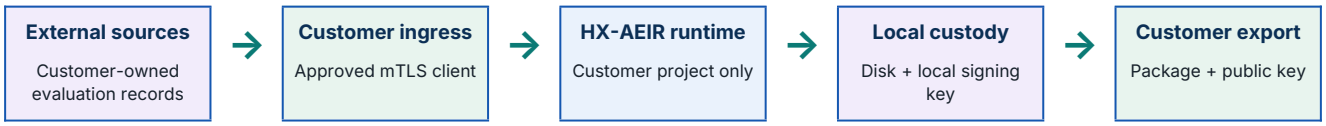
HX-AEIR is designed as a customer-controlled, single-tenant virtual appliance. The runtime, persistent evidence state, and application signing identity reside inside the customer Google Cloud project. Marketplace distribution, listing, billing, and support are outside the workload runtime, and no evidence automatically transits a HolonomiX-operated runtime service.

Security objective

Preserve the integrity, linkage, custody, and independent verifiability of agent-evaluation evidence while keeping prevention, monitoring, identity enforcement, network enforcement, and containment in the customer's existing control plane.

Control plane	Primary responsibility
Google Cloud Marketplace	Distribute the licensed image and deployment package.
Customer Google Cloud project	Own the VM, network, disk, IAM, runtime configuration, evidence, logs, and recovery controls.
HX-AEIR appliance	Validate, sign, link, export, and verify submitted evidence.
Customer security systems	Operate firewall, identity, monitoring, sandbox, policy, approval, and containment controls.
Customer verifier	Pin the public key and independently verify exported packages.
HolonomiX support	Provide product guidance without receiving customer evidence by default.

2. Trust and responsibility boundaries



Boundary	Security meaning
Partner-hosted runtime	None.
Evidence transit	No automatic transit to HolonomiX. Customer-directed export may cross the project boundary.
AI/model runtime	Outside HX-AEIR. The product contains no inference or agent-control component.
Signing identity	Generated during authorized initialization and retained locally under customer control.
Offline verifier	Optional customer-operated utility; not part of the deployed Marketplace runtime.
Availability	Single-zone, single-VM reference deployment; recovery depends on customer backup and restore objectives.

3. Identity and administrative access

The reference administration path uses Identity-Aware Proxy TCP forwarding to TCP/22 and OS Login. This separates operator access from the HTTPS application path and uses customer IAM for SSH authorization.

- Grant only the minimum deployment, IAP tunnel, OS Login, and service-account permissions required by the customer operating model.
- Do not grant broad project roles to the VM service account. The reference deployment module grants no project IAM roles to the attached VM identity.
- Use OS Login administrative access only for designated operators. Review access periodically and remove stale principals.
- Keep the SSH path independent from Nginx and the mTLS application path.
- Record administrative changes through the customer change-control and audit processes.

> **Customer prerequisite**
> IAP TCP forwarding and OS Login must be enabled and authorized in the customer project when the recommended administration path is used.

4. Network and application isolation

Network element	Reference posture
TCP/22 administration	Allow only from Google-documented IAP TCP forwarding ranges; authenticate with OS Login.
TCP/443 API	Allow only from customer-approved ingress sources; terminate at Nginx with mutual TLS.
Application listener	No network listener. Nginx forwards to a local Unix domain socket.
Default external IPv4	None.

Network element	Reference posture
Optional public mode	Customer-reserved external IPv4 plus customer-CIDR firewall restrictions.
Optional private mode	Customer-provided VPN, Interconnect, peering, or other private connectivity to the internal IP.
Other inbound traffic	Implicitly denied by customer firewall policy.

- Use customer-managed server TLS material, client CA, and client certificates.
- Define certificate issuance, rotation, revocation, and incident-response procedures before production use.
- Do not expose the Unix socket or the unprivileged application directly to the network.
- Treat optional external IP, private connectivity, and egress as customer-selected controls that require customer review.

5. ML-DSA-65 key lifecycle

HX-AEIR uses ML-DSA-65, the parameter set specified in NIST FIPS 204, to generate and verify digital signatures. The product does not claim that its deployed cryptographic module is FIPS 140-3 or CMVP validated unless a separate, current validation statement is provided.

Lifecycle stage	Required practice	Evidence to retain
Image creation	Ship a neutral image with no customer signing key embedded.	Image scan and build evidence.
Initialization	Generate the keypair during an authorized customer operation.	Change record, time, operator, public-key fingerprint.
Private-key custody	Keep the private key local; restrict file permissions and service access.	Permission check and support-bundle exclusion.
Public-key pinning	Store the public key or fingerprint independently from the appliance.	Pinned key record in customer-controlled system.
Backup and restore	Protect key material under an approved recovery process; test restoration.	Restore test and issuer-identity continuity result.
Rotation or retirement	Issue a new identity under change control; preserve old public keys for historical verification.	Key transition record and retention decision.
Decommission	Preserve public keys and required evidence before destroying the appliance.	Decommission checklist and destruction record.

Never export the private key in an evidence package

Evidence packages contain receipts, manifests, linked objects, artifacts, and the public verification material required by the workflow. They must not contain the application signing secret.

6. Evidence custody and disclosure

Persistent evidence is stored locally on the customer-controlled boot/data disk. Customer-directed API submissions, exports, backups, snapshots, and offline verification may cross the project boundary according to the customer's policy. HX-AEIR does not automatically forward evidence to HolonomiX.

- Classify source evidence before ingestion and retain only the material required for the intended reconstruction.
- Do not embed raw passwords, private keys, tokens, or other credentials in receipt payloads.
- Use content-addressed digests and explicit evidence references to bind artifacts without weakening custody controls.
- Treat public disclosure derivatives as separate signed objects. A public derivative should carry a signed commitment to the controlled source, not the restricted source body.
- Require the separately authorized source package for full source reconciliation.
- Apply customer retention, legal hold, records management, and deletion policy to exported packages and public keys.

Customer-selected control	Security boundary
Optional CMEK	Applies to persistent-disk encryption only. It is not the application signing key.
Optional backup/snapshot	Customer-directed. Define RPO/RTO, key protection, retention, and restore testing.
Support bundle	Must redact secrets and should exclude private evidence unless separately authorized.
Customer export	May include evidence package, verification report, and independently pinned public key.

7. Backup, recovery, upgrade, and decommissioning

7.1 Backup and restore

1. Define which application state, evidence, configuration, and key material are protected.
2. Protect backup access separately from the running appliance.
3. Test an isolated restore and verify that the restored issuer identity matches the approved recovery plan.
4. Verify historical packages after restore using the independently pinned public key.
5. Document recovery objectives and acknowledge that the reference architecture has no automatic zonal failover.

7.2 Upgrade and rollback

- Verify the release identity, image provenance, and vulnerability evidence before upgrade.
- Export or protect required evidence and public-key material before change.
- Test health, issuance, export, and offline verification after upgrade or rollback.
- Do not silently replace the signing identity unless the change is explicitly authorized and documented.

7.3 Decommissioning

- Preserve public verification material required for historical evidence.
- Export evidence required by policy and verify the exports before deletion.
- Revoke client certificates and remove network access.
- Destroy private key material and persistent disks under customer policy.
- Record the final issuer-retirement and evidence-retention decision.

8. Security operations and support

Operational signal	Customer action
Repeated mTLS failures	Review certificate validity, CA chain, client authorization, and source CIDR.
Unexpected receipt rejection	Inspect schema, semantic validation, unresolved evidence references, and raw-secret detection.
Public-key mismatch	Stop verification and reconcile the independently pinned key before trusting the package.

Operational signal	Customer action
Disk pressure	Apply the approved export/retention process or increase capacity.
Suspected key exposure	Isolate the appliance, preserve evidence, retire the issuer identity, and follow the incident plan.
Support request	Provide sanitized diagnostics only; do not transmit secrets or confidential evidence through general contact channels.

Responsible disclosure: HolonomiX Security

Product support: HolonomiX Support

9. Claim limits

> **Verification is not prevention**
> HX-AEIR does not enforce network, identity, tool-use, sandbox, or approval policy; it does not monitor or contain an agent. It binds evidence about those systems and actions.

- A valid signature demonstrates integrity and issuer-key verification for the signed material.
- A valid package does not establish semantic truth, legal correctness, decision quality, or completeness of unobserved telemetry.
- No-harm language must remain bounded to the observation cutoff and available evidence.
- A sandbox escape should not be asserted unless evidence shows that an effective boundary existed and was bypassed.
- The product is not a FIPS 140-3 or CMVP validated cryptographic module unless separately documented.

References

- Google Cloud Marketplace - Offering VM products
- Google Cloud - IAP TCP forwarding
- Google Cloud - OS Login
- NIST FIPS 204 - Module-Lattice-Based Digital Signature Standard

Reference links were verified on August 26, 2026. Product-specific behavior is governed by the deployed HX-AEIR release, the applicable Marketplace order or Private Offer, and the customer's configuration.