

NVR + SKIA / ENTERPRISE BROWSING

NVR, Skia, and the enterprise browsing boundary

A technical white paper on rendering fidelity, input handling, session isolation, data movement, and measurable user experience.

6 September 2026 / Technical edition

Inside this paper

- 01 Executive architecture
- 02 The rendering path
- 03 Keeping interaction natural
- 04 The security boundary
- 05 Where agentic auditing adds value
- 06 Performance is a budget, not a slogan
- 07 What the enterprise pilot should prove

01 / Executive architecture

Browser isolation should change the execution boundary without making everyday work feel like a remote desktop. Antara uses Network Vector Rendering (NVR) and Skia in its RBI product to pursue that goal. The enterprise value is the combination: isolated execution, controlled presentation, identity-bound access, and an audit trail that explains the session.

This paper defines the architecture and the deployment acceptance criteria. It does not treat a drawing engine as a security boundary by itself. Remote execution, authenticated transport, constrained decoding, browser hardening, and explicit data-transfer policy each have a separate job. A successful deployment validates all of them against the applications employees actually use.

NVR is an established browser-isolation approach in which drawing information is delivered instead of forwarding a destination page for ordinary local execution. Skia is a cross-platform 2D graphics library; CanvasKit exposes Skia capabilities through WebAssembly. These are useful foundations, not evidence that any particular isolation implementation has identical behavior.

References: [NVR industry background](#) / [Skia graphics architecture](#) / [CanvasKit and WebAssembly](#)

02 / The rendering path

Execution stays remote; presentation reaches the endpoint

01	Identity & policy Authenticate, select a region, and scope the browsing session.
02	Isolated browser Fetch the destination and execute its active content remotely.
03	NVR delivery Encode visual updates and approved interaction state.
04	Local presentation Render the controlled view and return user input.

The remote browser owns page execution and layout. The presentation layer conveys the visible result through a graphics-oriented channel. A visual update can describe changed regions, drawing operations, or reusable resources; it should not become an unbounded channel for arbitrary page scripts. The endpoint runs the Antara presentation client, while destination code remains in the isolation environment.

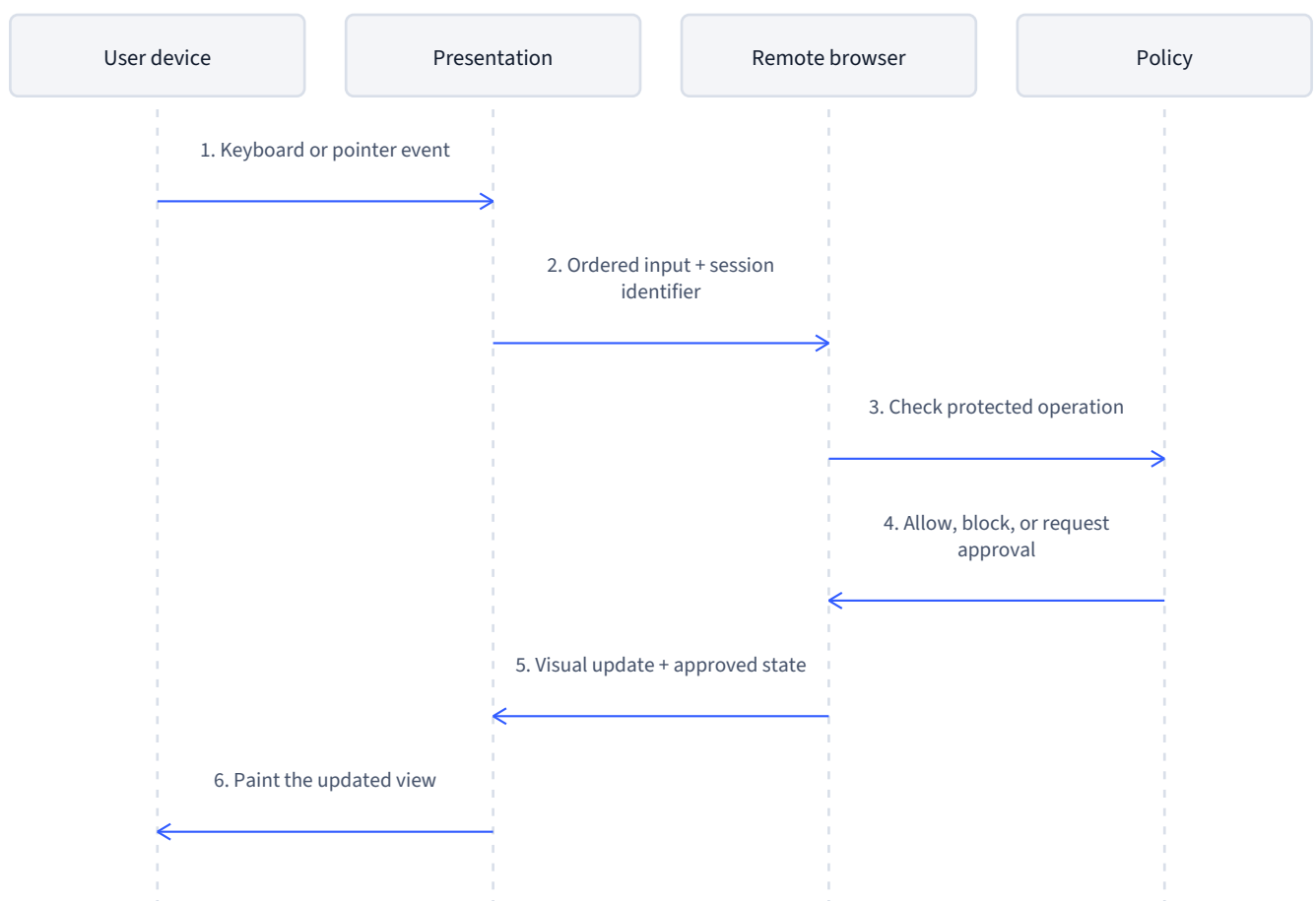
The engineering profile favors incremental updates over a complete repaint on every event. Resource reuse can reduce repeated font and image transfer; damage tracking can limit work to the region that changed. A cache

must remain scoped to its session or tenant, expire predictably, and never let one user infer another user's content. Compression and transport protection solve different problems and should be measured independently.

Skia contributes text, path, image, and compositing primitives. It does not automatically provide remote input synchronization, semantic accessibility, clipboard authorization, tenant isolation, or safe deserialization. Those requirements belong to the product architecture around the renderer. The acceptance test must inspect the entire path, including renderer failure and recovery.

03 / Keeping interaction natural

An interaction round trip



A useful interaction model distinguishes local feedback from authoritative application state. A cursor can move locally; a transaction confirmation must follow the remote application. Scrolling, text selection, focus changes, drag-and-drop, and input-method composition need their own test cases. Optimistic visual feedback must never imply that a blocked upload or unsaved edit succeeded.

Text fidelity involves font availability, shaping, scale, zoom, and display density. An application that looks correct at one zoom level may still fail with complex scripts or a screen reader. The product evaluation therefore includes keyboard-only navigation, IME composition, high-contrast modes, selection across lines, browser

zoom, and assistive technology. A graphics stream alone cannot communicate every semantic relationship that accessibility software requires.

Interaction	What to validate	Failure to detect
Typing and IME	Composition, focus, shortcuts and caret placement	Lost input or duplicate submission
Scrolling and zoom	Long documents and high-density displays	Stutter, clipped content or incorrect selection
SaaS sign-in	Redirects, popup flows and session expiry	Looping authentication or broken state
Media and graphics	Video, conferencing and graphics-heavy apps	Fallback that silently changes the security boundary

04 / The security boundary

The display protocol is a parser boundary. Enforce message size, resource count, image dimensions, nesting depth, and memory budgets before allocating work. A presentation process must not trust remote browser output simply because that browser belongs to the same service. Corrupted drawing resources, unexpected message ordering, or a stale session key should terminate or recover the presentation path without granting a less restricted browsing route.

Treat each browser session as an isolated execution context with scoped credentials, bounded storage, and a clear end-of-life operation. Separate control-plane administration from the browsing data plane. After revocation, invalidate the session's access grant, prevent new requests, and remove temporary state according to the retention policy. An operator should be able to distinguish a session that was closed from one whose audit record was retained.

- Downloads cross a file-transfer boundary: authorize, inspect where configured, then release or quarantine.
- Clipboard transfer is directional. Copy out and paste in can require different rules.
- Printing, uploads and sensitive form submission should be governed explicitly.
- Exceptions need an owner, scope, expiry and recorded reason; an exception must not be an invisible direct-access fallback.

05 / Where agentic auditing adds value

The agentic packet auditor gives the browsing session an investigative context. A request to an unfamiliar destination is more useful when connected to the signed-in user, the remote session, a file-transfer decision, and the policy version that governed it. The auditor can investigate those relationships and prepare an evidence-backed explanation for an operator.

The right observation point matters. On the remote browser side, authorized application telemetry can explain a navigation or transfer. On an encrypted network segment, a passive observer may see only metadata. The audit record must say which source produced each fact. It must not infer file contents from byte counts or claim to decrypt a TLS session without an authorized termination or inspection point.

A web page is also an adversarial input source for an agent. Retrieved page text, document contents, filenames, and network payloads remain evidence, never instructions. Investigation tools should be tenant-scoped and read-only by default. A recommendation to change policy follows an approval and enforcement workflow separate from the model's explanation.

06 / Performance is a budget, not a slogan

Responsive browsing depends on network round-trip time, remote execution, update encoding, transport, local decoding, and paint. NVR can reduce the amount of visual information that needs to move for suitable workloads; it cannot eliminate distance or guarantee that all pages produce small updates. A graphics-heavy canvas and a mostly static document have different cost profiles.

Measure the interaction path

```
Input-to-visible-result =  
  input transit + remote event handling  
  + layout / draw + encode / queue  
  + return transit + decode / paint
```

Report p50, p95 and p99 by region, device and application.
Compare the same task against direct browsing.

Evaluate cold launch separately from a warm, authenticated session. Run tests under packet loss, constrained bandwidth, and mobile network changes. Record task completion as well as frame timing: a fast view that loses keyboard focus is not a good experience. Product-specific measurements should be published with test conditions and workload definitions, rather than presented as universal zero-latency claims.

Other RBI implementations document compatibility constraints and delivery-mode differences. That is a reason to test complete application workflows, including authentication and media, rather than assume that every feature follows from the rendering technique.

References: [RBI compatibility considerations](#)

07 / What the enterprise pilot should prove

- Business workflows complete with the expected keyboard, accessibility, media and download behavior.
- A denied data operation remains denied during retries, reconnects and session migration.
- Tenant and user boundaries hold across caches, cookies, credentials and temporary storage.
- Latency and resource-use measurements include slow links and representative endpoint hardware.
- Operators can reconstruct a session decision from evidence without broad access to raw sensitive content.

The final pilot artifact is an application acceptance matrix, a region plan, a data-control policy, a tested exception process, and an operational owner. This turns "native-feeling browsing" into a property the buyer can evaluate and maintain.

References and continued reading

[NVR industry background](#)

[CanvasKit and WebAssembly](#)

[Product overview](#)

[Operations and evaluation](#)

[Skia graphics architecture](#)

[RBI compatibility considerations](#)

[Integration guide](#)