Executive Brief

Artifact A · IBR-PR-A-1.1 · Stage 2, pre-NDA · What Citadel is, why it exists, and what is actually real today.

● Proven ● Qualifying ● Held back

Issued 18 August 2026 **Supersedes** v1.0, 16 August 2026

Set A Executive Brief · B Ten Rings · C Claim & Evidence

Authority Iberion Holdings, LLC **Reading time** ~15 minutes

WHAT IS CITADEL?

Citadel is a licensable, application-neutral Internet protection architecture, developed and exercised inside a live production application.

Application-neutral is the important word. Citadel is not a streaming feature, not a browser add-on, and not a product tied to one industry. It protects an approved Internet journey — whatever application happens to be making it. It can be embedded inside another company's product, run standalone on a customer's device, or operated as managed infrastructure on a licensee's behalf.

It is built and owned by Iberion Holdings, the technology-licensing entity within Meridian Group Holdings. Iberion's business is licensing the architecture, not operating a consumer service.

WHY DOES IT EXIST?

Most security products protect one place: one application, one network boundary, one moment. Everything before and after that point is assumed to be fine.

Encryption is the clearest example. A tunnel encrypts traffic, and the customer is invited to believe the story ends there. It does not. Name resolution can leak outside the tunnel. IPv6 can route around it. A gateway sees both who is asking and what they asked for. The security tool itself often builds a browsing history — a new copy of exactly the information the customer was trying to protect. And when any of this quietly fails, the interface still says *Connected*.

Citadel exists because protection should not stop at encryption, and because a protection claim the customer cannot verify is not really a protection claim.

> *How much of the information journey can be protected without interrupting the traffic the customer actually wanted — and how can that protection be proven to the customer rather than asserted at them?*

WHAT MAKES IT DIFFERENT?

Ten coordinated defensive rings, not one tunnel. Each ring is a distinct defensive responsibility with its own scope, its own tests, and its own evidence record. Together they extend protection from transport, DNS and routing, through destination containment, resource and behavior defense, evidence minimization, bounded deception, endpoint and screen privacy, infrastructure hardening, destination-domain privacy, and device assurance.

They are composable controls — not ten VPNs stacked on each other, and not seven network layers renamed. A higher-numbered ring is never a substitute for a lower-numbered one that failed.

Protection that reports its own state honestly

Citadel reports configuration state and actual protection state as separate facts. An interface being "up" is never treated as proof that traffic is protected. Handshake currency, real traffic flow, DNS posture, IPv4/IPv6 route posture, and confirmed public egress are each surfaced independently. When something is degraded, the system says so rather than showing a green badge.

Evidence minimization as a design principle

A protection system that logs everything has simply moved the exposure. Citadel's operational receipts are minimized and expiring, and are scanned against a forbidden-data list — the security layer is not permitted to become the new collector.

Every claim is bounded by a recorded evidence state

Internally, no ring is described as operational until specific, named runtime evidence exists. Rings sit in explicit states — isolated, validated, deployed, runtime-verified, under observation, production-proven — and a status cannot advance without a change record, test evidence, and a rollback path. This is why we can hand a communications professional a per-ring evidence table instead of adjectives.

WHAT'S REAL TODAY?

This is the part most technology companies blur. We do not.

MATURITY	RINGS	COUNT
PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE	Aegis · TrueNorth · Gatewatch · Sentinel · Veil · Mirage · Infrastructure Defense	7
CLIENT-VALIDATED Under qualification. Validated on a physical device.	Obscura	1
IMPLEMENTED — QUALIFYING Implemented across the canonical server and Android client; database migration and endpoint upload executed. Integrated-client correction and qualification in progress.	Anonymous Destination Domain Register	1
DEPLOYMENT-AUTHORIZED, NOT DEPLOYED Stage G v2 is implemented and deployment-authorized. Managed continuity is deferred and is not a deployment prerequisite.	Device Assurance	1

Supporting evidence includes live reboot-recovery testing (full node restart with zero manual intervention), adversarial burst-load testing showing measured containment, blocked-probe testing, and one real production incident that was root-caused, fixed, and independently re-verified end to end — with the entire account preserved as evidence rather than quietly closed.

> **Whole-system boundary.** Evidence status is assigned by ring. Citadel's ten-ring architecture should not be described as wholly deployed, universally qualified, or independently certified.

Two further qualifiers are load-bearing and should survive into any public copy. "Production-proven within the registered evidence scope" means proven within the scope that was registered and tested — not a universal guarantee across every platform, configuration, or workload. And the newest infrastructure component remains inside an active observation window.

WHAT'S THE BIGGER IDEA?

Citadel is the working, shipping expression of a larger proposition Iberion calls **Information Defense**.

The proposition: the digital economy has spent decades extracting information, building profiles, and monetizing identity — usually without meaningful consent, compensation, or defensible boundaries. The objective is not to stop information from moving. Information exchange is how commerce, medicine, and communication work.

Iberion is not anti-sharing. The customer decides whether to share, with whom, for what purpose, and under what agreed terms—including compensation. The customer can also choose not to share.

The objective is to **reduce involuntary information extraction while preserving legitimate, consensual information exchange** — to make each information journey purpose-bound, policy-governed, privacy-minimized, recoverable, and economically measurable.

> If you want my information — pay me.
> If you want my identity — protect me.
> If you want my enterprise — earn my trust.

Citadel is a component within that doctrine, not the whole of it. Iberion's doctrinal frameworks (PIDI and EIDI) cover a wider information lifecycle — admission, minimization, recipient control, evidence, expiration, revocation, recovery. Citadel is the transport and route-control layer of that idea, in production today. **Citadel's ring numbers and the PIDI/EIDI doctrinal ring model are separate schemes and must never be mapped one-to-one in public material.**

WHAT CAN YOU SHOW ME?

MiraTV — a live IPTV platform carrying real customer traffic on Android and Android TV, with Citadel integrated into it.

MiraTV is the demonstration environment. It is a demanding, latency-sensitive, customer-facing application, which makes it a genuine test: protection that breaks video playback is not protection anyone will accept.

> **MiraTV is not Citadel.** MiraTV is a production application environment in which Citadel has been integrated and exercised. Citadel is separately licensable technology with its own product identity, its own platform surfaces (Android, Linux, Windows), and its own standalone deployment modes.

Available demonstration material includes the running application with Citadel active, the customer-facing protection-verification surface (the screens showing route, DNS, egress and degradation state as separate facts), and recorded evidence of the reboot-recovery and containment tests.

DEPLOYMENT AND COMMERCIAL SHAPE

Citadel is offered as an embedded module inside a licensee's platform, as a standalone one-gateway client, in an optional two-hop mode that separates customer-facing ingress from Internet-facing egress, as backend/platform licensing, or as Iberion-operated managed infrastructure.

Commercial paths run from a fixed-fee assessment, through a time-bounded pilot against a bounded production path, to annual licensing, managed-service retainer, or a First Production Partner arrangement. Pricing is not fixed by schedule; deployment scope, support burden, infrastructure, and reference rights determine terms.

WHAT WE NEED FROM A COMMUNICATIONS PARTNER

We are not asking anyone to explain the engineering. We are asking for help placing the technology before credible journalists, researchers, and industry voices who can scrutinize its claims and determine whether the story merits independent coverage — and for help reaching the right buyers: privacy-conscious platforms, OEMs and application developers needing an embeddable protection layer, managed service providers, and enterprises that need protected egress they can actually verify.

The constraint is that everything said publicly must stay inside the recorded evidence. Artifact C — Claim & Evidence Sheet exists to make that constraint workable rather than paralyzing: it states what can be said, what backs it, and what must not be said, so a writer can be creative without accidentally putting words in our mouth that the architecture does not support. It is released under NDA.

Deeper technical substantiation exists — reference architectures, system specifications, component inventories, deployment registries, and qualification guides — and is released selectively when a specific journalist or analyst question requires it.
