Ten Rings Capability & Evidence Sheet

Artifact B · IBR-PR-B-1.1 · Stage 2, pre-NDA · Per-ring capability, maturity, and limitation.

● 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

Citadel composes ten independent defensive responsibilities around a single customer-approved Internet journey. They are **coordinated controls, not ten VPN tunnels**. Numbers describe responsibility, not activation order — a higher-numbered ring never substitutes for a lower-numbered one that failed.

> **Customer agency.** 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.

RING	NAME	PROTECTS AGAINST / CONTROLS	EVIDENCE STATUS
1	**Aegis**	Encrypted transport. Owns the single approved route, its continuity, and visible degradation of it.	PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE
2	**TrueNorth**	DNS and route integrity. Keeps name resolution inside the protected route instead of leaking around it.	PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE
3	**Gatewatch**	Destination containment. Detects unsafe resolution and contains destination intent.	PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE
4	**Sentinel**	Resource and behavior defense. Contains abuse and resource pressure without interfering with wanted traffic.	PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE
5	**Veil**	Evidence minimization. Keeps operational receipts minimal and expiring; the security layer does not become a browsing-history collector.	PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE

RING	NAME	PROTECTS AGAINST / CONTROLS	EVIDENCE STATUS
6	**Mirage**	Signed, bounded deception. Scoped, expiring, signed containment and decoy responses to verified probes.	**PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE**
7	**Obscura**	Endpoint and screen privacy. Screen-capture protection and local hostile-device posture detection on the customer's own device.	**CLIENT-VALIDATED** Under qualification. Android client physically live-validated.
8	**Infrastructure Defense**	Infrastructure-level containment. Firewall policy, service hardening, resource-pressure containment, and exact peer/CIDR validation — protection that holds on nodes where the transport ring deliberately does not apply.	**PRODUCTION-PROVEN WITHIN THE REGISTERED EVIDENCE SCOPE** Deployed and evidenced on the second-hop egress node; still inside its observation boundary.
9	**Anonymous Destination Domain Register**	Personal DNS privacy. Maintains a customer-controlled, purpose-bounded register of approved destination domains and minimizes durable customer/domain association outside the trusted resolver boundary.	**IMPLEMENTED — QUALIFYING** Implemented across the canonical server and Android client; database migration and endpoint upload executed. Integrated-client correction and qualification in progress.
10	**Device Assurance**	Device and key security posture. Records graded confidence in the device's key backing, credential authority, route witness, and platform integrity, for the rest of Citadel to observe.	**DEPLOYMENT-AUTHORIZED, NOT DEPLOYED** Stage G v2 is implemented and **deployment-authorized**. Managed continuity is **deferred** and is not a deployment prerequisite.

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.

READING THE STATUS COLUMN

- **Production-proven within the registered evidence scope** — verified against live infrastructure *within the scope that was registered and tested*. Not a claim of universal qualification across every platform, configuration, or workload.
- **Client-validated, under qualification** — real evidence from a physical device, but the capability is not complete end to end.
- **Implemented — qualifying** — built and carried into the canonical server and client, with qualification still in progress.
- **Deployment-authorized, not deployed** — implemented and cleared for deployment, but not yet deployed, activated, or qualified.
- **Deferred** — specified and deliberately not built, and not required for deployment.

Seven of ten rings are production-proven within their registered evidence scope. Three are stated honestly as something less. That distinction is the story, not a caveat to be smoothed over — a vendor that reports its own unfinished work is making a credibility claim no competitor's marketing can match.

TEN PLACES A STORY CAN START

01 **Aegis**
Protection that reports its own degradation instead of showing a green badge.

02 **TrueNorth**
The leak nobody checks: DNS escaping the tunnel that was supposed to cover it.

03 **Gatewatch**
Containing where traffic is *going*, not just encrypting how it gets there.

04 **Sentinel**
Defending against abuse without breaking the traffic the customer wanted.

05 **Veil**
The security product that refuses to build a profile of you.

06 **Mirage**
Answering a hostile probe with something bounded, signed, and expiring.

07 **Obscura**
Protection that continues *after* information reaches the screen.

08 **Infrastructure Defense**
Hardening that holds where the VPN layer deliberately isn't.

09 **Anonymous Destination Domain Register**
A personal DNS register the customer controls — approved destinations without a durable customer-to-domain association outside the trusted resolver boundary.

10 **Device Assurance**
Graded trust in a device, where the response to weak evidence is greater scrutiny rather than lockout — never withholding protection from the devices least able to prove themselves.

SUBSTANTIATION

Each ring's status is backed by a registered internal evidence package — test records, acceptance evidence, and, where applicable, incident and recovery history. These are controlled records rather than public documents. They are made available on request through Iberion, under NDA and scoped to the specific question being asked.

> Citadel's ring numbers are **independent of** the PIDI/EIDI doctrinal ring model. The two schemes must never be mapped number-for-number in public material.