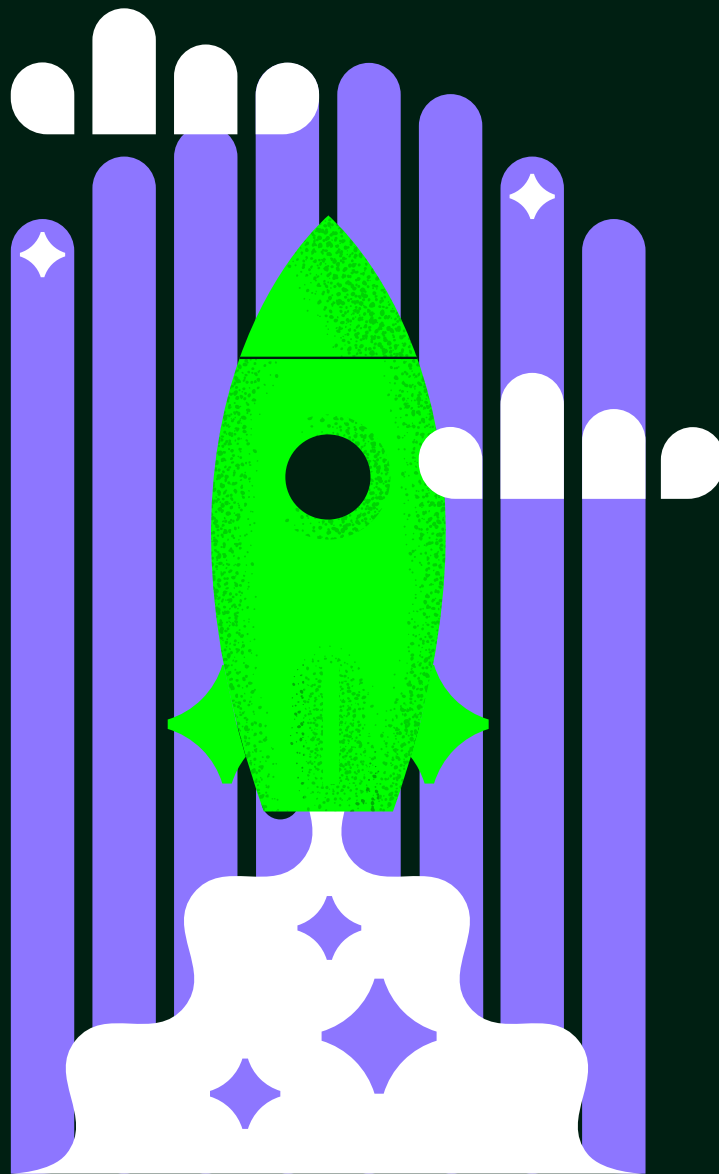
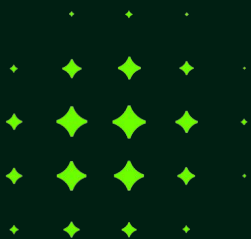




Owned Assets vs Risk Exposure – Gap Checklist

Identify where your current domain program has visibility gaps that create real exposure.





A

Portfolio visibility (owned assets)

- ☐ We have a current inventory of the domains we own
- ☐ We know where each domain is registered and who has access to it
- ☐ We have renewal controls and escalation processes for critical domains

B

Exposure visibility (outside owned assets)

- ☐ We don't have a consistent view of lookalike or typo domains related to our brand
- ☐ We can't quickly tell which lookalikes are active vs inactive
- ☐ We don't track DNS or email signals that indicate misuse or increasing risk
- ☐ We can't easily explain to leadership where the biggest exposure is today

C

Common "gap" indicators

- ☐ Different teams maintain different lists (IT vs. Security vs. IP/Legal)
- ☐ No shared process for deciding what to act on
- ☐ Responses are reactive (after an incident), not prioritized prevention
- ☐ We can't answer: "What should we protect next and why?"

D

Gap-closing quick wins (no overhaul required)

- ☐ Create a shared weekly view: Owned / Exposed / Actioned
- ☐ Agree on three decision buckets: Protect next / Monitor / Deprioritize
- ☐ Define 3–5 escalation triggers (what moves something into Protect next)
- ☐ Standardize one place to document decisions and owners

Start with a
strategic conversation

Book a session with Matt Serlin,
Senior Director Domain Management (US)

