Domain Monitoring PRD

Enable self-serve domain monitoring in a freemium entry product called CheckPhish, allowing users to track suspicious domains and receive alerts, while establishing a foundation for PLG by focusing on user acquisition and product activation rather than immediate monetization.

Team: CheckPhish
Contributors: PM, Designer, Engineer, Analyst
Resources: Figma Link, Jira Epic, Notion Research Wiki
Status: Draft / Problem Review / Solution Review / Launch Review / Launched

---

Problem Alignment

Currently, lookalike domain monitoring on the Bolster platform requires manual setup, creating friction for users who want to get started independently without a sales demo at the top of the funnel. This lack of self-serve capability limits user acquisition and activation, preventing high-intent users from seamlessly experiencing the value of lookalike domain detection.

Why does this matter to our customers and business?

- Users expect self-serve onboarding to quickly access security insights without waiting for a sales team. This aligns with the current PLG strategies, where reducing friction improves conversion rates.
- The current process of identifying threats is highly manual and often reactive, meaning that threats are already live before action is taken.
- There is no scalable self-serve solution in the market that allows Security teams to proactively monitor and detect domain abuse.

What evidence or insights do you have to support this?

- Feedback shows a strong preference for self-serve tools to explore security insights before engaging in a sales conversation.
- High inbound traffic related to domain monitoring queries, but limited conversions due to manual setup barriers.
- Companies with frictionless onboarding see significantly higher activation rates, reinforcing the need for a seamless self-serve experience. Currently, domain monitoring is a manual setup process on the Bolster platform, creating friction for users who want to get started independently without a sales demo.

Additionally, sales and SEO data highlight domain monitoring as one of the biggest self-serve opportunities, with high search interest and inbound inquiries. Without an accessible way to engage with this feature, we are missing a key PLG opportunity to capture high-intent users.

From a business strategy perspective, Bolster is committed to establishing a PLG foundation, enabling self-serve usage as a growth lever before monetization. By reducing onboarding friction and providing a clear path to activation, we align with our long-term strategy of converting engaged users into paying customers through demonstrated value.

High-Level Approach

We will introduce an automated, self-serve monitoring experience that enables users to:

- Sign up for domain monitoring via a freemium product called CheckPhish.
- Automatically track a single domain under a free plan.
- Receive notifications for phishing/suspicious activity.
- Expand product adoption through guided engagement, not direct monetization.

Goals

Primary Goals:

1. Increase acquisition by driving more web visitors to new account creations (Baseline demo request conversion rate: X%).
2. Improve activation by enabling users to set up domain monitoring seamlessly (Industry benchmark: XX%).

Non-Goals:

- Providing enterprise-grade monitoring and dedicated support resources for freemium users.
- Handling auto domain takedowns in this phase.
- Validating pricing and Stripe integration in this phase

Reviewer	Status
EPD	🟢
Leadership	🟢

Solution Alignment

Key Features

Plan of Record:

1. **Monitoring Setup**
    - User-entered domains upon signup.
    - Loading animation with progress bar (Generation CTA → Identifying → Scanning).
    - Ability to navigate to other tabs while loading with educational copy in UI.
2. **Dashboard Experience**
    - Users can see monitoring results limited to 1 free domain.
    - Additional sources in the Enterprise are greyed out.
    - Pre-malicious monitoring limited to 300 results with highest risk detected sort from high to low
3. **Notifications & Alerts**
    - Email alerts: Triggered when new threats are detected.
    - In-app alerts (Phase 2.0): Red notification dot, directing users to results.
4. **Feature Gates & Expansion**
    - Users see guided engagement prompts (butter bar, pop-ups) to explore additional features.
    - Focus on educating users on broader security risks rather than direct monetization.

Future Considerations:

- Multi-domain monitoring for premium users.
- Advance risk scoring and AI-powered threat assessment.

Key Flows

[see Figma link]

1. **First-time user flow:**
    - Visits Website → Enters domain → Creates account → Auto-monitoring setup.
2. **Returning user flow:**

    - Receives email alert → Logs into dashboard → Reviews threat results.
3. **Expansion flow:**
    - Users engage with additional security features → Explore domain acquisition insights.

Key Logic

- Users can monitor only 1 domain daily.
- If a domain change is requested, previous data is lost, export option provided.
- Alerts trigger based on new phishing/suspicious domain detection.

Launch Plan

Phase	Milestone	Description	Exit Criteria
1.0 web and sign up	Web acquisition	Homepage CTAs and onboarding flow	Visitor to sign up CRV
1.0 Product usage	Product activation	Initiate domain monitoring	Achieve industry benchmark activation
2.0 notification and alerts	Alerts and engagement	Introduction to email or in app alerts	Drive users back from new threats
3.0 Expansion	Feature growth	Expand new feature based on feedback	Define self-serve strategy from learnings

Reference links