MyDomainRisk

EXECUTIVE BRIEF

May 2026 Product Update

What changed, why it matters, and which tiers benefit from the latest product developments.

PERIOD
May 2026

PREPARED FOR
Signed-up users

PUBLISHER
Huro Data Technologies Ltd

REPORTING
Clearer PDFs and progress language

WORKFLOW
Owners, status, due dates and evidence

MSP
Client bundles, portal access and audit trail

Contents

Sections and subheadings included for review planning.

MyDomainRisk May 2026 Product Update

Newsletter for signed-up users
29 May 2026

May was a busy month for MyDomainRisk. Our focus was simple: make the product easier to understand, easier to report from, and more useful for showing security progress over time.

Many of this month's improvements are about confidence. When a scan highlights a problem, the report should explain it clearly. When something improves, you should be able to show that progress. And when you are working with clients or senior stakeholders, the output should be easier to share without rewriting it yourself.

Summary

In May, MyDomainRisk improved in five main areas:

- **Clearer reports** - findings now use plainer language and better separate confirmed issues from things the scanner could not fully verify.
- **Better progress tracking** - portfolio and client reports now show movement over time, including improved domains and resolved findings.
- **Stronger remediation workflow** - Pro and MSP users can now manage findings with owners, due dates, status, comments, and evidence that a fix has been checked.
- **More flexible suspicious-link checks** - the authenticity app now supports more ways to submit suspicious domains for review.
- **Better MSP client reporting** - MSP users now have stronger client-ready reports, branding, report checks, delegated portals, and audit trails.

Free Tier

Free users received several improvements that make scans easier to interpret and easier to trust.

Clearer Scan Findings

Reports now explain results more carefully, especially around website certificates and connection issues. For example, a genuine certificate problem is now described differently from a situation where a firewall or protection service prevented the scanner from completing a check.

This helps reduce confusion and makes it easier to decide whether a result needs action or simply needs a re-check.

Less Noise In Reports

Some lower-priority technical signals are now treated more appropriately as advisory information rather than urgent security problems. The aim is to help users focus on the issues that matter most.

Better Suspicious-Domain Checks

The authenticity app, which helps assess suspicious links and domains, received clearer verdicts and supporting explanations. It is now easier to understand why a domain looks malicious, suspicious, uncertain, probably legitimate, or genuine.

Improved Help And Glossary

Help content and glossary explanations were updated so users can better understand what scan terms mean and how to interpret results.

Pro Tier

Pro users saw the largest improvement in operational workflow and reporting.

Portfolio Progress Tracking

The Portfolio area now gives a clearer view of whether the tracked domain estate is improving or getting worse. It can show:

- domains that improved
- domains that declined
- average score movement
- new findings
- resolved findings
- overall movement across the portfolio

This is designed for teams managing several domains who need a quick answer to: “Are we making progress?”

Priorities Workflow

The Priorities page now works more like a remediation board. Users can track findings with:

- status
- owner
- due date
- accepted-risk expiry
- comments
- history
- overdue indicators
- evidence that a fix has been checked

This helps turn scan results into a practical weekly action list rather than a static report.

Better Progress Reporting

Reports now include clearer progress language, including short summaries of what changed recently. Where enough history exists, reports can also use longer time windows to show whether posture is improving over time.

This makes reports more useful for management updates, compliance conversations, and quarterly reviews.

Non-Intrusive Asset View

Pro users now have an asset view showing infrastructure already seen in completed non-intrusive external checks, such as domains, subdomains, DNS hosts, mail hosts, IPs, and takeover-risk

indicators.

This helps teams spot forgotten or overlooked public-facing assets without adding intrusive scanning.

Verified-Owner Controls

Pro users can now prove control of a domain using a DNS record and, with a separate consent step, run a clearly labelled verified-owner check across the verified domain and known subdomains already observed in scan history.

This remains conservative and non-intrusive. It does not add penetration testing, password testing, large crawling, or internal network scanning.

More Ways To Submit Suspicious Domains

The authenticity workflow now supports more intake options. Suspicious domains can be submitted manually, from pasted email content, or through browser, Slack, and Teams workflows.

Everything lands in one review queue, making it easier to manage investigations.

MSP Tier

MSP users received major improvements for client management and reporting.

Client-Ready Report Bundles

MSP reports are now better suited for client conversations. They are ordered around the domains needing attention first and include clearer progress context.

This helps MSPs show not only what is wrong, but what is improving.

Report Check Before Download

Before downloading a client report, MSP users now see a report check screen. It highlights:

- who the report is prepared for
- who prepared it
- whether branding is present
- how many domains were scanned
- which domains need the most attention
- whether any domains have not yet been scanned

This reduces the chance of sending an incomplete or poorly labelled report.

Prepared By And Prepared For

Client reports now include dedicated Prepared by and Prepared for fields. This makes reports feel more professional and avoids manual editing after export.

Client Branding And Audit Trail

MSPs can manage client report branding and keep a simple audit trail of report branding changes, logo uploads, invites, portal access, and access revocation.

This supports better client governance without adding unnecessary complexity.

Delegated Client Portal

MSPs can invite client contacts into a read-only client portal. Clients can view their own dashboard and reports without being able to edit domains, schedules, alerts, or other client records.

Client Progress Narratives

Client dashboards and client portals now include plain-English progress summaries. This makes it easier to have regular client conversations about risk reduction and ongoing work.

Reliability And Product Quality

Behind the scenes, we also improved scan reliability, preview performance, caching, app loading behaviour, and pre-release checks. These changes are mostly invisible, but they help make the product

feel faster and more dependable.

We also tightened the way reports describe external security evidence, so customer-facing language is clearer and less supplier-specific.

Closing

Thank you for using MyDomainRisk. May’s improvements were all aimed at the same goal: making external security monitoring easier to explain, easier to act on, and easier to share with the people who need to understand progress.

The MyDomainRisk team