MyDomainRisk

EXECUTIVE BRIEF

August 2026 Product Update

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

PERIOD
August 2026

PREPARED FOR
Signed-up users

PUBLISHER
Huro Data Technologies Ltd

FREE TIER
AI assistant now on every plan

PRO TIER
Scans you can follow and stop

MSP TIER
Client report correction

MyDomainRisk August 2026 Product Update

Newsletter for signed-up users
3 September 2026

Contents

Sections and subheadings included for review planning.

August brought the AI assistant to every plan, including Free, and put a set of common answers in front of it that cost nothing at all. The rest of the month went on something less visible and rather more important: checking our own work. Several findings were overstating a problem, one piece of advice was firing on a perfectly correct configuration, and a credential figure had been reading the wrong way round. All are corrected, and where a domain was being held back unfairly, its score improves.

Summary

This month, MyDomainRisk improved in five main areas:

- The AI assistant is now available on every plan, including Free, with a set of common questions answered instantly and free of charge.
- We corrected how credential findings are counted and described, which improves the score of a number of domains that were being held back unfairly.
- A domain we could not read properly now returns no score and says why, rather than a low score that looked like a verdict.
- Several checks that were overstating a problem have been corrected, including one that told every Microsoft 365 customer their email was unencrypted.
- Independent security testing was carried out across the apps, with the findings closed.

Free Tier

The AI Assistant Is Now On Every Plan

The in-app assistant used to be a paid feature. It is now available on every plan, including Free, with an allowance of 30 questions a month that resets on the first.

Alongside that, a set of common questions is now answered instantly from a written answer rather than by the model. **Those answers are free and are never counted against your allowance**, however many you ask.

They are also now browsable. Previously there was no way to find them at all: no page, no link, so the one free route through the product was effectively invisible. They now appear on the Help page under **Common questions**, and in the assistant itself when you open a new conversation.

The assistant on every plan

The Assistant Understands More Of The Product

The assistant applies a scope check before answering, and that check had drifted behind the product. Terms that appear on your own screens, including several of our own findings, were being refused as out of scope.

The scope now tracks the product itself rather than a list someone maintained by hand, so a question phrased in the words you can actually see in front of you gets an answer. Both apps also now share one set of common questions, so a question about authenticity asked in the security app is answered rather than deflected, and vice versa.

Your Score Now Carries Its Own Caveat

On the Free plan some checks draw on a lighter set of external evidence, which means a Free score can only ever be the same or higher than a full scan, never lower. That was already stated, but it sat in small grey text beneath the report where it was easy to miss entirely.

It now appears as a clearly marked note directly under the score itself. If a figure is a floor rather than a final answer, you should not have to hunt for that.

API Access

An account-level API key can now be created and revoked from your Account page on any plan. The key inherits your plan's own limits: it is another way into the same account, not a way around it.

Scores And Findings

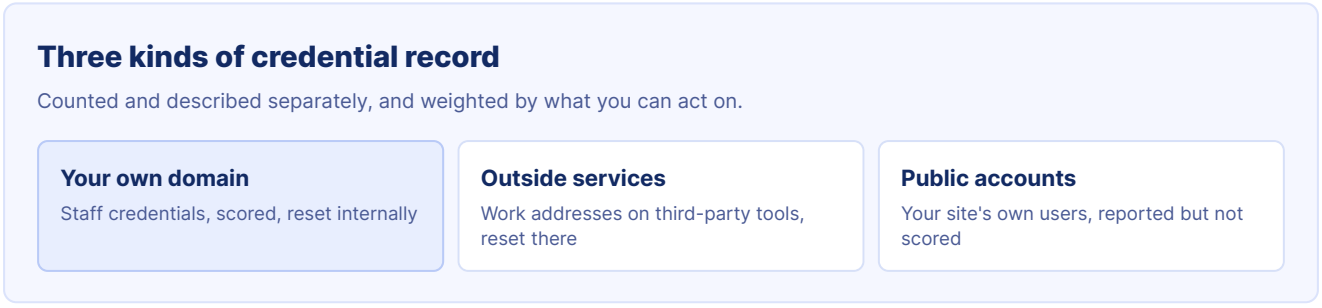
Credential Findings, Counted Properly

Our credential intelligence reports three separate things, and we had one of them the wrong way round for some time: records we described as supplier contacts with access to your organisation#8220;supplier contacts with access to your organisationsupplier contacts with access to your organisation#8221; are in fact **your own people's work addresses appearing on outside services**, such as a booking tool, a service desk, an expenses or recruitment platform.

That is close to the opposite meaning, and it mattered beyond wording. Those records were weighted as though they were staff credentials on your own domain, which held a number of otherwise healthy domains below the band they had earned.

The two are now counted and described separately, and weighted according to what you can actually do about them. **If your domain was affected, its score improves on the next scan.** The action is different too: for records on an outside service, the fix is a password reset on that service, not anything inside your own systems.

Records belonging to members of the public who hold an account on your site are reported separately again, and are not scored, because nobody at your organisation can reset those passwords.



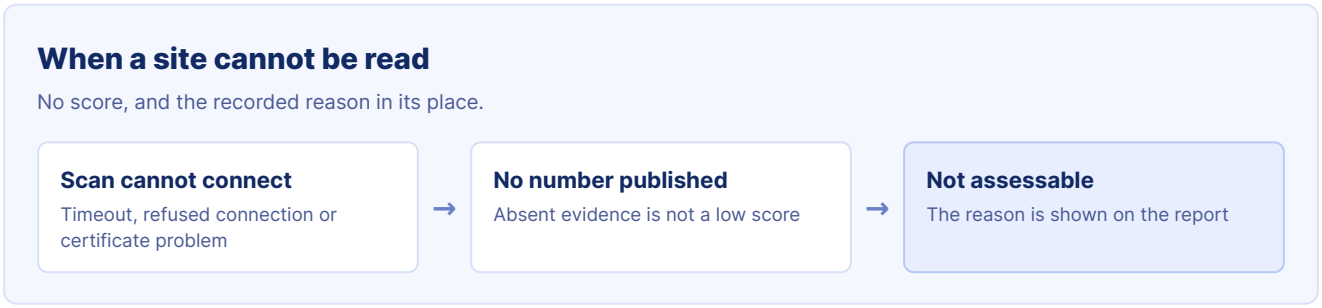
Credential findings, counted properly

A Site We Cannot Read No Longer Gets A Low Score

If a website refused our connection or did not respond properly, the scan used to publish a score anyway. That score was not wrong about what we saw; it was wrong about what it implied, because most of the missing points were simply absent evidence.

Those scans now complete as **Not assessable**, with the recorded reason, whether a timeout, a refused connection or a certificate problem, shown in place of the number. We would rather publish no score than a misleading one.

Related, a domain that refused our connection is no longer reported as having broken encryption. Those are different problems with different causes, and one was being reported as the other.



Not assessable, with the reason recorded

Checks That Were Overstating A Problem

Several checks were corrected this month after review:

- Email-authentication advice was firing on one of the **commonest correct configurations**, recommending a change that would not have helped.
- A credential finding raised a high-severity "you may be compromised"#8220;you may be compromised"you may be compromised"#8221; for addresses that were not the customer's to begin with.
- **PCI DSS was grouped under a US heading.** It is not a US standard: it applies to anyone who takes card payments, including a UK charity with a donate button. It now has its own section, and only the genuinely US-specific privacy items sit under the US heading.
- Websites hosted on large shared platforms were picking up findings that described the platform rather than the site.

None of these were faults in the underlying checks. They were faults in what we said about the results, which is the part you actually read.

Pro Tier

Scans That Tell You What They Are Doing

Scan progress now advances as each stage completes, rather than sitting on one figure. A running scan can be stopped from the domain list, and the control now looks like what it is.

A domain is also scanned once at a time. Starting a scan for a domain already being scanned no longer queues a duplicate.

Domains That Only Answer On www

If a tracked address has no public DNS record but the same address with a leading **www.** does answer, the scan now retries there and gives you a complete result. The tracked name changes only if that full retry produces a real score, and the report says so when it happens.

Deleting A Domain Is Now Contained

Removing a domain from your Dashboard no longer empties it from a Portfolio client that also tracks it. Before deleting, the app now shows exactly which clients and bulk scans hold that domain.

MSP Tier

A Compact Toolbar For Client Domains

Selecting one or more domains inside a client opens a compact toolbar: scan the selection, stop active scans, apply or clear a tier, apply or clear an assignee, or delete. Each icon names its action on hover and to a screen reader, and the stop and delete confirmations remain written out in full.

Delegated Access Follows Your Plan

Delegated client-portal access is an MSP capability, and it now ends when an MSP plan does. Previously an invited contact kept access indefinitely after a downgrade. Access records are not deleted: a downgrade pauses access rather than revoking it, and revocation remains a separate, audited action.

A Correction To The Client Report

The client-ready report told **every Microsoft 365 customer** that their email was not encrypted in transit. Microsoft enforces encryption at their end; our check was looking in a place where the answer could not appear, and then reporting the absence as a finding.

If you sent a client report during August that carried that line, it was wrong, and a fresh report will not repeat it.

Privacy, Reliability And Product Quality

Independent security testing was carried out across both apps during August. The findings were closed and the results reviewed; one reported issue was withdrawn after testing showed it was not reachable.

We found that our email system recorded a message as **sent** once our provider had accepted it, whether or not it was then delivered. A small number of sign-in links in August reached that state and never arrived, while our own records showed success, so if you requested a link in August and it did not come, that is the likely reason. Delivery is now recorded from the provider's own confirmation, and accepted-but-not-delivered is visible as exactly that.

Scheduled reminder emails now leave a durable record of each send, so a message that failed or was sent twice is visible on our side rather than only on yours.

We also completed further dependency and infrastructure work, including changes that let the service run across more than one instance without duplicating your scheduled scans or your emails.

> ### One Question, If You Have A Moment
>
> Plenty of people run a scan, read their report, and we never hear from them again. If that was you, we would genuinely like to know what you expected that you did not get.
>
> A reply to this email with a single line is more useful to us than any amount of guessing on our part. It goes to a person, not a form, and we read every one.

What To Try

- Ask the assistant something. It is available on your plan now, and the common questions cost nothing at all.
- If a domain of yours has ever shown credential findings, re-run the scan: the recount may improve its score, and the finding now tells you where the action actually lies.
- If you have a domain that only answers on its **www.** address, try scanning the bare name and see whether it now completes.
- If you saw a low score on a domain that was slow or refused to load, re-run it. It should now say **Not assessable** and tell you why.

Closing

Thanks for using MyDomainRisk. This month's work was mostly a matter of holding our own reports to the standard we ask of the domains we scan: say what you measured, say what you could not, and do not let a confident sentence stand in for evidence.

Next up: making it easier to get your own data out of the product, and continuing to work through the findings whose wording is stronger than what we can actually see.

The MyDomainRisk team