

Why a Unified Cyber Maturity Dashboard

The case for measuring security posture, compliance and risk in one continuously computed view

Published 2026-09-06 Reading time 14 minutes

For CISOs, VPs of Security, GRC leads, vCISOs, and the executives who fund them

Read it now — the PDF opens either way.

Open the PDF

Leave your e-mail and we'll follow up by hand — the PDF opens either way.

you@company.com

Save my e-mail

☐ I agree to be emailed occasionally about new CMDash resources. See the [privacy policy](#).

No email — download directly

Executive summary

The question has not changed; its due date has. “How are we doing?” used to be answered once a quarter, by hand. Continuous disclosure rules, board-accountability laws and contract-gated certification now expect a current answer at any moment.

The estate is fragmented by design. Surveyed organisations run an average of 83 security solutions from 29 vendors, and half their executives say that fragmentation limits their ability to deal with threats.^[1] Each tool is right about its slice. None is responsible for the whole.

Frameworks multiplied; controls did not. The same access review is evidence for SOC 2, ISO 27001, NIST CSF, CMMC and HIPAA. Collecting it five times is

the single largest avoidable cost in a compliance programme.

Third parties are now inside the blast radius. Third-party involvement in confirmed breaches doubled in one year, from 15% to 30%.^[3] A posture view that stops at your own perimeter is missing a third of the picture.

A unified cyber maturity dashboard is a specific thing. It is a continuously computed score from connected telemetry, mapped once to every framework, backed by collected rather than attested evidence, expressed in the language of the people who fund it, and served from one dataset to the operator, the auditor and the board. Section 4 defines each property; section 5 gives ten questions to ask any vendor, including us.

1. The question, and the morning it takes to answer

Every security leader answers the same question, from the CEO, the audit committee, the cyber-insurance underwriter, a prospect's procurement team, a regulator: *how are we doing?* The honest process behind the answer rarely survives being written down. It is a SIEM tab for incidents, a scanner console for open vulnerabilities, an identity console for MFA coverage, an endpoint console for agent health, a compliance tracker for control status, a risk register in a spreadsheet, and a slide deck that reconciles them, by hand, the night before the meeting.

That assembly has three properties that made sense when the question was asked quarterly and no longer do. It is **stale** the moment it is finished. It is **unverifiable**: the number on the slide is whatever the person who built the slide believed. And it is **expensive in the scarcest resource the programme has**, senior attention, because the only person who can reconcile six consoles is the person who understands all six.

A maturity dashboard is not a report about the security programme. It is the programme's instrument panel: the thing you look at to decide what to do next, and the thing you show to prove you looked.

2. Five forces that moved the due date

2.1 Oversight moved from the audit cycle to the board calendar

In 2023 the U.S. Securities and Exchange Commission required public companies to disclose a material cybersecurity incident within four business days of deciding it is material, and to describe their risk management, strategy and board oversight every year.^[5] A four-day clock cannot be met from a quarterly snapshot; the materiality decision has to start from a current picture of what is exposed and what is controlled.

NIST answered the same shift from the framework side. CSF 2.0, published in February 2024, added a sixth core function, **Govern**, that makes strategy, roles, policy and oversight part of the framework rather than an assumption behind it.^[4] In Europe, NIS 2 makes management bodies personally accountable for approving and overseeing cybersecurity risk measures,^[8] and DORA has applied to financial entities and their critical ICT providers since January 2025, with its own incident-reporting and third-party obligations.^[7]

Four regimes, one direction: the people accountable for cyber risk are now named, and they are expected to be able to see it at any time, not at the end of the quarter.

2.2 Frameworks multiplied; controls did not

A mid-market company today can reasonably be asked for SOC 2 by its customers, ISO 27001 by its European partners, HIPAA by its healthcare clients, PCI DSS by its acquirer, CMMC by its defence prime, and NIST CSF by its insurer. The requirement lists are different. The underlying controls are mostly the same: an access review is an access review, whichever framework is asking.

Programmes that treat each framework as its own project collect the same evidence once per framework, keep it in a folder per framework, and answer the same auditor question once per framework. Programmes that map controls once and let every framework read from that map do the work once. The difference is not a matter of tooling preference. It is the largest avoidable line in the compliance budget, and it compounds every time a new framework is added.

2.3 Your perimeter now includes your suppliers

Verizon's 2025 Data Breach Investigations Report found that third-party involvement in confirmed breaches doubled year over year, from 15% to 30%, and that exploitation of vulnerabilities was the initial vector in one breach in five.^[3] DORA's register-of-information requirement and NIS 2's supply-chain provisions turn that finding into an obligation.^{[7][8]} A posture view that scores your own estate and ignores the vendors with access to it is not wrong; it is a third short of complete.

2.4 The board wants a number, then a dollar figure

IBM's 2025 Cost of a Data Breach study puts the global average cost of a breach at USD 4.44 million and the United States average at USD 10.22 million.^[2] Boards that read those figures do not ask whether the programme is "high" or "medium" risk. They ask what the expected loss is, what the proposed spend buys down, and how that compares with the other uses of the money. The same study found that 63% of breached organisations had no AI governance policy at all,^[2] which is the next question the board will ask once the first one is answered.

2.5 Certification became a condition of the contract

For the defence industrial base, the CMMC acquisition rule took effect on 10 November 2025, establishing a three-year phased structure for when CMMC requirements appear in DoD solicitations; that later phase-in has been paused since 2026-07-13 with no resumption date announced. (checked as of 2026-09-15)^[6] A self-assessment score that is wrong is no longer an internal embarrassment; it is a false statement to the government on a contract you may not be eligible to win. The score has to be traceable to evidence, and the evidence has to be current.

3. Why the current answers fail

3.1 The spreadsheet dashboard

The most common maturity dashboard in the world is a spreadsheet with a traffic-light column, refreshed by a senior engineer before each meeting. It has the great virtue of existing. It has every other disadvantage: it is attested rather than

measured, it is current for the afternoon it was built, it cannot show a trend without someone keeping old copies, and it consumes hours of the one person whose hours are most valuable. When that person leaves, the dashboard leaves with them.

3.2 The point-tool mosaic

The second most common answer is to trust the consoles. Each is authoritative about its own domain, and each has a dashboard. The trouble is that none of them is responsible for the whole: the endpoint console does not know which of its unprotected hosts are in scope for PCI, the scanner does not know which findings are on assets that hold CUI, and the identity console cannot say whether a missing MFA enrolment is a compliance gap or a service account. With an average of 83 solutions from 29 vendors in the estate,^[1] the reconciling is the job, and it lands on a human.

3.3 The audit-era GRC platform

Enterprise governance, risk and compliance platforms were built to run the audit cycle, and they run it well. They were not built for the morning briefing. Their unit of work is the assessment, their cadence is the quarter, their pricing assumes a dedicated team, and their implementation is a project measured in months and in professional-services fees. For a large enterprise with a GRC function, that is a reasonable trade. For a mid-market company with one security leader and a fractional GRC resource, it means the platform is either never implemented or never opened.

The test for any of these is the same. When the CEO asks “are we secure?” on a Tuesday at 4pm, can you answer from what is on the screen, and can you show your working?

4. What “unified cyber maturity dashboard” means

The phrase is used loosely, so it is worth being precise. A unified cyber maturity dashboard has five properties. A product missing any one of them is a useful tool

of some other kind.

01 One score, computed, continuous, explainable

The headline is a single grade derived from live signals across the connected estate: patch latency, MFA coverage, open vulnerabilities by severity, incident frequency, control coverage. It recomputes when an integration syncs, not when someone remembers to update it. And it decomposes: any reader can click from the grade to the signal to the asset, and see why the number is what it is and when it last moved.

02 Map once, report to every framework

Controls are the primary object; frameworks are views over them. A control is implemented once, evidenced once, and counted toward every framework that requires it through an explicit crosswalk with a confidence you can inspect. Adding a framework is a mapping exercise, not a new programme. The control text is the publisher's own wording, with its citation, because that is what the auditor will test against.

03 Evidence collected, not collected about

Where an integration can produce the evidence, the dashboard collects it on a schedule, versions it, and flags it stale past a freshness window. Where a person must upload it, the dashboard says so, and says when. Above all it separates three states that are usually conflated: a control that is *implemented*, one that someone has *attested* is implemented, and one that has been *tested* and found working. Most control failures are in the gap between the second and the third.

04 Risk in the language of the people who fund it

A risk register that stops at "high" cannot take part in a budget conversation. The dashboard should express material risks as loss exposure in currency, using an open method such as FAIR with the assumptions visible, and it should produce a plain-language narrative of the top exposures, whether each is improving, and what to do next. The number is for the CFO. The narrative is for the rest of the board.

05 One dataset, three audiences, any number of entities

The operator's view, the auditor's evidence package and the board deck are generated from the same data at the same moment, so they cannot disagree. And the dashboard rolls up: across business units for a group, across subsidiaries for an acquirer, across clients for a vCISO or managed service provider, without re-keying anything.

What it is not

Not a SIEM. It consumes the SIEM's conclusions; it does not replace detection.

Not a document vault. Policies and evidence live in it, but the point is what they prove, not where they are stored.

Not an outside-in rating. External security ratings look at what an attacker can see from the internet. A maturity dashboard looks at what you can see from inside, and can use a rating as one signal among many.

Not another console. If it adds a seventh tab to the six you already open, it has failed at the one thing it is for.

5. Ten questions to ask any vendor, including us

The properties above translate into questions a buyer can put to any product in a demonstration. None of them can be answered with a feature list; each has to be shown.

Is the score computed from connected telemetry, or entered by a person?

An attested score measures diligence at filling in forms. A computed one measures the estate.

When an integration stops syncing, what does the dashboard show?

The honest answer is "stale, since <date>". A dashboard that keeps showing yesterday's green is worse than no dashboard.

Can one control, with one piece of evidence, satisfy every framework it applies to?

If evidence has to be uploaded per framework, the tool has not unified anything. It has added a tab.

Does the control text come from the publisher, or a paraphrase?

Auditors test against the published requirement. A paraphrase is a second thing to argue about.

Does it distinguish "implemented", "attested" and "tested"?

Most control failures in the wild are controls everyone believed were working.

Can it express a risk in currency, with the assumptions visible?

A budget conversation happens in dollars. "High" is not a number the CFO can compare to anything.

Can it roll up across business units, subsidiaries or clients without re-keying?

Groups, acquirers, MSSPs and vCISOs manage a portfolio, not a single workspace.

Is the board output generated from the same data the operator sees?

Two sources of truth eventually disagree, and they disagree in front of the board.

Where does the data live, and can you take it with you?

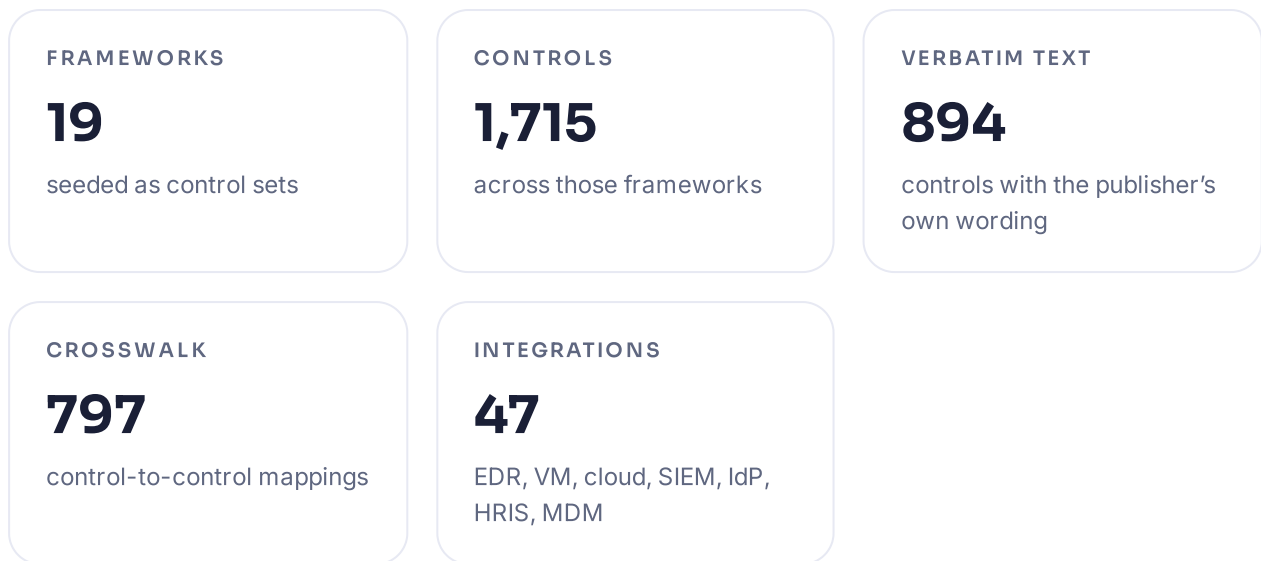
Organization isolation, residency, deployment topology and export format are procurement questions, not afterthoughts.

How long from signup to the first defensible score?

Months of implementation means the tool needs a project to exist. Days means it can survive a budget cycle.

6. How CMDash answers them

CMDash was built to be the instrument panel described in section 4, for the security leader who needs it every morning rather than the GRC team that needs it every quarter. The figures below are computed from the product's own catalogues when this page is built, so they cannot drift from what ships.



Computed score. A live A–F posture grade from up to seven weighted signals, recomputed every 4 hours once a tool is connected and on demand, with 30- and 90-day trend and an industry reference baseline to compare against.

Map once. A crosswalk engine with confidence scoring, publisher-verbatim control text where the framework's text is public-domain, and CSV import of your own licensed copy where it is not.

Collected evidence. Scheduled collection from integrations, dated manual evidence, freshness windows, continuous-control-monitoring drift detection, and control-efficacy validation that records tested separately from attested.

Risk in dollars and in English. FAIR loss-exposure modelling with visible assumptions, and a risk register with treatment plans.

One dataset, three audiences. Operator dashboard, auditor evidence packages, POA&M export, and one-click board decks generated from the same data, with multi-business-unit and vCISO client roll-ups.

What we do not claim

Not every framework has shipped connector rules; CMMC Level 1, CMMC Level 2, HIPAA and the AI-governance frameworks are tracked as real controls with owners and evidence, attested by you. Frameworks published under copyright are shown by scope and source, not reproduced. The [per-framework pages](#) state each of these limits explicitly, and the [AI governance](#) page says in its first paragraph what is and is not automated. We would rather you read that before the trial than discover it during one.

7. A thirty-day path

Day 1. Connect one endpoint, one identity and one vulnerability source. Read the first score, and the explanation under it.

Week 1. Pick the framework a customer or regulator is asking for most urgently. Map, mark the controls you already run, and let the integrations fill in what they can.

Week 2. Add the second framework and count how many of its controls were already satisfied by the first. That number is the crosswalk paying for itself.

Week 3. Put the top three risks in the register with a loss-exposure estimate. Generate the board snapshot and compare it with the slide you built by hand last quarter.

Week 4. Decide whether you would rather have the dashboard or the hours back. That is the whole purchase decision.

References

IBM Institute for Business Value, with Palo Alto Networks. "Capturing the cybersecurity dividend: How security platforms generate business value." 2025. <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform>
Cited for: Surveyed organisations run an average of 83 security solutions from 29 vendors; 52% of executives say fragmentation of security solutions limits their ability to deal with threats. Checked 2026-09-06.

IBM. "Cost of a Data Breach Report 2025." 2025. <https://www.ibm.com/reports/data-breach>
Cited for: Global average breach cost of USD 4.44 million; United States average of USD 10.22 million; 63% of breached organisations had no AI governance policy. Checked 2026-09-06.

Verizon. "2025 Data Breach Investigations Report." 2025. <https://www.verizon.com/business/resources/reports/dbir/>
Cited for: Third-party involvement in confirmed breaches doubled year over year, from 15% to 30%; exploitation of vulnerabilities was the initial vector in 20% of breaches. Checked 2026-09-06.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." 2024. <https://www.nist.gov/cyberframework>
Cited for: CSF 2.0, published February 2024, added a sixth core function, GOVERN, covering strategy, roles, policy and oversight of cybersecurity risk. Checked 2026-09-06.

U.S. Securities and Exchange Commission. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." 2023. <https://www.sec.gov/newsroom/press-releases/2023-139>

Cited for: Registrants must disclose a material cybersecurity incident on Form 8-K within four business days of determining materiality, and describe risk management, strategy and board oversight annually. Checked 2026-09-06.

U.S. Department of Defense, Office of the CIO. "Cybersecurity Maturity Model Certification (CMMC) Program." 2025. <https://dodcio.defense.gov/CMMC/>

Cited for: The CMMC acquisition rule (48 CFR) took effect on 10 November 2025, establishing a three-year phased structure for when CMMC requirements can appear in DoD solicitations. Rollout timing for later phases is not fixed and can change — check current DoD CIO guidance before relying on a specific date. Checked 2026-09-06.

European Union. "Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)." 2025. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

Cited for: DORA has applied to EU financial entities and their critical ICT providers since 17 January 2025, including ICT risk management, incident reporting and third-party risk obligations. Checked 2026-09-06.

European Union. "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2)." 2024. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

Cited for: NIS 2 member-state transposition was due by 17 October 2024 and makes management bodies accountable for approving and overseeing cybersecurity risk-management measures. Checked 2026-09-06.

CMDash figures in section 6 are derived at build time from the product's shipped framework and integration catalogues. External figures are quoted from the sources above as of the date shown against each; if a publisher revises a figure, the reference will be out of date until the next revision of this paper. Last revised 2026-09-06.

Not ready to trial today?

Get the next paper

One email when a new white paper publishes. Nothing else.

Notify me

☐ I agree to be emailed when a new CMDash white paper publishes. See the

[privacy policy](#)