VERITYPOINT SECURITY · SIGNALBOARD

User Manual

The independent executive assessment of your Microsoft 365 environment. How to run it, how to read it, and what to do with what it tells you.

Product	SignalBoard
Operated by	JJS Partners, LLC d/b/a VerityPoint Security
URL	https://signalboard.veritypointsecurity.com
Manual version	2.0
Document date	July 2026
Audience	CEOs, CFOs, owners, board members, IT and MSP leaders
Sign-in	Microsoft 365 account (read-only)
Support	hello@veritypointsecurity.com

> This manual is the executive companion to the platform. For the legal document covering data handling, retention and GDPR, see **Privacy & Legal** in the dashboard, or **/legal.html**.

Contents

Twenty sections. Section 14 is the one most people skip and shouldn't.

1. What SignalBoard is — and what it refuses to be

One minute. What this is, who it is for, and the promises it keeps.

SignalBoard is an **executive bridge**. It reads your Microsoft 365 environment directly from Microsoft, and turns what it finds into a business judgement an executive can act on — without becoming a security expert first.

It exists because most leadership teams have no independent way to answer a simple question: *is our technology environment actually healthy, and is it getting better?* The people who run the environment are also the people who report on it. SignalBoard is the second opinion.

Who it is for

- CEOs, CFOs, owners and board members who need a defensible read on posture each quarter.
- Lean IT teams and MSPs who want a consistent executive readout they don't have to hand-build.
- Insurance brokers and underwriters who want clean evidence at renewal.

What it will never do

- **It never changes anything.** Every permission SignalBoard holds is read-only. It cannot alter a policy, a licence, a user or a setting — by design, not by policy.
- **It never guesses.** If a control cannot be read, SignalBoard says so and withholds the grade rather than averaging around the hole. See Section 17.
- **It never blames the wrong party.** When something fails, the product tells you whether the cause is your licence, your permissions, or our own bug — and says which.
- **It never sends your data to an AI vendor on your behalf.** Ask AI assembles a prompt for you to review and paste. Nothing leaves without your click.

> The single design rule: **SignalBoard would rather tell you nothing than tell you something false.** Everything else in this manual follows from that.

2. Getting access: subscription, consent, seats

Three things happen once. After that, signing in is just signing in.

Step 1 — Subscription

SignalBoard is licensed **per tenant**, not per user. Your Microsoft 365 tenant ID is the key. Any authorised person from a licensed tenant can use the platform; nobody needs their own licence.

Step 2 — One consent, once

A Global Administrator approves SignalBoard's read-only permissions **one time, for the whole organisation**. That is the only administrative act required, ever. Buying an additional capability later never re-prompts for consent.

After consent, SignalBoard reads your tenant using its **own application identity** — not the signed-in person's. That matters more than it sounds: a CFO with no admin role can run a full assessment and get a complete score, because the reading is done by the application, not by them. Nobody needs to be made an administrator to see their own company's posture.

Step 3 — Authorized Users (5 seats)

A tenant may have up to **five people who can sign in**. The first person to sign in becomes the administrator of that list and can add or remove the others from **Setup** → **Authorized Users**.

> This is a **login** limit, not a save limit. (Earlier versions of this manual described a save-based seat model. That is no longer how it works.)

3. Running an assessment

One click. Between forty seconds and a couple of minutes, depending on how much you have.

Starting

Press the centre of the octagon. That's it. There is no configuration, no scope to choose, no agent to install.

What you are watching

The octagon assembles a section at a time, and each section lights as its evidence actually lands — it is a live readout, not a progress bar with a fake percentage. Beneath it, the **Evidence Ledger** lists what has been read, with real counts. The executive watches SignalBoard read things they did not know it read.

Past about eight seconds a quiet line of type begins drifting across, one thought every twenty seconds. It is there because a long wait shouldn't feel like a stall. It never claims to know how long is left, because we don't.

How long it takes

Typically 40–90 seconds. A large tenant takes longer, and SignalBoard **does not sample** — it reads everything, which is precisely why the number is worth having. If it runs long, the product will tell you so, in plain words, and will not invent an excuse.

> **One assessment at a time.** If a scan is already running, starting another cannot make the first finish faster — it can only make both slower. SignalBoard will decline, and say so.

4. The command bar: your ten chapters

The dashboard is a narrative, numbered in the order an executive actually asks the questions.

Across the top sits a numbered bar. Each entry answers one question, and they are ordered the way a board meeting runs — the score, then why, then what to do, then the evidence.

#	Chapter	The question it answers
1	Overall Health	Where do we stand this quarter?
2	Why This Score	What is actually driving the number?
3	Next Steps	What should leadership do first?
4	Workspace	Your command center — open anything, rescan, generate board materials.
5	Trend Analysis Workspace	Are we getting better — and where?
6	Reports	Every board-ready output in one place.
7	Shield	What does our posture look like, as one picture?
8	Vault Library	Every assessment we've kept, in one secure place.
9	Insurance	Can we evidence our controls at renewal?
10	AI Governance	Is our Copilot / AI adoption governed?

Behind a **Show Governance Modules** toggle sit five more: Service Health, Security & Risk, Policies, Licensing and Domain Governance. They are hidden by default so the first screen stays clean — but they are where a great deal of the value lives, and Section 14 is devoted to them.

5. Overall Health

The single independent number, and its direction.

One score, 0–100, with a letter grade — the weighted health of eight operational domains. Beneath it: the direction of travel since last quarter, and whether that movement is real or noise.

This is the number you can take to a board. It is independent — it does not come from the people who run your environment — and it is reproducible: the same tenant, unchanged, produces the same score.

> If SignalBoard could not read every domain, **it does not show you a grade at all.** It shows coverage instead. See Section 17 — this is the most important rule in the product.

6. Why This Score

The number, decomposed. No executive should have to take a score on faith.

Eight domains around a centre, each with its own grade and score. Strong ones hold the number up; failing ones pull it down, and you can see exactly which is doing which.

Alongside: **Biggest Strengths** and **Biggest Risks**, each written in business language — what the domain protects, and what happens if it is weak. Not 'Conditional Access policy coverage is 29%', but 'whether MFA is actually enforced, and whether risky sign-ins are challenged'.

Click any domain to open its **Executive Guide** — an explanation written for the person who has to decide something, not for the administrator who has to configure it. We deliberately do not link you to Microsoft's documentation: that would hand the explanation of our own score to someone else, in a language you did not ask for.

7. Next Steps — the Executive Action Plan

Four moves, in order, that leadership can actually make.

Step	What it does
1. Validate	Put the findings in front of the people who run the environment — and ask them to confirm or correct.
2. Assess	Open Insurance Readiness and see what you could evidence today.
3. Build the narrative	Assemble the board paragraph — the story behind the number.
4. Track	Save the quarter so next quarter has something to compare against.

None of these steps is technical. That is deliberate: the action plan is for the person who decides, not the person who configures.

8. Workspace

The command center.

Every capability, one click away. Run a rescan. Generate board materials. Open any governance module. If you don't know where something lives, it lives here.

9. Trend Analysis Workspace

The question no single scan can answer: are we actually getting better?

A single scan tells you where you stand. Only a trend tells you whether the money you spent last quarter did anything — and that is the question a board will eventually ask.

- Your score over time, against a best-practice line and a target band.
- Per-domain movement — which areas improved, which slipped, and by how much.

- The biggest movers, called out, so you don't have to hunt for them.
- A plain-language **'So what?'** that interprets the shape of the line rather than leaving you to.

> This is the tab that turns SignalBoard from a report into a **management instrument**. A score is a photograph; a trend is accountability.

10. The Executive Shield

Your posture as one picture — the only view a CEO understands without reading a number.

Eight control areas rendered as one protective structure, shown twice: **best practice** on the left, whole and luminous; **your posture** on the right.

A module at full strength is razor-sharp and brightly lit. A weakened one goes soft, desaturated and faint — but it **stays in place**. It does not vanish. That distinction is the whole design: a hole would read as 'missing data'; a ghost reads as *'present, but not protecting you'* — and only one of those is true.

Nobody has to explain this slide. The eye does the arithmetic before the brain arrives. It is also slide 2 of your board deck, for exactly that reason.

11. Vault Library

Every assessment you've kept, in one secure place. No files to manage.

Save each quarter's assessment; open, compare and archive them later. Saved assessments are encrypted, scoped to your tenant, and are what the Trend Analysis Workspace is built from.

> Deleting an assessment from the Vault also removes that point from your trend. If you want to keep the quarter on the line, keep the assessment.

12. Reports

Every board-ready output in one place.

Output	For
Quarterly Leadership Briefing	The short written summary — what changed, what matters, what you're being asked to approve.
Full PDF report	The complete record, including the technical appendix for your IT team, MSP and auditors.

Output	For
Visual Executive Edition (deck)	The board presentation. Opens on the score, then the Shield, then the priorities.
Classic deck	The same substance, conventionally laid out — for audiences who prefer it.

Both decks are generated from the same assessment data. They cannot disagree with each other, and neither can disagree with the dashboard.

13. Executive Questions & Insights

A knowledge center, not a FAQ.

The questions a leadership team actually asks — *'is this good?'*, *'what would our insurer think?'*, *'is our MSP doing what we pay them for?'* — answered in the context of **your** assessment, with your numbers in them.

14. GOVERNANCE MODULES — the independent audit layer

Five modules, hidden behind one toggle, that answer the questions nobody inside your organisation is incentivised to answer.

The first thirteen chapters tell you **how healthy you are**. The Governance Modules tell you something harder and more valuable: **whether the people responsible for that health are actually doing the job** — and whether you would know if they weren't.

Every one of these modules exists because of the same structural problem. The party who runs your technology is also the party who reports on it. Your MSP tells you patching is current. Your IT lead tells you policies are enforced. Your licence reseller tells you the spend is right. None of them are lying — but none of them are independent, and none of them are audited.

> **This is the accountability layer.** SignalBoard reads these signals from Microsoft directly, on its own authority, with nobody in between. It is not adversarial and it is not a scorecard on your staff. It is simply the difference between *being told* and *knowing*.

They live behind a **Show Governance Modules** toggle because the first screen an executive sees should answer the first question, not every question. Turn them on when you want to go from 'how are we?' to 'who owns this, and is it being handled?'

Module	The board-level question it answers
Service Health	Are the Microsoft services we depend on healthy right now — and would we be told if they weren't?
Security & Risk	What is exposed, and what needs executive attention rather than IT attention?
Policies	Are our security policies merely configured, or actually enforced?
Licensing	What are we paying for, what do we use, and what are we leaving on the table?
Domain Governance	Do we know who owns our Internet identity — and is it being properly governed?

14.1 Service Health

An independent early-warning view of the Microsoft services your business runs on.

When Exchange, Teams or SharePoint degrades, the question is rarely 'is it down?' — you find that out from the complaints. The question is **'did anyone tell us, and did anyone act?'**

Service Health reads Microsoft's own service advisories for *your* tenant and shows what is healthy, what is degraded, and what incidents are open right now — independently of whether your provider passed the message on.

Why it matters to leadership

- It closes the gap between an incident starting and leadership hearing about it.
- It gives you a record: when there was an outage, what was affected, and for how long — useful when a customer or regulator asks.
- It is the difference between an MSP that watches your tenant and one that reacts to your phone call.

14.2 Security & Risk

What is exposed — filtered to what an executive should actually look at.

Your security posture and the risks that need **executive** attention, as distinct from the hundreds that need IT attention. Most security tooling produces a queue for administrators. This produces a shortlist for a board.

Each item is stated as a business consequence, not a control name — what could happen, who it would affect, and whether it is getting better or worse.

14.3 Policies — configured vs. enforced

The most valuable distinction in the entire product.

A policy that exists is not a policy that works. Conditional Access can be written and left in **report-only** mode. MFA can be required — and excluded for a group somebody added last year. DMARC can be published at p=none, which means it watches impersonation happen and does nothing about it.

In every one of those cases, an honest administrator will tell you, honestly, that the policy is **in place**. And they are right. It is also doing nothing.

> **Policies is the module that catches the gap between the box being ticked and the control actually protecting you.** It reads what is configured, and separately reads whether it is *enforced* — and reports where those two things disagree.

This is not a hypothetical failure. It is the single most common finding in the product, and it is almost never anyone's fault: policies get created in monitor mode with the intention of enforcing them later, and later never arrives. Nobody is lying to you. Nobody is checking, either.

14.4 Licensing — what you own vs. what you use

The module that most often pays for the subscription outright.

Microsoft licensing is deliberately hard to reason about, and almost every organisation is simultaneously **overspending** and **under-using**. Both at once. Licensing shows you three things:

- **What you own** — every SKU and service plan in the tenant, and how many are actually assigned.
- **What you already have but never turned on.** The capability is paid for, sitting in the licence, switched off. This list is usually longer than anyone expects — and every line on it is a security or productivity improvement available at **zero additional cost**.
- **What you are paying for and nobody uses** — assigned licences with no activity behind them.

There is also an **Executive Portfolio** view that organises Microsoft's products by *business function* rather than by product name, and marks the ones you already own. It answers a question executives ask constantly and rarely get a straight answer to: *'do we need to buy something for this, or do we already have it?'*

> The most expensive software in most organisations is **the software they already own and never switched on.** This module is how you find it.

14.5 Domain Governance — your Internet identity

The one that will wake you up at night, and the one nobody owns.

Your domain *is* your business online. It is your email, your website, your identity to every customer, bank and regulator you deal with. And in most small and mid-sized organisations, **nobody owns it** — it was registered years ago, by someone who may have left, on an account nobody can name.

What this module reads

- **Registry expiry** — when each domain lapses, with a warning as it comes due. An expired domain is not a technical problem; it is a business outage with a date on it. Email stops. The website stops. You cannot reset a password because the reset goes to a mailbox that no longer exists.
- **Ownership and registrar** — who holds it, where, and whether that is still someone you employ.
- **Email authentication** — SPF, DKIM and DMARC. Whether a stranger can send mail that appears to come from you. (And whether DMARC is set to p=none, which means you are watching it happen — see 14.3.)
- **DNS integrity** — DNSSEC, name servers, and whether your DNS answers can be forged.
- **Public web posture** — HTTPS enforcement, HSTS, security headers, TLS certificate and expiry, SSL grade, CDN/WAF. Read live, from the outside, exactly as an attacker or a customer would see it.

Each domain carries a one-glance verdict — **Expiring 12d**, **No DMARC**, **No SPF** — so the one that matters is the one you see first. You should never have to read seven rows to find the emergency.

> You can also check **any** domain on demand, not just the ones verified in your tenant — a domain you are about to acquire, a supplier's, or one you suspect is being used to impersonate you.

15. Insurance Readiness

Underwriting-ready evidence of your controls, before your broker asks.

A control checklist mapped to recognised frameworks (CIS, NIST, HIPAA), combining what SignalBoard **measured** from your tenant with what you **attest** to yourself.

The two are always kept apart and always labelled. A measured control is evidence. An attested control is a statement. An underwriter treats them very differently, and so do we — a product that blurred the line would be helping you mislead your own insurer.

At renewal, this is the difference between a conversation and a questionnaire.

16. AI Governance

Govern Copilot and enterprise AI the way a board expects to see it governed.

AI arrived in your Microsoft 365 tenant whether or not anyone decided it should. Copilot reads what your staff can read — which means your AI exposure is exactly your data-access exposure, and most organisations have never measured that.

- Which AI capabilities you own, which are switched on, and who administers them.

- **Data readiness** — because Copilot is only as safe as the permissions underneath it. Oversharing that was survivable when a human had to go looking becomes serious when a machine will summarise it on request.
- Whether sensitivity labelling exists at all — and if it doesn't, that is a finding, not a blank.
- Adoption: who is licensed, who actually uses it, and what that spend is returning.

17. How the score works — your score cannot be bought

Two promises the whole product hangs on. Read this one.

The score is the weighted health of eight operational domains, 0–100, with a letter grade. Green is 85+, amber 70–84, red below 70.

The rule: missing information may never improve your score

If SignalBoard cannot read a domain, it does **not** quietly average the remaining ones and hand you a grade. That would mean a tenant with *less* visibility scores *better* — and a score that rewards blindness is worse than no score, because people will act on it.

Instead SignalBoard withholds the grade entirely and shows you **coverage**: how much of your environment it could actually see, and precisely which domains it could not. You are told what you don't know.

> **A missing measurement is never a passing measurement.** If we cannot see it, we say so — and you get no grade until we can.

Your score cannot be bought

The Overall Health score is the weighted health of eight operational domains, and **nothing you purchase can change it**. Insurance Readiness and AI Governance are separate capabilities with separate scores. Buying one gives you a new *view* — never a better *grade*.

This is not a detail. If buying a module could move the number, the number would be **for sale**. Two identical organisations would grade differently based on what they had paid for. Your score would stop being comparable across quarters the moment you added a capability. And “your score went up” could mean “you bought something” rather than “you got safer.”

> **The score is the one thing in SignalBoard that money cannot touch.** It is the same eight domains, weighted the same way, for every organisation, in every quarter, at every price. That is what makes it worth taking to a board — and it is the whole reason the product exists.

The same principle runs the other way: a module you have *not* bought never drags your score down, and never leaves a hole in it. What you own changes what you can **see**. It never changes what you **are**.

Measured vs. attested

Anything SignalBoard read from Microsoft is **measured**. Anything you told us is **attested**. These are labelled everywhere they appear, and never mixed into a single number without saying so.

Why a control might be unreadable

Cause	What fixes it
Licence	Your Microsoft plan doesn't include the capability. No permission change can unlock it — only a licence change.
Consent	The one-time admin approval hasn't been given. A Global Administrator approves it once.
Microsoft	Occasionally Microsoft's own API misbehaves. We say so, and never dress it up as your problem.

SignalBoard always tells you which of the three it is. Sending an executive to their IT team to fix a licensing problem — or to buy a licence to fix a consent problem — wastes everyone's time and costs us your trust the second time we do it.

18. When something goes wrong

It shouldn't. If it does, the product is built to tell you why rather than to look away.

Need help?

In the menu. It opens a window where you can send a message, or book time directly. If anything has gone wrong in your session, you can tick one box to attach the technical detail — you see exactly what will be sent before it goes, and nothing is ever sent without that click.

The diagnostics page

If a support conversation needs more, we may ask you to open **/errors.html**. It shows everything your browser recorded while SignalBoard was running: every failed request, what Microsoft said, who was signed in, and — importantly — **what is actually wrong and what would fix it**.

Press **Send this to SignalBoard** and it comes straight to us, already diagnosed. You do not have to describe the problem. We can read it.

> Nothing on that page is confidential. Access tokens, passwords, your data and your scan results are stripped out **before** anything is written down — not filtered out afterwards. And nothing leaves the page until you press Send.

Common messages

You see	It means
“Your tenant is not licensed for this feature.”	A Microsoft licence limit — usually Entra ID P2. Consent cannot fix this; only a licence can.
“Additional permissions are required.”	The one-time admin consent hasn't been granted yet. A Global Administrator can approve it for the whole organisation.
“An assessment is already running.”	Exactly that. A second one would only slow the first down. Give it a moment.
“This is taking longer than usual.”	A large tenant. Nothing is wrong — SignalBoard is still reading, and it does not sample.

19. Your data

Short version: read-only, tenant-scoped, encrypted, and yours to delete.

- **What we read.** Microsoft 365 *configuration* — via read-only Microsoft Graph permissions. Never passwords, never tokens, never the contents of documents or email.
- **What we change.** Nothing. There is no write permission anywhere in the product.
- **Where it lives.** Encrypted at rest in Azure, scoped to your tenant, access-controlled through Microsoft Entra ID.
- **How long.** For the life of your subscription. On lapse: a 30-day export window, then permanent deletion.
- **Deleting.** You delete assessments yourself, from the Vault Library. It is immediate.
- **AI.** SignalBoard does not send your data to any AI vendor. Ask AI builds a prompt for you to review and paste yourself.

The full Privacy Policy and Data Processing Addendum are at **/legal.html**.

20. Support, and a glossary

Where to write, and what the words mean.

Topic	Email
General questions	hello@veritypointsecurity.com
Privacy / GDPR / DPA	privacy@veritypointsecurity.com
Security / vendor risk	security@veritypointsecurity.com
Book time	Use “Need help?” in the menu — it books directly.

Glossary

Term	Plain meaning
Assessment	One complete reading of your tenant. What older versions called a “scan”.
Coverage	How much of your environment SignalBoard could actually read. Below 100%, no grade is issued.
Measured	Read from Microsoft. Evidence.
Attested	Stated by you. A statement, not evidence — and always labelled as such.
Enforced	A policy that is actually acting. As opposed to merely configured. See 14.3.
Tenant	Your Microsoft 365 organisation. The unit SignalBoard is licensed to.
Seat	One of five people who may sign in to your tenant's SignalBoard.
Governance Modules	The five independent audit modules behind the toggle. Section 14.
DMARC p=none	Email protection that watches impersonation happen and does nothing. Configured, not enforced.
Secure Score	Microsoft's own scorecard of your tenant. Underwriters and auditors recognise it.

End of manual. Questions or corrections: hello@veritypointsecurity.com
Full Privacy Policy and DPA: https://signalboard.veritypointsecurity.com/legal.html