USER MANUAL

SignalBoard

Executive scorecard for Microsoft 365 security posture. How to sign in, run a scan, read your score, and manage your saved data.

Product	SignalBoard
Operated by	JJS Partners, LLC d/b/a VerityPoint Security
URL	https://signalboard.veritypointsecurity.com
Manual version	1.0
Document date	June 2026
Audience	CEOs, CFOs, business owners, board members, IT leaders
Sign-in	Microsoft 365 admin credentials
Support	hello@veritypointsecurity.com

*This manual is the executive companion to the platform. For the legal and contractual document covering data handling and GDPR, see **Privacy & Legal** in the dashboard or https://signalboard.veritypointsecurity.com/legal.html.*

Contents

1. Welcome to SignalBoard

Intent. *Set expectations in one minute. What SignalBoard is, who it is for, what it will and will not do.*

What SignalBoard is

SignalBoard is an executive bridge platform. It reads your Microsoft 365 environment over Microsoft Graph and renders an executive-friendly scorecard that translates technical security configuration into business language. It runs in your browser; nothing is installed.

Who SignalBoard is for

- CEOs, CFOs, owners, and board members who need a meaningful read of security posture without becoming security experts.
- IT and MSP teams who want a consistent, repeatable executive readout per quarter.
- Insurance brokers and underwriters who want a clean snapshot to support a renewal conversation.

What SignalBoard does *not* do

- It does **not** modify any Microsoft 365 settings, policies, or configuration. Read-only.
- It does **not** automatically remediate findings. Remediation is your IT team or MSP's call.
- It does **not** access email contents, SharePoint files, OneDrive contents, Teams messages, passwords, or financial records.
- It does **not** transfer scan data to any generative AI provider.
- It does **not** guarantee insurability, premium reductions, or regulatory compliance — it is decision-support.

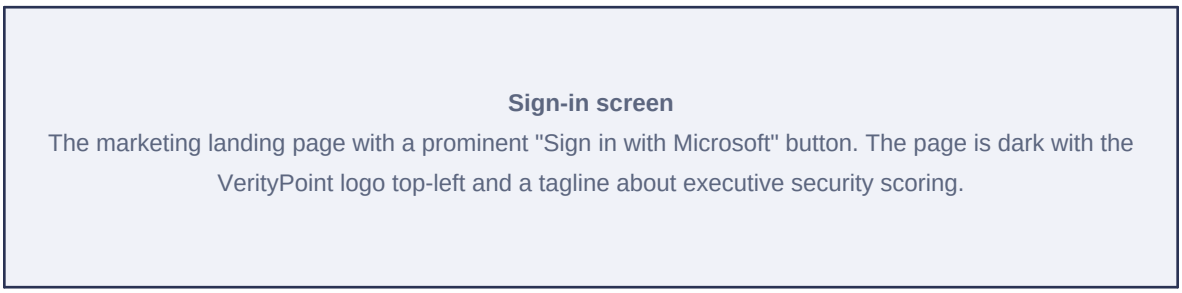
Heads-up. SignalBoard is read-only. You can scan as often as you like and nothing about your Microsoft 365 environment changes as a result of the scan.

2. Signing in for the first time

Intent. *Get a brand-new user into the dashboard. The first sign-in has one extra step (Microsoft consent) that future sign-ins skip.*

Step-by-step

1. In your browser, go to https://signalboard.veritypointsecurity.com.
2. Click **Sign in with Microsoft**. A Microsoft 365 sign-in window opens.
3. Sign in with your Microsoft 365 account. Use an account that has the Microsoft Graph permissions needed (typically a Global Administrator on the first run, so the read-only scopes can be consented).
4. Approve the read-only Graph permissions on the consent screen. This appears once per tenant; subsequent users in the same tenant skip it.
5. You land on the dashboard. If a prior scan exists in your tenant's cloud storage, it auto-loads. If this is your first time, you'll see an empty halo with an **Initiate Scan** button in the center.



What happens after sign-in

- SignalBoard verifies your tenant's license against the backend.
- The dashboard tries to auto-load your most-recent saved scan from cloud audit storage. If a scan is found, you land on the populated dashboard. If not, you see an empty halo.
- A status line under the halo confirms what happened (for example: *"Loaded last saved scan (Jun 4, 2026, 1:57 PM)"*).

If you see "Tenant not licensed." Email hello@veritypointsecurity.com to start the subscription process. Until the license is active you can sign in but cannot scan.

3. The dashboard at a glance

Intent. *Orient the user to the main screen so the halo and surrounding controls make sense.*

Anatomy of the home screen

- **Top-left:** VerityPoint brand logo, **Audit Upload** button (for legacy JSON imports), **Audit Save** button (after a scan completes).
- **Top-right:** the three-bar hamburger menu (About, Privacy & Legal, Personalization, Manage cloud storage, User Manual, Sign out).
- **Center:** the halo. Inside the halo is your **Microsoft Secure Score** reading. Eight satellites orbit the halo, one per security domain.
- **Above the halo:** a view-toggle bar with three views — **Technology Telemetry** (the halo), **Scorecard** (bar chart per domain), and **Organizational Posture** (the business view with action cards).
- **Below the halo:** the action row — Insurance Readiness, Print PDF, Save Deck, Trend.

Empty halo + action row

Dashboard immediately after sign-in, before a scan has run. Center: large circular halo with a button reading "Initiate Scan" in the middle. Eight grey-stroked dots arranged at 45° around the halo. View toggle (Technology Telemetry / Scorecard / Organizational Posture) sits above the halo. Action buttons sit below.

The eight domains

Every scan grades eight domains. Each satellite represents one. Click a satellite to see the underlying findings.

Executive label	Technical name	What it measures
Cyber Maturity	Microsoft Secure Score	Microsoft's composite of recommended baseline actions.
Device Trust	Devices & Intune	Intune-managed devices, compliance, encryption.
Workforce Protection	Defender / Endpoint	EDR coverage, real-time protection, tamper protection.
Executive Access	Privileged Accounts	Global Admin count, PIM use, role assignments.
Identity Security	Identity Hygiene	Active users, stale accounts, guests, MFA enrollment.

Sign-in Trust	Conditional Access & MFA	CA policy enforcement + MFA coverage.
Communications Risk	Email Security	SPF, DKIM, DMARC domain authentication.
Identity Modernization	Hybrid Identity Posture	On-premises sync, federation, device authority.

4. Running a scan

Intent. *Walk through the one-button scan and what to expect during the ~30-second run.*

How to start

1. On the dashboard, click **Initiate Scan** in the center of the halo.
2. The button is replaced by a status line that narrates each domain as it loads (*"Reading Microsoft Secure Score…", "Reading Conditional Access policies…"*, etc.).
3. The eight satellites illuminate one at a time as their data arrives. Tier colors (green / amber / red) appear immediately.
4. When the scan completes, the dashboard switches to the **Organizational Posture** view and shows the executive summary. Total time: roughly 30 seconds.

Scan in progress

The halo with several satellites lit up (some green, some amber, some still dim/grey). A status line in the halo center reads something like "Reading Conditional Access policies…". The narrative paces about 1.5 seconds per domain.

When to scan

- **Each quarter** at minimum. The trend lines need successive runs to be meaningful.
- **After a material change** — a new device rollout, a Conditional Access policy change, an admin role reorganization, or a Microsoft 365 license upgrade.
- **Before an insurance renewal** so the snapshot in your application is current.

What's being read

SignalBoard uses your delegated Microsoft 365 sign-in to read configuration data through Microsoft Graph. Read-only scopes only. The list of permissions appears on the first-time consent screen and is documented in About > Scope.

Demo mode. If a yellow banner reads "DEMO MODE — License check bypassed for review walkthrough," you are signed in as a demonstration account. Scans, saves, and reports all work, but the banner reminds reviewers the license gate has been intentionally relaxed.

5. Reading the scorecard

Intent. *Translate the scorecard into something an executive can speak to without context.*

Switching views

- **Technology Telemetry** — the halo. Best for "show me everything at once."
- **Scorecard** — a clean bar chart of all eight domains. Best for "where am I weakest?"
- **Organizational Posture** — the business view. Best for "what should leadership pay attention to?" (default after a scan completes)

Scorecard view

Horizontal bar chart with one row per domain. Each bar is colored by tier (green / amber / red). Numerical score 0–100 shown at the right edge of each bar. Title above reads "Overall posture — X/100 (Grade)". The view toggle is highlighted on "Scorecard".

What the colors mean

Tier	Range	Read
Green	85–100	Strong. Well-aligned with Microsoft baselines.
Amber	65–84	Moderate. Improvement opportunities present.
Red	0–64	Needs work. Material gaps in core controls.

The trend pill

On the upper-right of the Organizational Posture banner you'll see a small pill comparing this scan with your historical baseline:

- → **Unchanged** — score moved by zero points.
- → **Stable +/-N pts** — moved a few points but still within band.
- ↑ **Improving +N pts since [date]** — meaningful upward move.
- ↓ **Declining –N pts since [date]** — meaningful downward move.

Trend data comes from your Cloud audit storage (see Section 11). Deleting saved scans reduces the comparison set on the next load.

6. Organizational Posture — the business view

> ***Intent.*** *The view a CEO or board member opens with. Anchored by a plain-language banner and three concrete recommendations.*

Banner and recommendations

The Business Exposure / Operational Confidence banner across the top translates the score into a sentence: "*Operational Confidence: Moderate. Identity governance and access controls are the highest-leverage areas to harden next.*"

To the right of the banner is the **Top Recommendations** panel — three cards from the Insurance Readiness library, prioritized as Gaps first, then Unknowns, then Partials. Each card has the control name, status pill, one-line detail, and the framework tag (CIS / NIST / HIPAA). Clicking a card opens the full Insurance Readiness page.

Organizational Posture

Two-column layout. Left: a colored banner with the title "Business Exposure Level: Elevated" (or similar) and a paragraph below explaining the read. An "Ask Claude / Copilot / ChatGPT" pill sits at the bottom of the banner. Right: three stacked recommendation cards with red/amber left borders. Below: an 8-card grid of domains with a circular "Next Steps" button in the center.

The 8-card grid

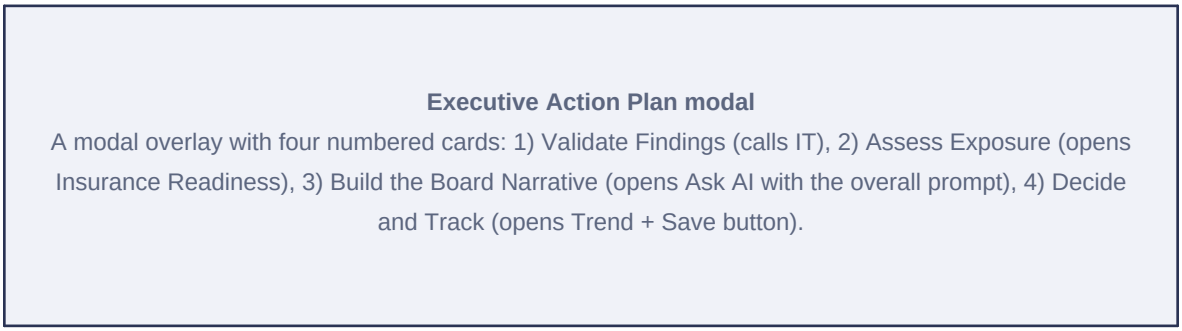
Below the banner row is a 4×2 grid of executive-labeled domain cards. Each card shows tier color, plain-language title (e.g. "Workforce Protection" instead of "Defender / Endpoint"), a one-line read, and a per-card "Ask AI about this" link. In the center of the grid is the **Next Steps** circular button — see Section 7.

7. Next Steps — Executive Action Plan

Intent. *Give leadership four concrete moves they can take this quarter, in order, without becoming security experts.*

Opening the plan

Click the circular **Next Steps** button in the center of the 8-card grid. A modal opens with four numbered steps and one primary action button per step.



The four steps

Step	What it does
1. Validate Findings	Opens an email composer pre-addressed to your IT team or MSP. The body summarizes the s
2. Assess Exposure	Opens the Insurance Readiness Analysis (Section 8).
3. Build the Board Narrative	Opens Ask AI with a vendor-neutral prompt that produces a board paragraph (Section 10).
4. Decide and Track	Opens the Trend page and offers a Save button so the current scan goes into the historical bas

Step 4 Save — cloud or local

The Step 4 Save button asks where to save: **OK = cloud (recommended)** joins the trend lines automatically and auto-loads next sign-in. **Cancel = download a local JSON copy** lets you keep a record outside the platform.

8. Insurance Readiness Analysis

Intent. *A 17-control checklist mapped to CIS, NIST, and HIPAA frameworks. Combines auto-assessed findings with executive attestations.*

Opening the page

- From the Organizational Posture view, click the **Insurance Readiness Analysis** button in the action row below the halo.
- Or click any Top Recommendation card to land scrolled into the relevant section.

Insurance Readiness page

A long page with a score panel at the top (large percentage and rating: Strong / Moderate / Needs work). Below: two tables — auto-assessed controls (Met / Partial / Gap) and evidence-attested controls (Full / Partial / Gap dropdown per row). Each row has a framework tag. A "Save Insurance information" button sits in the top-right of the page header.

Two kinds of controls

- **Auto-assessed.** Read directly from your scan data. SignalBoard sets these — you cannot override them here, only fix the underlying issue in Microsoft 365 and re-scan.
- **Evidence-attested.** Things SignalBoard cannot detect (immutable backups, MDR contracts, employee training cadence). You pick **Full**, **Partial**, or **Gap** from a dropdown per row and optionally add notes.

Saving your attestations

Click **Save Insurance information** at the top of the page when done. The attestations and notes get baked into the audit bundle and pushed to your tenant's encrypted Cloud audit storage. They will then appear automatically on any future trip you take to this page, on any device. The save also feeds the trend lines.

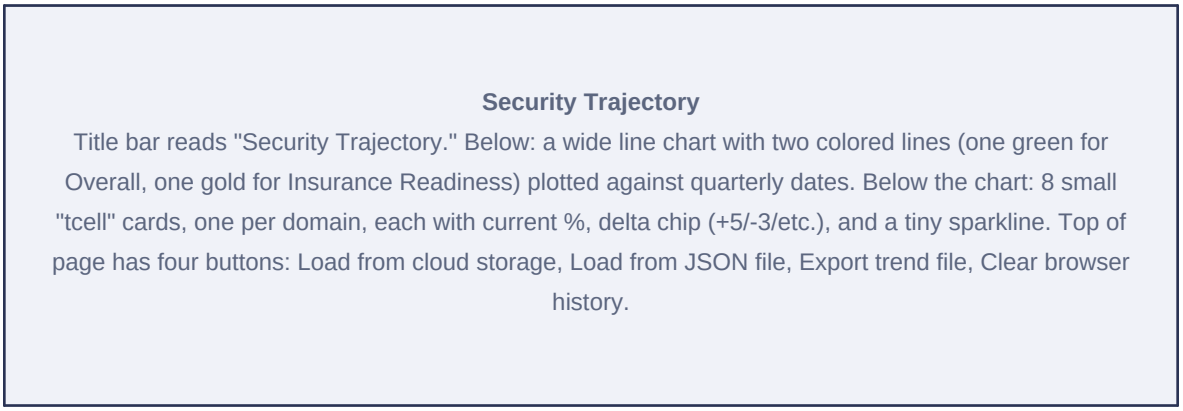
If nothing has changed. SignalBoard checks the saved payload against your last save. If nothing has changed, no new history blob is written and you'll see "No changes since the last save." This keeps storage tidy.

9. Security Trajectory (trend over time)

Intent. *See whether posture is improving or slipping across quarters. Sourced from Cloud audit storage.*

What you see

A multi-line chart with two series: Overall Grade and Insurance Readiness. Below the chart, a grid of per-domain mini-trends shows current value, delta since first scan, and a small spark line. Delta chips on each card make it easy to spot the biggest movers.



Where the data comes from

The trend is built from your **Cloud audit storage** blobs. Every time you save a scan, a small numbers-only snapshot is stamped on the blob as metadata. The trend page reads those snapshots without decrypting any blob.

Deleting a saved scan from Cloud audit storage reduces your trend. The trend is now a direct reflection of what's in cloud storage — there is no separate browser-local history to drift out of sync.

Loading older runs

- **Load from cloud storage** — opens the Cloud audit storage page where you can multi-select historical scans and pull them into the trend.
- **Load from JSON file** — for older scans saved to disk before Cloud audit storage existed. Accepts multiple files at once; files that don't match the SignalBoard naming convention are ignored.

10. Ask AI — vendor-neutral prompts

Intent. *Let leadership get an AI-generated board paragraph or per-domain summary, without sending data to a third-party AI through SignalBoard.*

How it works

Every "Ask Claude / Copilot / ChatGPT" button assembles a structured prompt that includes a redacted snapshot of your scan and a question (overall board paragraph, or per-domain explanation). The prompt opens in a modal where you can review it, copy it to your clipboard, and then paste it into your AI assistant of choice.

Ask AI modal

A modal with a large text area showing the assembled prompt (structured JSON snapshot + question). Three vendor buttons sit at the top: Claude, Copilot, ChatGPT. A "Copy prompt" button and a "Don't show again" toggle sit at the bottom. The data shown is name-redacted; tenant identity is masked.

Important. SignalBoard does **not** send your data to any AI vendor on your behalf. *You* open the prompt, copy it, and paste it into your own AI tool. We never transit your scan to OpenAI, Anthropic, Google, or Microsoft AI. This is documented in Privacy & Legal.

11. Cloud audit storage

Intent. *Manage every saved scan — load, delete, see who saved it, see which scans contain insurance attestations.*

Opening the page

Click the hamburger menu (three bars, top-right) and choose **Manage cloud storage**.

Cloud audit storage page

Page title: "Cloud audit storage — Select the periods you want to trend or delete." Bulk-action row with Select all checkbox, "Load N selected" button, "Delete N selected" button, and a legend (Gold highlight = contains insurance attestations). Below: a table with columns Saved / Saved by / Insurance / Size. Rows with insurance data have a gold left border and an "X/17 attested" badge.

What you can do

- **Select all** — header checkbox toggles every row.
- **Load N selected** — fetches each chosen scan, captures snapshots into the trend, and renders the most-recent as the active dashboard view.
- **Delete N selected** — permanently removes the selected blobs from your tenant's storage. No recovery.

The gold highlight

Rows with a **gold left border** and an attested badge contain Insurance Readiness attestations. Useful when you want to find the quarter where you last completed an insurance questionnaire and pull that one for reference.

12. Reports and exports (PDF, PowerPoint, redacted JSON)

Intent. *Three formats for three audiences: PDF for the board, PowerPoint for the deck, redacted JSON for outside sharing.*

PDF report

- From the action row below the halo, click **Print PDF**.
- The browser's print dialog opens. Choose **Save as PDF** as the printer to write a file.
- The report includes a cover, methodology, all eight domains, insurance readiness, evidence, and the data privacy summary.

PowerPoint deck

- From the action row, click **Save Deck**.
- A .pptx file downloads (or saves to the folder you chose in Personalization — see Section 16).
- The deck has executive summary, current posture, eight-domain analysis, and "where we go from here."

Redacted JSON

- From About > Data Privacy section, click **Download redacted JSON**.
- Counts and percentages are preserved; names and UPNs are removed.
- Best for sharing with an insurance broker, board member, or auditor who needs the numbers without the personal data.

13. Data management

Intent. *The complete picture of what SignalBoard does with your data — where it lives, how long it stays, what triggers deletion, and how to export before lapse.*

Where your data lives

Saved scans are stored as **encrypted blobs in Microsoft Azure**, scoped to your Microsoft 365 tenant. Saved scans are logically isolated by tenant and access-controlled through Microsoft Entra ID — customer users may only access data associated with their own tenant.

By default the storage account is in **East US**. EU customers can request EU-region deployment (typically West Europe or North Europe) at contract execution. Multi-region routing is wired into the backend; provisioning a regional account and flipping your storageRegion flag moves your future scans to that region.

What is and isn't in a saved scan

Is in the bundle	Is NOT in the bundle
Tenant name and ID	Passwords, tokens, API keys
Verified domains	OneDrive / SharePoint contents
Named admin and unprotected users	Teams messages, calls, recordings
Aggregate user / device counts	Email contents
Policy names and assignments	PHI (protected health information)
MFA enrollment, Secure Score	Customer financial records
Insurance attestations and notes	Per-user sign-in history
Schema version, scan timestamp	—

How long it is retained

Default: 24 months of rolling history while your subscription is active. Customer-configurable from 30 days to "until deleted by the customer" via in-app Cloud audit storage controls.

Subscription lapse = permanent deletion. Saved scans live only while your subscription is active. On lapse you get a **30-day grace window** to export. After that window, every encrypted blob for your tenant is permanently and irreversibly removed from Azure storage. **There is no recovery process** — we don't keep off-cluster backups. Export before lapsing.

Trend continuity

The Security Trajectory page reads its history directly from your cloud-stored scans. **Deleting a scan from Cloud audit storage immediately reduces your trend.** If you want to keep a historical quarter on the trend, don't delete its blob.

Local copies

You can always download a copy of any scan to your laptop as JSON. From Cloud audit storage, select a scan and use your browser's Save Page As. From the Next Steps Step 4 button, choose Cancel when prompted to download instead of saving to cloud. Store local copies in your own Microsoft 365 (OneDrive / SharePoint with restricted access) or on an encrypted disk.

Encryption and access

- **Encryption in transit:** TLS 1.2 minimum on every endpoint.
- **Encryption at rest:** Azure Storage Service Encryption (AES-256, Microsoft-managed keys).
- **Authentication:** Microsoft Entra ID delegated permissions only. We do not hold application secrets that could read your tenant in the background.
- **Tenant isolation:** every blob is namespaced by tenant ID; access is gated by Entra ID and enforced on every read, list, and delete operation.
- **No long-term token storage:** the dashboard's session token cache is cleared on tab close.

Schema versioning

Every saved bundle carries a **schemaVersion** field. As SignalBoard evolves, this lets the dashboard read older bundles without breaking. Loading a bundle from a newer build than your dashboard knows about prints a warning and renders what it recognizes; loading an older bundle prints a note and renders with defaults for missing fields.

14. The 5-user-per-tenant access policy

Intent. *Important: SignalBoard limits the number of distinct users who can save scans inside a single tenant. Understand the rule, the rationale, and the cleanup path.*

The rule. Within a single Microsoft 365 tenant, SignalBoard allows a maximum of **five distinct users** to save scans into Cloud audit storage. A "user" is identified by Microsoft Entra ID object ID — the unique, immutable identifier Microsoft assigns to every account. Renaming an account does not create a new seat; using a brand-new account does.

How seats are counted

- Every saved blob is tagged with the object ID of the user who saved it.
- A "seat" is occupied as soon as a user saves their first scan.
- If five distinct users have saved scans, the tenant is at capacity.
- A sixth user can sign in and run scans, but their **first save attempt fails** with a clear message naming the current seated users.

How to free a seat

1. Any signed-in user can open **Manage cloud storage** from the hamburger menu.
2. Find scans saved by the user whose seat you want to free (the **Saved by** column shows the UPN of the creator).
3. Select all of that user's scans (use the Select-all checkbox plus filter).
4. Click **Delete N selected** and confirm.
5. Once a user has zero scans remaining in the tenant's storage, their seat is released. The next new user's save will succeed.

Why this limit exists

SignalBoard's subscription tier provisions for a small, focused executive readership — not a broad enterprise rollout. Five seats fit a typical engagement: one or two executives, an IT lead, the MSP's primary contact, and one extra for cross-coverage. Customers needing more should contact hello@veritypointsecurity.com for an enterprise tier.

Important. Deleting another user's data is permanent. There is no recovery. Make sure you have the consent or authority to remove someone else's saved scans before you do so. Consider exporting the user's scans first if their work needs to be preserved for the record.

15. Hamburger menu reference

Intent. *One-line description of every item in the three-bar menu at the top-right of the dashboard.*

Item	What it does
About	Opens the About modal at the Scope tab. Tab strip: Scope, Best Practice, Scoring, How to F
Privacy & Legal	Opens About > Privacy & Legal. Contains at-a-glance summary plus a link to the full standa
Personalization	Opens About > Personalization. Logo upload and PowerPoint save folder.
Manage cloud storage	Opens the Cloud audit storage page (Section 11).
User Manual	Opens this PDF in a new browser tab. Hosted as a separate file so updates do not require r
Sign out	Signs you out of Microsoft 365 in the SignalBoard tab.

16. Personalization (logo, save folder)

Intent. *For MSPs and consultants scanning multiple clients. Set a client logo per browser, and choose a default PowerPoint save folder.*

Client logo

- Upload a PNG or SVG. Embedded in your browser only; not stored on a server.
- Applied to the PDF report cover and the PowerPoint title slide.
- When Demo mode is on, the default logo is shown instead — useful for prospect walkthroughs.

PowerPoint save location

- Default: browser Downloads folder.
- Pick a folder once and every deck goes there. Requires Chrome or Edge (uses the File System Access API).
- Toggle **Always ask** if you prefer the system save dialog each time.

17. Privacy & Legal — quick reference

Intent. *A one-page executive summary. The full document is at /legal.html.*

- **Who we are.** JJS Partners, LLC, d/b/a VerityPoint Security. SignalBoard is the product.
- **What we collect.** Microsoft 365 configuration data via Microsoft Graph read-only delegated scopes. Never passwords, tokens, document contents, or PHI.
- **Where it lives.** Encrypted at rest in Azure Blob Storage, scoped to your tenant. You delete from the in-app Cloud audit storage page.
- **How long.** Active subscription only. **On lapse: 30-day export grace, then permanent deletion. No recovery.**
- **Sub-processors.** Microsoft Corporation (Azure / Entra / Graph), Stripe Inc. (payments), Cloudflare Inc. (DNS / edge for marketing site).
- **Your rights.** Access, rectification, erasure, restriction, portability, objection. Email privacy@veritypointsecurity.com.
- **Breach notification.** 72 hours from confirmation, per GDPR Article 33.
- **Sample DPA.** Section 13 of the legal page is the exact contract text we will sign. Counter-signed within 5 business days of request.

18. Troubleshooting

> ***Intent.*** *The most common issues, in plain language. If none of these match, email security@veritypointsecurity.com.*

"Tenant not licensed."

Your Microsoft 365 tenant ID is not in our subscription registry. Email hello@veritypointsecurity.com to start the subscription process.

"Tenant at 5/5 users."

See Section 14. A signed-in user needs to delete some saved scans from another seat to free capacity, or you need to talk to us about an enterprise tier.

"Failed to fetch."

A network error reaching the SignalBoard API. Try refreshing. If the error persists, check your VPN or firewall — outbound HTTPS to signalboard-api.azurewebsites.net must be allowed. Email security@veritypointsecurity.com if it still won't connect.

Cloud audit storage shows zero saved scans.

You may be signed in as a different tenant than the one whose scans you remember. Each tenant has its own private storage. Check the username in the status line.

Sign-in works but the halo stays empty.

You are signed in but no prior scan exists in your tenant's cloud storage. Click Initiate Scan to run your first one. This is the normal first-time state.

PDF report is missing the trend page.

The trend page is only rendered when you have at least two saved scans. Save a second scan, then re-print.

Browser blocked the Microsoft sign-in popup.

Allow popups for signalboard.veritypointsecurity.com and retry.

"Cannot connect to /api/audit/list."

Your subscription may have lapsed. Check your billing portal. If the subscription is active and the error persists, email security@veritypointsecurity.com.

19. Support and contact

Intent. *The right address for each kind of question.*

Topic	Email
General questions	hello@veritypointsecurity.com
Privacy / data protection / GDPR	privacy@veritypointsecurity.com
Security / vendor risk / vulnerability reports	security@veritypointsecurity.com
Abuse	abuse@veritypointsecurity.com
Signed DPA request	hello@veritypointsecurity.com (subject: "DPA request")
BAA / HIPAA	hello@veritypointsecurity.com (subject: "BAA request")

Response time

- 5 business days for acknowledgment.
- 30 days for substantive response.
- Security and breach inquiries triaged within 1 business day.

20. Glossary

Intent. *Plain definitions for terms that appear throughout the platform and this manual.*

Audit bundle

The JSON document SignalBoard produces from a scan. Contains meta, sections, optional insurance attestations, and a schemaVersion.

CIS

Center for Internet Security. Source of one of the control frameworks used in Insurance Readiness.

Conditional Access

Microsoft Entra ID policy framework. Defines when MFA, device compliance, or location must be required.

Delegated permissions

Microsoft Graph permission model where the app acts on the signed-in user's behalf with the user's scope.

Halo

The circular visualization at the center of the dashboard. Houses Microsoft Secure Score and eight orbiting domain satellites.

HIPAA

Health Insurance Portability and Accountability Act. US healthcare data privacy regime. SignalBoard requires a BAA before processing PHI.

Insurance Readiness

A 17-control checklist mapped to CIS / NIST / HIPAA. Drives a percentage score used in insurance renewal conversations.

NIST

National Institute of Standards and Technology. Source of one of the control frameworks used in Insurance Readiness.

Object ID

The unique, immutable identifier Microsoft Entra ID assigns to every account. SignalBoard uses this to track seats.

Operational Confidence

SignalBoard's plain-language read of overall posture: Strong, Moderate, or Elevated business exposure.

Posture

The state of your security configuration relative to Microsoft baselines. Expressed as a 0–100 score per domain plus an overall.

Schema version

A number stamped on every saved bundle. Lets the dashboard read older bundles without breaking when fields change.

Seat

A licensed access slot. Five per tenant. Occupied when a user saves their first scan.

Tenant

Your Microsoft 365 organization. Identified by a UUID. Every saved scan is scoped to a single tenant.

UPN

User Principal Name. The email-format identifier for a Microsoft 365 user (e.g. alice@contoso.com).

End of manual

Email hello@veritypointsecurity.com with questions or corrections.
For the full Privacy Policy and Data Processing Addendum, see
https://signalboard.veritypointsecurity.com/legal.html.