A FREE GUIDE FROM VERI-TECH, INC.

Veri-Tech, OpenIntuneBaseline, and *CIS Microsoft 365.*

A compatibility statement for Intune admins who already use OIB and want to know how Veri-Tune fits alongside it.

Engineers shouldn't also be the audit team.

Executive summary

If you manage a Microsoft 365 tenant, you have probably already taken two of the three steps that matter. You have deployed the OpenIntuneBaseline as your starting Windows device baseline, and you have read the CIS Microsoft 365 Foundations Benchmark to understand the tenant-side controls that OIB does not address. The third step, the one almost nobody automates, is keeping all of that posture from drifting back over time.

Veri-Tune is a continuous posture engine for Microsoft Intune. It scans your Intune tenant against more than 350 device-management controls, scores configuration drift, and produces remediation guidance. It does not ship a starter baseline. OIB does that, and does it well. Veri-Tune sits on top of whatever Intune baseline you have deployed, including OIB, including Microsoft Security Baselines, including in-house variants, and tells you when something has changed, drifted, or fallen out of policy.

Veri-Guard, our companion product, scans the M365 tenant configuration that lives outside Intune entirely: Conditional Access, Defender for Office, DLP, SharePoint, Teams, Exchange Online. That is where the CIS Microsoft 365 Foundations Benchmark lives. Together, Veri-Tune and Veri-Guard cover the surface that OIB plus the Foundations Benchmark are designed to cover, with the same posture-management discipline applied to both.

This document is the proof. It maps OIB profile families to Veri-Tune control categories, names the gaps in both directions, places the CIS Microsoft 365 Foundations Benchmark in its correct scope, and acknowledges the 14 Foundations Benchmark controls that Veri-Tech does not yet automate.

What "compatible" means here

We use compatible deliberately. Three claims, each narrow:

1. **Veri-Tune does not break OIB.** Veri-Tune is a read-only scanner by default. It connects to Microsoft Graph using a scoped read-only application identity, enumerates your existing Intune policies, and compares the deployed configuration to its own baseline. It does not rewrite, replace, or unassign OIB profiles. If you choose to use Veri-Tune's auto-remediation path, you grant a separate write-scoped consent and you opt in per control. Nothing happens silently.
2. **Veri-Tune respects OIB's intent.** OIB makes deliberate choices to skip certain CIS Intune Benchmark settings on user-experience or relevance grounds. Veri-Tune does not flag those skipped controls as failures simply because OIB does not ship them. Where OIB has a published rationale (the OIBvsCIS-Rationale CSV in the OIB Windows folder), we treat the OIB position as a defensible policy decision and surface it as a configuration choice, not a gap.
3. **Veri-Tune extends OIB's scope.** OIB v3.7 is a Windows-first baseline. Veri-Tune covers Windows, plus iOS, Android, and macOS through Compliance Policies and App Protection Policies. It also extends into tenant-

side Intune configuration that OIB does not currently address: enrollment restrictions, Autopilot deployment profiles, app deployment posture, and platform-enrollment hygiene.

What we do not claim:

- We do not claim OpenIntuneBaseline endorses, certifies, or partners with Veri-Tech. OIB is a community project maintained by James (SkipToTheEndpoint) and contributors, licensed for community use. Veri-Tech has no formal relationship with OIB or its maintainer.
- We do not claim CIS endorses, certifies, or partners with Veri-Tech. Veri-Tech surfaces CIS frameworks on a nominative basis, with paraphrased control summaries and no verbatim Benchmark prose. See the disclaimer at the end of this document.

OpenIntuneBaseline at a glance

What it is. A starter Intune configuration baseline maintained as an open community project. The Windows variant is the most mature and the one this document focuses on.

Current Windows release. v3.7, published 2025-10-15, aligned with Windows 11 25H2.

What it ships. Roughly 58 Settings Catalog profiles, 14 Endpoint Security profiles, 4 Compliance Policies, plus delivery-optimisation and update-ring policies. Categories include Defender Antivirus, Attack Surface Reduction, BitLocker, Windows Firewall, Windows LAPS, Windows Hello for Business, Edge security, Office security, OneDrive client configuration, Local Security Policies, User Rights, and the Windows Update for Business rings.

Frameworks consulted during construction. NCSC Device Security Guidance, CIS Windows Benchmarks, ACSC Essential Eight, Microsoft Intune Security Baselines for Windows, Edge, and Defender for Endpoint, and Microsoft Best Practice. The OIB author publishes an OIBvsCIS-Rationale.csv documenting which CIS Intune Benchmark settings OIB deliberately skips, and why.

What OIB explicitly does not do. OIB is a starting point and a reference implementation. It does not run drift detection. It does not score your live tenant. It does not produce per-control remediation guidance against your existing assignments. It does not cover the tenant-config surface that the CIS Microsoft 365 Foundations Benchmark targets (Conditional Access, Defender for Office, SharePoint, Teams, Exchange).

Veri-Tune at a glance

What it is. The Intune posture-management product in the Veri-Tech suite. Scans, scores, and remediates Microsoft Intune configurations across Windows, iOS, Android, and macOS.

Control coverage. 379 controls in our published Intune baseline registry, broken down approximately as:

Detection method	Count	What it covers
Settings Catalog	257	Windows OS hardening, Defender, BitLocker, Edge, Office, LAPS
Compliance Policy	48	Cross-platform device compliance gates
App Protection Policy	49	iOS and Android MAM controls
Device Configuration	16	Legacy template profiles still in active use
Other	9	Conflict detection, CA-compliance gates, enrollment hygiene

Frameworks mapped. NIST SP 800-53 Rev 5, CIS Microsoft Intune for Windows Benchmark, CIS Microsoft 365 Foundations Benchmark, HIPAA Security Rule, ISO 27001:2022, SOC 2 Trust Services Criteria, CISA SCuBA. Each Veri-Tune control carries one or more framework citations so that fixing it moves multiple framework rows at once.

What Veri-Tune does that OIB does not.

- Continuous drift detection against whatever baseline you have deployed.
- Per-control gap reports with remediation guidance, runbooks, and (with separate consent) one-click auto-remediation.
- Cross-platform scope: iOS and Android App Protection, macOS configuration, Windows 365 Cloud PC.
- Framework cross-walking: one finding maps to multiple framework rows in the same report.
- Configuration export and audit-ready evidence in PDF and JSON.

The CIS Microsoft 365 Foundations Benchmark at a glance

What it is. A tenant-configuration benchmark for Microsoft 365 published by the Center for Internet Security. The current Foundations Benchmark covers nine sections of tenant-level configuration. None of these sections are device-baseline controls. None of them are addressed by OpenIntuneBaseline.

Sections we cover.

Section	Topic	Veri-Tech product
1	Account and Authentication, admin role hygiene	Veri-Guard
2	Defender for Office anti-phishing, anti-spam, anti-malware policies	Veri-Guard
3	Data Loss Prevention	Veri-Guard
4	(reserved)	n/a
5	Identity and Access Management, Conditional Access, MFA	Veri-Guard
6	Sensitivity labels and information protection	Veri-Guard
7	SharePoint Online and OneDrive	Veri-Guard
8	Microsoft Teams	Veri-Guard
9	Power BI and Microsoft Fabric	Veri-Guard (partially, see honest-gaps section)

Side-by-side coverage table

This is the canonical mapping. Read it as: "if you have deployed this OIB profile family, here is the CIS Microsoft 365 section it relates to (where any relation exists), and here is the Veri-Tune control category that scans the same surface."

OIB Windows profile family	CIS Microsoft 365 section	Veri-Tune category (control count)
ES, Encryption (BitLocker OS Disk, Personal Data Encryption)	n/a, device scope only	encryption (22)
ES, Defender Antivirus + Defender Update Rings	Section 2 (cloud-side Defender for Office, complementary)	antivirus (14)
ES, Attack Surface Reduction (ASR Rules)	n/a, device scope only	applicationControl (23) + attackSurfaceReduction (1)
ES, Windows Firewall	n/a, device scope only	firewall (30)
ES, Windows LAPS	n/a, device scope only	localSecurity (26)
ES, Windows Hello for Business	Section 5 (passwordless and MFA, cloud-side)	authentication (18)
ES, Local Group Membership	n/a, device scope only	accountManagement (6)
SC, Device Security (multiple profiles)	n/a, device scope only	deviceSecurity (76)
SC, Microsoft Edge (Security, Updates, Extensions, Profiles)	n/a, device scope only	browserSecurity (33)
SC, Microsoft Office (Security, Updates, User Experience)	n/a, device scope only	officeSecurity (23)
SC, Microsoft OneDrive (client config)	Section 7 (server-side OneDrive, complementary)	dataProtection (21)
SC, Windows Update for Business + Delivery Optimisation	n/a, device scope only	updateManagement (10) + deliveryOptimization (7)
SC, Credential Management, Microsoft Accounts	Section 1 (Account and Authentication, cloud-side)	accountProtection (4)
Compliance Policies (Defender for Endpoint, Device Health, Device Security, Password)	Section 5 (compliance gates feeding CA)	compliance (43)
(no OIB equivalent, OIB is Windows-only)	n/a	App Protection Policy (49 controls, iOS + Android)
(no OIB equivalent)	Sections 1 through 9 (all tenant-config)	(covered by Veri-Guard, not Veri-Tune)

Two things to read carefully:

1. **Most OIB profiles have no CIS Microsoft 365 section equivalent.** That is correct. OIB is a Windows endpoint baseline. CIS Microsoft 365 is a tenant-config benchmark. The two address different layers of the same Microsoft 365 estate. Veri-Tune covers the OIB layer. Veri-Guard covers the CIS Microsoft 365 layer.
2. **Where a relation exists, it is "complementary," not "equivalent."** OIB's Defender Antivirus profile hardens the local agent. CIS Microsoft 365 Section 2 hardens cloud-side Defender for Office. You need

both. OIB ships the device half. Veri-Guard scans the cloud half.

What OIB covers that Veri-Tune does not

We are honest about the directions where OIB still does something Veri-Tune does not.

- **Pre-built, deployable JSON profiles.** OIB ships ready-to-import IntuneManagement JSON. Veri-Tune is a scanner, not a baseline distributor. If you do not already have a baseline deployed, OIB is the fastest way to get one. Run OIB first, then turn Veri-Tune on against the resulting tenant.
- **Detailed per-setting CIS Intune Benchmark rationale.** OIB's OIBvsCIS-Rationale.csv is a public artifact that explains why specific CIS Intune Benchmark controls are not implemented in OIB (user experience, relevance to Entra-joined estates, default behaviour already in place, alternative mitigation already in place). Veri-Tune carries control-level rationale in its registry but does not republish OIB's published rationale verbatim.
- **Windows 365 Cloud PC and macOS starter baselines as separate, named bundles.** OIB ships discrete Windows 365 v1.0 and macOS v1.0 baselines. Veri-Tune covers macOS and Windows 365 within its broader Intune scope but does not partition them as named "starter baselines."
- **Community review, public PRs, and a documented changelog.** OIB is open and you can audit every change in the public repo. Veri-Tune's registry is closed source, with framework citations published in customer reports.

If your goal is "stand up a known-good Windows baseline and deploy it tomorrow," OIB is the right answer. Use it. Then use Veri-Tune to keep it from drifting.

What Veri-Tune covers that OIB does not

The other direction.

- **Drift detection over time.** OIB ships you a starting point. It does not tell you when an admin has unassigned a profile, when Microsoft has changed a default underneath you, or when a new policy has been created that conflicts with an existing one. Veri-Tune does all three, on a schedule you set.
- **Cross-platform App Protection Policies.** OIB does not currently ship iOS or Android MAM profiles. Veri-Tune scans 49 App Protection controls covering data transfer, encryption, PIN policy, jailbreak detection, and selective wipe across iOS and Android.
- **Compliance Policy depth across platforms.** OIB ships 4 Windows Compliance Policies. Veri-Tune scans 43 compliance controls across Windows, iOS, Android, and macOS, with explicit checks for compliance-gate-to-Conditional-Access linkage.
- **Conflict detection.** When two Settings Catalog profiles target the same setting with different values, OIB has no way to flag it (OIB is a static baseline). Veri-Tune surfaces every conflict as a finding with the conflicting profile names and the contested setting value.

- **Framework cross-walking.** A single Veri-Tune finding maps to multiple framework rows (CIS, NIST, HIPAA, SOC 2, ISO 27001, CISA SCuBA). One fix, multiple audit checkboxes.
- **Auto-remediation with explicit consent.** With a separate write-scoped consent grant, Veri-Tune can apply remediations one-click. Every change is logged, attributable, and reversible. Auto-remediate is opt-in per control, not blanket.
- **Tenant-config coverage through Veri-Guard.** OIB does not address Conditional Access, Defender for Office presets, DLP, Exchange Online mail flow, SharePoint sharing settings, or Teams federation. Those live in Veri-Guard, scoring against the CIS Microsoft 365 Foundations Benchmark and CISA SCuBA.

Honest gaps in Veri-Tech's CIS Microsoft 365 coverage

If we are positioning Veri-Tech as compatible with the current CIS Microsoft 365 Foundations Benchmark, you should know exactly where our coverage is incomplete. As of 2026-04-28, our registry contains 94 CIS Microsoft 365 control IDs. Of those:

- **71 are actively wired and scanned** on every Veri-Guard run. They produce live pass-or-fail findings.
- **9 are reclassified as manual.** The CIS-recommended posture exists for these controls, but the underlying setting is not exposed via Microsoft Graph in a way that supports automated detection (per-user MFA legacy state, the keep-me-signed-in toggle, custom-script restrictions on personal SharePoint sites, and similar). These return a `skipped-manual` result with a runbook pointing at the admin-portal verification path.
- **14 are still pending automation.** This is the honest gap. They break down as:
  - **9 controls in Section 9 (Power BI and Microsoft Fabric).** Power BI tenant settings are not exposed through the same Graph endpoints we use for other sections. We have a planned ingest path through the Power BI Admin REST API, gated on a Scanner-app permission update. Until that ships, Section 9 results return `pending`, not pass-or-fail.
  - **5 controls in other sections.** Defender for Cloud Apps configuration, per-user MFA legacy state, the keep-me-signed-in toggle, LinkedIn account-connection enablement, and SharePoint personal-site custom-script restriction. Each has a documented blocker (no Graph endpoint, scope mismatch, audience-restricted legacy IAM API). All five are queued for reclassification to manual or for delegated-only detection in a forthcoming worker release.

Net coverage of the current Foundations Benchmark: 71 wired + 9 manual + 14 pending = 94. Wired plus manual is 80 of 94, or roughly 85 percent automated coverage. The remaining 14 are pending and disclosed.

We do not claim full coverage of the current Foundations Benchmark. We claim active coverage of 71 controls, manual coverage of 9, and a documented roadmap for the remaining 14.

Recommended side-by-side workflow

Four steps. Each one is concrete.

1. Deploy OIB as your starter baseline (if you have not already).

Import the OIB Windows v3.7 IntuneManagement bundle (or the relevant macOS or Windows 365 release) into your Intune tenant. Assign profiles to a pilot device group. Validate. Roll out. This is OIB's wheelhouse and Veri-Tune does not displace it.

2. Run a Veri-Tune baseline assessment.

Connect Veri-Tune to your tenant in read-only mode. Run a baseline assessment. You will see three numbers: how many of Veri-Tune's 379 controls are passing, how many are failing or unassigned, and what your configuration drift looks like vs. the deployed posture. Most OIB-using tenants score well on the device-hardening categories and have gaps in App Protection (if iOS or Android is in scope) and tenant-side Intune hygiene.

3. Run a Veri-Guard tenant-config scan.

Veri-Guard covers the CIS Microsoft 365 Foundations Benchmark surface that OIB does not address. Conditional Access, Defender for Office presets, DLP, SharePoint and OneDrive sharing, Teams federation, Exchange Online mail flow. This is the half of the M365 estate OIB never claimed to cover. The scan is a separate run with a separate read-only consent grant.

4. Set both scanners on a schedule.

Veri-Tune and Veri-Guard both support recurring scans. Once your baseline is deployed and your tenant config is hardened, the value of continuous scanning is catching the moment something drifts: an admin unassigns a profile, a new CA policy weakens MFA enforcement, a default flips during a Microsoft service rollout. Daily for high-change tenants, weekly for steady-state, monthly for compliance-only postures.

The simplest mental model: OIB ships you the policies, Veri-Tune watches them, Veri-Guard watches the rest of M365.

Disclaimer and nominative naming

Veri-Tech, Inc. is not affiliated with, endorsed by, certified by, or partnered with the OpenIntuneBaseline project, its maintainers, the Center for Internet Security, Microsoft Corporation, the National Institute of Standards and Technology, the International Organization for Standardization, the American Institute of Certified Public Accountants, or the Cybersecurity and Infrastructure Security Agency.

 OpenIntuneBaseline is a community project maintained at github.com/SkipToTheEndpoint/OpenIntuneBaseline.

Veri-Tech surfaces these frameworks using paraphrased control summaries authored by Veri-Tech. We do not republish verbatim Benchmark prose. See the publishers for the authoritative control text.

Engineers shouldn't also be the audit team.

Veri-Tech, Inc. Veteran-owned. Indiana-based. Founded 2026. veri-tech.net · security@veri-tech.net